Electronic Acknowledgement Receipt

EFS ID:	1547809
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	Method for Establishing Secure Communication Link Between Computers of Virtual Private Network
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	22907
Filer:	Steve S. Chang/Tarsha Howard
Filer Authorized By:	Steve S. Chang
Attorney Docket Number:	
Receipt Date:	27-FEB-2007
Filing Date:	
Time Stamp:	14:39:40
Application Type:	Utility

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$1000
RAM confirmation Number	1
Deposit Account	190733
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1		007170cont1.pdf	343992	yes	80
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	78	
	Claims		79	79	
	Abstract		80	80	
Warnings:					
Information:					
2	Oath or Declaration filed	007170dec.pdf	101669	no	2
Warnings:					
Information:					
3	Drawings	007170figs.pdf	625625	no	40
Warnings:					
Information:					
4	Application Data Sheet	ADS.pdf	1121183	no	5
Warnings:					
Information:					
5	Fee Worksheet (PTO-06)	fee-info.pdf	8391	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2200860		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	1547809
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	Method for Establishing Secure Communication Link Between Computers of Virtual Private Network
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	22907
Filer:	Steve S. Chang/Tarsha Howard
Filer Authorized By:	Steve S. Chang
Attorney Docket Number:	
Receipt Date:	27-FEB-2007
Filing Date:	
Time Stamp:	14:39:40
Application Type:	Utility

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$1000
RAM confirmation Number	1
Deposit Account	190733
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1		007170cont1.pdf	343992	yes	80
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	78	
	Claims		79	79	
	Abstract		80	80	
Warnings:					
Information:					
2	Oath or Declaration filed	007170dec.pdf	101669	no	2
Warnings:					
Information:					
3	Drawings	007170figs.pdf	625625	no	40
Warnings:					
Information:					
4	Application Data Sheet	ADS.pdf	1121183	no	5
Warnings:					
Information:					
5	Fee Worksheet (PTO-06)	fee-info.pdf	8391	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2200860		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority from and is a divisional patent application of co-pending U.S. application serial number 09/558,209, filed April 26, 2000, which is a continuation-in-part patent application of previously-filed U.S. application serial number 09/504,783, filed on February 15, 2000, now U.S. Pat. No. 6,502,135, issued December 31, 2002, which claims priority from and is a continuation-in-part patent application of previously-filed U.S. application serial number 09/429,643, filed on October 29, 1999. The subject matter of U.S. application serial number 09/429,643, which is bodily incorporated herein, derives from provisional U.S. application numbers 60/106,261 (filed October 30, 1998) and 60/137,704 (filed June 7, 1999). The present application is also related to U.S. application serial number 09/558,210, filed April 26, 2000, and which is incorporated by reference herein.

BACKGROUND OF THE INVENTION

A tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet. The variety stems, in part, from the different needs of different Internet users. A basic heuristic framework to aid in discussing these different security techniques is illustrated in FIG. 1. Two terminals, an originating terminal 100 and a destination terminal 110 are in communication over the Internet. It is desired for the communications to be secure, that is, immune to eavesdropping. For example, terminal 100 may transmit secret information to terminal 110 over the Internet 107. Also, it may be desired to prevent an eavesdropper from discovering that terminal 100 is in communication with terminal 110. For example, if terminal 100 is a user and terminal 110 hosts a web site, terminal 100's user may not want anyone in the intervening networks to know what web sites he is "visiting." Anonymity would thus be an issue, for example, for companies that want to keep their market research interests private and thus would prefer to prevent outsiders from knowing which web-sites or other Internet resources they are "visiting." These two security issues may be called data security and anonymity, respectively.

Data security is usually tackled using some form of data encryption. An encryption key 48 is known at both the originating and terminating terminals 100 and 110. The keys may be

Petitioner Apple Inc. - Exhibit 1026, p. 7

private and public at the originating and destination terminals 100 and 110, respectively or they may be symmetrical keys (the same key is used by both parties to encrypt and decrypt). Many encryption methods are known and usable in this context.

To hide traffic from a local administrator or ISP, a user can employ a local proxy server in communicating over an encrypted channel with an outside proxy such that the local administrator or ISP only sees the encrypted traffic. Proxy servers prevent destination servers from determining the identities of the originating clients. This system employs an intermediate server interposed between client and destination server. The destination server sees only the Internet Protocol (IP) address of the proxy server and not the originating client. The target server only sees the address of the outside proxy. This scheme relies on a trusted outside proxy server. Also, proxy schemes are vulnerable to traffic analysis methods of determining identities of transmitters and receivers. Another important limitation of proxy servers is that the server knows the identities of both calling and called parties. In many instances, an originating terminal, such as terminal A, would prefer to keep its identity concealed from the proxy, for example, if the proxy server is provided by an Internet service provider (ISP).

To defeat traffic analysis, a scheme called Chaum's mixes employs a proxy server that transmits and receives fixed length messages, including dummy messages. Multiple originating terminals are connected through a mix (a server) to multiple target servers. It is difficult to tell which of the originating terminals are communicating to which of the connected target servers, and the dummy messages confuse eavesdroppers' efforts to detect communicating pairs by analyzing traffic. A drawback is that there is a risk that the mix server could be compromised. One way to deal with this risk is to spread the trust among multiple mixes. If one mix is compromised, the identities of the originating and target terminals may remain concealed. This strategy requires a number of alternative mixes so that the intermediate servers interposed between the originating and target terminals are not determinable except by compromising more than one mix. The strategy wraps the message with multiple layers of encrypted addresses. The first mix in a sequence can decrypt only the outer layer of the message to reveal the next destination mix in sequence. The second mix can decrypt the message to reveal the next mix and so on. The target server receives the message and, optionally, a multi-layer encrypted payload containing return information to send data back in the same fashion. The only way to defeat such

Petitioner Apple Inc. - Exhibit 1026, p. 8

a mix scheme is to collude among mixes. If the packets are all fixed-length and intermixed with dummy packets, there is no way to do any kind of traffic analysis.

Still another anonymity technique, called 'crowds,' protects the identity of the originating terminal from the intermediate proxies by providing that originating terminals belong to groups of proxies called crowds. The crowd proxies are interposed between originating and target terminals. Each proxy through which the message is sent is randomly chosen by an upstream proxy. Each intermediate proxy can send the message either to another randomly chosen proxy in the "crowd" or to the destination. Thus, even crowd members cannot determine if a preceding proxy is the originator of the message or if it was simply passed from another proxy.

ZKS (Zero-Knowledge Systems) Anonymous IP Protocol allows users to select up to any of five different pseudonyms, while desktop software encrypts outgoing traffic and wraps it in User Datagram Protocol (UDP) packets. The first server in a 2+-hop system gets the UDP packets, strips off one l ayer of encryption to add another, then sends the traffic to the next server, which strips off yet another layer of encryption and adds a new one. The user is permitted to control the number of hops. At the final server, traffic is decrypted with an untraceable IP address. The technique is called onion-routing. This method can be defeated using traffic analysis. For a simple example, bursts of packets from a user during low-duty periods can reveal the identities of sender and receiver.

Firewalls attempt to protect LANs from unauthorized access and hostile exploitation or damage to computers connected to the LAN. Firewalls provide a server through which all access to the LAN must pass. Firewalls are centralized systems that require administrative overhead to maintain. They can be compromised by virtual-machine applications ("applets"). They instill a false sense of security that leads to security breaches for example by users sending sensitive information to servers outside the firewall or encouraging use of modems to sidestep the firewall security. Firewalls are not useful for distributed systems such as business travelers, extranets, small teams, etc.

SUMMARY OF THE INVENTION

A secure mechanism for communicating over the internet, including a protocol referred to as the Tunneled Agile Routing Protocol (TARP), uses a unique two-layer encryption format and special TARP routers. TARP routers are similar in function to regular IP routers. Each TARP router has one or more IP addresses and uses normal IP protocol to send IP packet

Petitioner Apple Inc. - Exhibit 1026, p. 9

messages ("packets" or "datagrams"). The IP packets exchanged between TARP terminals via TARP routers are actually encrypted packets whose true destination address is concealed except to TARP routers and servers. The normal or "clear" or "outside" IP header attached to TARP IP packets contains only the address of a next hop router or destination server. That is, instead of indicating a final destination in the destination field of the IP header, the TARP packet's IP header always points to a next-hop in a series of TARP router hops, or to the final destination. This means there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet since the destination could always be next-hop TARP router as well as the final destination.

Each TARP packet's true destination is concealed behind a layer of encryption generated using a link key. The link key is the encryption key used for encrypted communication between the hops intervening between an originating TARP terminal and a destination TARP terminal. Each TARP router can remove the outer layer of encryption to reveal the destination router for each TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal by the sender/receiver IP numbers in the cleartext IP header.

Once the outer layer of encryption is removed, the TARP router determines the final destination. Each TARP packet 140 undergoes a minimum number of hops to help foil traffic analysis. The hops may be chosen at random or by a fixed value. As a result, each TARP packet may make random trips among a number of geographically disparate routers before reaching its destination. Each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined. This feature is called *agile routing*. The fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. The associated advantages have to do with the inner layer of encryption discussed below. Agile routing is combined with another feature that furthers this purpose; a feature that ensures that any message is broken into multiple packets.

The IP address of a TARP router can be changed, a feature called *IP agility*. Each TARP router, independently or under direction from another TARP terminal or router, can change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time

Petitioner Apple Inc. - Exhibit 1026, p. 10

by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs.

The message payload is hidden behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the intervening TARP routers. The session key is used to decrypt the payloads of the TARP packets permitting the data stream to be reconstructed.

Communication may be made private using link and session keys, which in turn may be shared and used according to any desired method. For example, public/private keys or symmetric keys may be used.

To transmit a data stream, a TARP originating terminal constructs a series of TARP packets from a series of IP packets generated by a network (IP) layer process. (Note that the terms "network layer," "data link layer," "application layer," etc. used in this specification correspond to the Open Systems Interconnection (OSI) network terminology.) The payloads of these packets are assembled into a block and chain-block encrypted using the session key. This assumes, of course, that all the IP packets are destined for the same TARP terminal. The block is then interleaved and the interleaved encrypted block is broken into a series of payloads, one for each TARP packet to be generated. Special TARP headers IP_T are then added to each payload using the IP headers from the data stream packets. The TARP headers can be identical to normal IP headers or customized in some way. They should contain a formula or data for deinterleaving the data at the destination TARP terminal, a time-to-live (TTL) parameter to indicate the number of hops still to be executed, a data type identifier which indicates whether the payload contains, for example, TCP or UDP data, the sender's TARP address, the destination TARP address, and an indicator as to whether the packet contains real or decoy data or a formula for filtering out decoy data if decoy data is spread in some way through the TARP payload data.

Note that although chain-block encryption is discussed here with reference to the session key, any encryption method may be used. Preferably, as in chain block encryption, a method should be used that makes unauthorized decryption difficult without an entire result of the encryption process. Thus, by separating the encrypted block among multiple packets and making it difficult for an interloper to obtain access to all of such packets, the contents of the communications are provided an extra layer of security.

Petitioner Apple Inc. - Exhibit 1026, p. 11

Decoy or dummy data can be added to a stream to help foil traffic analysis by reducing the peak-to-average network load. It may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to portion, or entirety, of a message, and that portion or entirety then interleaved into a number of separate packets. Considering the agile IP routing of the packets, and the attendant difficulty of reconstructing an entire sequence of packets to form a single block-encrypted message element, decoy packets can significantly increase the difficulty of reconstructing an entire data stream.

The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Because the encryption system described above is insertable between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the Network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of

Petitioner Apple Inc. - Exhibit 1026, p. 12

immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicating that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. In addition, it may create a subprocess that maintains the original IP address and continues interacting with the attacker in some manner.

Decoy packets may be generated by each TARP terminal on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis.

In various other embodiments of the invention, a scalable version of the system may be constructed in which a plurality of IP addresses are preassigned to each pair of communicating nodes in the network. Each pair of nodes agrees upon an algorithm for "hopping" between IP addresses (both sending and receiving), such that an eavesdropper sees apparently continuously random IP address pairs (source and destination) for packets transmitted between the pair. Overlapping or "reusable" IP addresses may be allocated to different users on the same subnet, since each node merely verifies that a particular packet includes a valid source/destination pair from the agreed-upon algorithm. Source/destination pairs are preferably not reused between any two nodes during any given end-to-end session, though limited IP block sizes or lengthy sessions might require it.

Further improvements described in this continuation-in-part application include: (1) a load balancer that distributes packets across different transmission paths according to

Petitioner Apple Inc. - Exhibit 1026, p. 13

transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities

The present invention provides key technologies for implementing a secure virtual Internet by using a new agile network protocol that is built on top of the existing Internet protocol (IP). The secure virtual Internet works over the existing Internet infrastructure, and interfaces with client applications the same way as the existing Internet. The key technologies provided by the present invention that support the secure virtual Internet include a "one-click" and "no-click" technique to become part of the secure virtual Internet, a secure domain name service (SDNS) for the secure virtual Internet, and a new approach for interfacing specific client applications onto the secure virtual Internet. According to the invention, the secure domain name service interfaces with existing applications, in addition to providing a way to register and serve domain names and addresses.

According to one aspect of the present invention, a user can conveniently establish a VPN using a "one-click" or a "no-click" technique without being required to enter user identification information, a password and/or an encryption key for establishing a VPN. The advantages of the present invention are provided by a method for establishing a secure communication link between a first computer and a second computer over a computer network, such as the Internet. In one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication, preferably by merely selecting an icon displayed on the first computer. Alternatively, the secure communication mode of communication can be enabled by entering a command into the first computer. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. According to the invention, it is determined whether a secure communication software module is stored on the first computer in response to the step of enabling the secure communication mode of communication. A predetermined computer network address is then accessed for loading the secure communication

Petitioner Apple Inc. - Exhibit 1026, p. 14

software module when the software module is not stored on the first computer. Subsequently, the proxy software module is stored in the first computer. The secure communication link is a virtual private network communication link over the computer network. Preferably, the virtual private network can be based on inserting into each data packet one or more data values that vary according to a pseudo-random sequence. Alternatively, the virtual private network can be based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses or other data values in packets transmitted between the first computer and the second computer, such that the second computer compares the data values in each data packet transmitted between the first computer and the second computer to a moving window of valid values. Yet another alternative provides that the virtual private network can be based on a comparison between a discriminator field in each data packet to a table of valid discriminator fields maintained for the first computer.

According to another aspect of the invention, a command is entered to define a setup parameter associated with the secure communication link mode of communication. Consequently, the secure communication mode is automatically established when a communication link is established over the computer network.

The present invention also provides a computer system having a communication link to a computer network, and a display showing a hyperlink for establishing a virtual private network through the computer network. When the hyperlink for establishing the virtual private network is selected, a virtual private network is established over the computer network. A non-standard top-level domain name is then sent over the virtual private network communication to a predetermined computer network address, such as a computer network address for a secure domain name service (SDNS).

The present invention provides a domain name service that provides secure computer network addresses for secure, non-standard top-level domain names. The advantages of the present invention are provided by a secure domain name service for a computer network that includes a portal connected to a computer network, such as the Internet, and a domain name database connected to the computer network through the portal. According to the invention, the portal authenticates a query for a secure computer network address, and the domain name database stores secure computer network addresses for the computer network. Each secure

Petitioner Apple Inc. - Exhibit 1026, p. 15

computer network address is based on a non-standard top-level domain name, such as .scom, .sorg, .snet, .snet, .sedu, .smil and .sint.

The present invention provides a way to encapsulate existing application network traffic at the application layer of a client computer so that the client application can securely communicate with a server protected by an agile network protocol. The advantages of the present invention are provided by a method for communicating using a private communication link between a client computer and a server computer over a computer network, such as the Internet. According to the invention, an information packet is sent from the client computer to the server computer over the computer network. The information packet contains data that is inserted into the payload portion of the packet at the application layer of the client computer and is used for forming a virtual private connection between the client computer and the server computer. The modified information packet can be sent through a firewall before being sent over the computer network to the server computer and by working on top of existing protocols (i.e., UDP, ICMP and TCP), the present invention more easily penetrates the firewall. The information packet is received at a kernel layer of an operating system on the server side. It is then determined at the kernel layer of the operating system on the host computer whether the information packet contains the data that is used for forming the virtual private connection. The server side replies by sending an information packet to the client computer that has been modified at the kernel layer to containing virtual private connection information in the payload portion of the reply information packet. Preferably, the information packet from the client computer and the reply information packet from the server side are each a UDP protocol information packet. Alternative, both information packets could be a TCP/IP protocol information packet, or an ICMP protocol information packet.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an illustration of secure communications over the Internet according to a prior art embodiment.

FIG. 2 is an illustration of secure communications over the Internet according to a an embodiment of the invention.

FIG. 3a is an illustration of a process of forming a tunneled IP packet according to an embodiment of the invention.

Petitioner Apple Inc. - Exhibit 1026, p. 16

FIG. 3b is an illustration of a process of forming a tunneled IP packet according to another embodiment of the invention.

FIG. 4 is an illustration of an OSI layer location of processes that may be used to implement the invention.

FIG. 5 is a flow chart illustrating a process for routing a tunneled packet according to an embodiment of the invention.

FIG. 6 is a flow chart illustrating a process for forming a tunneled packet according to an embodiment of the invention.

FIG. 7 is a flow chart illustrating a process for receiving a tunneled packet according to an embodiment of the invention.

FIG. 8 shows how a secure session is established and synchronized between a client and a TARP router.

FIG. 9 shows an IP address hopping scheme between a client computer and TARP router using transmit and receive tables in each computer.

FIG. 10 shows physical link redundancy among three Internet Service Providers (ISPs) and a client computer.

FIG. 11 shows how multiple IP packets can be embedded into a single "frame" such as an Ethernet frame, and further shows the use of a discriminator field to camouflage true packet recipients.

FIG. 12A shows a system that employs hopped hardware addresses, hopped IP addresses, and hopped discriminator fields.

FIG. 12B shows several different approaches for hopping hardware addresses, IP addresses, and discriminator fields in combination.

FIG. 13 shows a technique for automatically re-establishing synchronization between sender and receiver through the use of a partially public sync value.

FIG. 14 shows a "checkpoint" scheme for regaining synchronization between a sender and recipient.

FIG. 15 shows further details of the checkpoint scheme of FIG. 14.

FIG. 16 shows how two addresses can be decomposed into a plurality of segments for comparison with presence vectors.

FIG. 17 shows a storage array for a receiver's active addresses.

Petitioner Apple Inc. - Exhibit 1026, p. 17

FIG. 18 shows the receiver's storage array after receiving a sync request.

FIG. 19 shows the receiver's storage array after new addresses have been generated.

FIG. 20 shows a system employing distributed transmission paths.

FIG. 21 shows a plurality of link transmission tables that can be used to route packets in the system of FIG. 20.

FIG. 22A shows a flowchart for adjusting weight value distributions associated with a plurality of transmission links.

FIG. 22B shows a flowchart for setting a weight value to zero if a transmitter turns off.

FIG. 23 shows a system employing distributed transmission paths with adjusted weight value distributions for each path.

FIG. 24 shows an example using the system of FIG. 23.

FIG. 25 shows a conventional domain-name look-up service.

FIG. 26 shows a system employing a DNS proxy server with transparent VPN creation.

FIG. 27 shows steps that can be carried out to implement transparent VPN creation based on a DNS look-up function.

FIG. 28 shows a system including a link guard function that prevents packet overloading on a low-bandwidth link LOW BW.

FIG. 29 shows one embodiment of a system employing the principles of FIG. 28.

FIG. 30 shows a system that regulates packet transmission rates by throttling the rate at which synchronizations are performed.

FIG. 31 shows a signaling server 3101 and a transport server 3102 used to establish a VPN with a client computer.

FIG. 32 shows message flows relating to synchronization protocols of FIG. 31.

FIG. 33 shows a system block diagram of a computer network in which the "one-click" secure communication link of the present invention is suitable for use.

FIG. 34 shows a flow diagram for installing and establishing a "one-click" secure communication link over a computer network according to the present invention.

FIG. 35 shows a flow diagram for registering a secure domain name according to the present invention.

Petitioner Apple Inc. - Exhibit 1026, p. 18

FIG. 36 shows a system block diagram of a computer network in which a private connection according to the present invention can be configured to more easily traverse a firewall between two computer networks.

FIG. 37 shows a flow diagram for establishing a virtual private connection that is encapsulated using an existing network protocol.

DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG. 2, a secure mechanism for communicating over the internet employs a number of special routers or servers, called TARP routers 122-127 that are similar to regular IP routers 128-132 in that each has one or more IP addresses and uses normal IP protocol to send normal-looking IP packet messages, called TARP packets 140. TARP packets 140 are identical to normal IP packet messages that are routed by regular IP routers 128-132 because each TARP packet 140 contains a destination address as in a normal IP packet. However, instead of indicating a final destination in the destination field of the IP header, the TARP packet's 140 IP header always points to a next-hop in a series of TARP router hops, or the final destination, TARP terminal 110. Because the header of the TARP packet contains only the next-hop destination, there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet 140 since the destination could always be the next-hop TARP router as well as the final destination, TARP terminal 110.

Each TARP packet's true destination is concealed behind an outer layer of encryption generated using a link key 146. The link key 146 is the encryption key used for encrypted communication between the end points (TARP terminals or TARP routers) of a single link in the chain of hops connecting the originating TARP terminal 100 and the destination TARP terminal 110. Each TARP router 122-127, using the link key 146 it uses to communicate with the previous hop in a chain, can use the link key to reveal the true destination of a TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal (which may indicate the link key used) by the sender field of the clear IP header. Alternatively, this identity may be hidden behind another layer of encryption in available bits in the clear IP header. Each TARP router, upon receiving a TARP message, determines if the message is a TARP message by using authentication data in the TARP packet. This could be recorded in available bytes in the TARP packet's IP header. Alternatively, TARP packets could be authenticated by attempting to decrypt

Petitioner Apple Inc. - Exhibit 1026, p. 19

using the link key 146 and determining if the results are as expected. The former may have computational advantages because it does not involve a decryption process.

Once the outer layer of decryption is completed by a TARP router 122-127, the TARP router determines the final destination. The system is preferably designed to cause each TARP packet 140 to undergo a minimum number of hops to help foil traffic analysis. The time to live counter in the IP header of the TARP message may be used to indicate a number of TARP router hops yet to be completed. Each TARP router then would decrement the counter and determine from that whether it should forward the TARP packet 140 to another TARP router 122-127 or to the destination TARP terminal 110. If the time to live counter is zero or below zero after decrementing, for an example of usage, the TARP router receiving the TARP packet 140 may forward the TARP packet 140 to the destination TARP terminal 110. If the time to live counter is above zero after decrementing, for an example of usage, the TARP router receiving the TARP packet 140 may forward the TARP packet 140 to a TARP router 122-127 that the current TARP terminal chooses at random. As a result, each TARP packet 140 is routed through some minimum number of hops of TARP routers 122-127 which are chosen at random.

Thus, each TARP packet, irrespective of the traditional factors determining traffic in the Internet, makes random trips among a number of geographically disparate routers before reaching its destination and each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined as described above. This feature is called *agile routing*. For reasons that will become clear shortly, the fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. Agile routing is combined with another feature that furthers this purpose, a feature that ensures that any message is broken into multiple packets.

A TARP router receives a TARP packet when an IP address used by the TARP router coincides with the IP address in the TARP packet's IP header IP_C. The IP address of a TARP router, however, may not remain constant. To avoid and manage attacks, each TARP router, independently or under direction from another TARP terminal or router, may change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or

Petitioner Apple Inc. - Exhibit 1026, p. 20

terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs. In reality, whenever a TARP router looks up the address of a destination in the encrypted header, it must convert a TARP address to a real IP address using its LUT.

While every TARP router receiving a TARP packet has the ability to determine the packet's final destination, the message payload is embedded behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the TARP routers 122-127 intervening between the originating 100 and destination 110 TARP terminals. The session key is used to decrypt the payloads of the TARP packets 140 permitting an entire message to be reconstructed.

In one embodiment, communication may be made private using link and session keys, which in turn may be shared and used according any desired method. For example, a public key or symmetric keys may be communicated between link or session endpoints using a public key method. Any of a variety of other mechanisms for securing data to ensure that only authorized computers can have access to the private information in the TARP packets 140 may be used as desired.

Referring to FIG. 3a, to construct a series of TARP packets, a data stream 300 of IP packets 207a, 207b, 207c, etc., such series of packets being formed by a network (IP) layer process, is broken into a series of small sized segments. In the present example, equal-sized segments 1-9 are defined and used to construct a set of interleaved data packets A, B, and C. Here it is assumed that the number of interleaved packets A, B, and C formed is three and that the number of IP packets 207a-207c used to form the three interleaved packets A, B, and C is exactly three. Of course, the number of IP packets spread over a group of interleaved packets may be any convenient number as may be the number of interleaved packets over which the incoming data stream is spread. The latter, the number of interleaved packets over which the data stream is spread, is called the *interleave window*.

To create a packet, the transmitting software interleaves the normal IP packets 207a *et. seq.* to form a new set of interleaved payload data 320. This payload data 320 is then encrypted using a session key to form a set of session-key-encrypted payload data 330, each of which, A, B, and C, will form the payload of a TARP packet. Using the IP header data, from the original packets 207a-207c, new TARP headers IP_T are formed. The TARP headers IP_T can be identical

Petitioner Apple Inc. - Exhibit 1026, p. 21

to normal IP headers or customized in some way. In a preferred embodiment, the TARP headers IP_T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers:

1. A window sequence number – an identifier that indicates where the packet belongs in the original message sequence.
2. An interleave sequence number – an identifier that indicates the interleaving sequence used to form the packet so that the packet can be deinterleaved along with other packets in the interleave window.
3. A time-to-live (TTL) datum – indicates the number of TARP-router-hops to be executed before the packet reaches its destination. Note that the TTL parameter may provide a datum to be used in a probabilistic formula for determining whether to route the packet to the destination or to another hop.
4. Data type identifier – indicates whether the payload contains, for example, TCP or UDP data.
5. Sender's address – indicates the sender's address in the TARP network.
6. Destination address – indicates the destination terminal's address in the TARP network.
7. Decoy/Real – an indicator of whether the packet contains real message data or dummy decoy data or a combination.

Obviously, the packets going into a single interleave window must include only packets with a common destination. Thus, it is assumed in the depicted example that the IP headers of IP packets 207a-207c all contain the same destination address or at least will be received by the same terminal so that they can be deinterleaved. Note that dummy or decoy data or packets can be added to form a larger interleave window than would otherwise be required by the size of a given message. Decoy or dummy data can be added to a stream to help foil traffic analysis by leveling the load on the network. Thus, it may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

Petitioner Apple Inc. - Exhibit 1026, p. 22

Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to a portion, or the entirety, of a message, and that portion or entirety then interleaved into a number of separate packets.

Referring to FIG. 3b, in an alternative mode of TARP packet construction, a series of IP packets are accumulated to make up a predefined interleave window. The payloads of the packets are used to construct a single block 520 for chain block encryption using the session key. The payloads used to form the block are presumed to be destined for the same terminal. The block size may coincide with the interleave window as depicted in the example embodiment of FIG. 3b. After encryption, the encrypted block is broken into separate payloads and segments which are interleaved as in the embodiment of Fig 3a. The resulting interleaved packets A, B, and C, are then packaged as TARP packets with TARP headers as in the Example of FIG. 3a. The remaining process is as shown in, and discussed with reference to, FIG. 3a.

Once the TARP packets 340 are formed, each entire TARP packet 340, including the TARP header IP_T, is encrypted using the link key for communication with the first-hop-TARP router. The first hop TARP router is randomly chosen. A final unencrypted IP header IP_C is added to each encrypted TARP packet 340 to form a normal IP packet 360 that can be transmitted to a TARP router. Note that the process of constructing the TARP packet 360 does not have to be done in stages as described. The above description is just a useful heuristic for describing the final product, namely, the TARP packet.

Note that, TARP header IP_T could be a completely custom header configuration with no similarity to a normal IP header except that it contain the information identified above. This is so since this header is interpreted by only TARP routers.

The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Referring to FIG. 4, a TARP transceiver 405 can be an originating terminal 100, a destination terminal 110, or a TARP router 122-127. In each TARP Transceiver 405, a transmitting process is generated to receive normal packets from the Network (IP) layer and generate TARP packets

Petitioner Apple Inc. - Exhibit 1026, p. 23

for communication over the network. A receiving process is generated to receive normal IP packets containing TARP packets and generate from these normal IP packets which are "passed up" to the Network (IP) layer. Note that where the TARP Transceiver 405 is a router, the received TARP packets 140 are not processed into a stream of IP packets 415 because they need only be authenticated as proper TARP packets and then passed to another TARP router or a TARP destination terminal 110. The intervening process, a "TARP Layer" 420, could be combined with either the data link layer 430 or the Network layer 410. In either case, it would intervene between the data link layer 430 so that the process would receive regular IP packets containing embedded TARP packets and "hand up" a series of reassembled IP packets to the Network layer 410. As an example of combining the TARP layer 420 with the data link layer 430, a program may augment the normal processes running a communications card, for example, an Ethernet card. Alternatively, the TARP layer processes may form part of a dynamically loadable module that is loaded and executed to support communications between the network and data link layers.

Because the encryption system described above can be inserted between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

Note that IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

Petitioner Apple Inc. - Exhibit 1026, p. 24

As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicates that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. To accomplish this, the TARP process will construct a TARP-formatted message, in the style of Internet Control Message Protocol (ICMP) datagrams as an example; this message will contain the machine's TARP address, its previous IP address, and its new IP address. The TARP layer will transmit this packet to at least one known TARP router; then upon receipt and validation of the message, the TARP router will update its LUT with the new IP address for the stated TARP address. The TARP router will then format a similar message, and broadcast it to the other TARP routers so that they may update their LUTs. Since the total number of TARP routers on any given subnet is expected to be relatively small, this process of updating the LUTs should be relatively fast. It may not, however, work as well when there is a relatively large number of TARP routers and/or a relatively large number of clients; this has motivated a refinement of this architecture to provide scalability; this refinement has led to a second embodiment, which is discussed below.

Upon detection of an attack, the TARP process may also create a subprocess that maintains the original IP address and continues interacting with the attacker. The latter may provide an opportunity to trace the attacker or study the attacker's methods (called "fishbowling" drawing upon the analogy of a small fish in a fish bowl that "thinks" it is in the ocean but is actually under captive observation). A history of the communication between the attacker and the abandoned (fishbowled) IP address can be recorded or transmitted for human analysis or further synthesized for purposes of responding in some way.

As mentioned above, decoy or dummy data or packets can be added to outgoing data streams by TARP terminals or routers. In addition to making it convenient to spread data over a larger number of separate packets, such decoy packets can also help to level the load on inactive portions of the Internet to help foil traffic analysis efforts.

Decoy packets may be generated by each TARP terminal 100, 110 or each router 122-127 on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated

Petitioner Apple Inc. - Exhibit 1026, p. 25

in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. That is, when a series of messages are received, the decoy packet generation rate may be increased. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis. The rate of reception of packets, decoy or otherwise, may be indicated to the decoy packet dropping and generating processes through perishable decoy and regular packet counters. (A perishable counter is one that resets or decrements its value in response to time so that it contains a high value when it is incremented in rapid succession and a small value when incremented either slowly or a small number of times in rapid succession.) Note that destination TARP terminal 110 may generate decoy packets equal in number and size to those TARP packets received to make it appear it is merely routing packets and is therefore not the destination terminal.

Referring to FIG. 5, the following particular steps may be employed in the above-described method for routing TARP packets.

- S0. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.
- S2. The TARP packet may be probed in some way to authenticate the packet before attempting to decrypt it using the link key. That is, the router may determine that the packet is an authentic TARP packet by performing a selected operation on some data included with the clear IP header attached to the encrypted TARP packet contained in the payload. This makes it possible to avoid performing decryption on packets that are not authentic TARP packets.
- S3. The TARP packet is decrypted to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.
- S4. If the packet is a decoy packet, the perishable decoy counter is incremented.

Petitioner Apple Inc. - Exhibit 1026, p. 26

- S5. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the router may choose to throw it away. If the received packet is a decoy packet and it is determined that it should be thrown away (S6), control returns to step S0.
- S7. The TTL parameter of the TARP header is decremented and it is determined if the TTL parameter is greater than zero.
- S8. If the TTL parameter is greater than zero, a TARP address is randomly chosen from a list of TARP addresses maintained by the router and the link key and IP address corresponding to that TARP address memorized for use in creating a new IP packet containing the TARP packet.
- S9. If the TTL parameter is zero or less, the link key and IP address corresponding to the TARP address of the destination are memorized for use in creating the new IP packet containing the TARP packet.
- S10. The TARP packet is encrypted using the memorized link key.
- S11. An IP header is added to the packet that contains the stored IP address, the encrypted TARP packet wrapped with an IP header, and the completed packet transmitted to the next hop or destination.

Referring to FIG. 6, the following particular steps may be employed in the above-described method for generating TARP packets.

- S20. A background loop operation applies an algorithm that determines the generation of decoy IP packets. The loop is interrupted when a data stream containing IP packets is received for transmission.
- S21. The received IP packets are grouped into a set consisting of messages with a constant IP destination address. The set is further broken down to coincide with a maximum size of an interleave window The set is encrypted, and interleaved into a set of payloads destined to become TARP packets.
- S22. The TARP address corresponding to the IP address is determined from a lookup table and stored to generate the TARP header. An initial TTL count is generated and stored in the

Petitioner Apple Inc. - Exhibit 1026, p. 27

header. The TTL count may be random with minimum and maximum values or it may be fixed or determined by some other parameter.

- S23. The window sequence numbers and interleave sequence numbers are recorded in the TARP headers of each packet.
- S24. One TARP router address is randomly chosen for each TARP packet and the IP address corresponding to it stored for use in the clear IP header. The link key corresponding to this router is identified and used to encrypt TARP packets containing interleaved and encrypted data and TARP headers.
- S25. A clear IP header with the first hop router's real IP address is generated and added to each of the encrypted TARP packets and the resulting packets.

Referring to FIG. 7, the following particular steps may be employed in the above-described method for receiving TARP packets.

- S40. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.
- S42. The TARP packet may be probed to authenticate the packet before attempting to decrypt it using the link key.
- S43. The TARP packet is decrypted with the appropriate link key to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.
- S44. If the packet is a decoy packet, the perishable decoy counter is incremented.
- S45. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the receiver may choose to throw it away.
- S46. The TARP packets are cached until all packets forming an interleave window are received.
- S47. Once all packets of an interleave window are received, the packets are deinterleaved.
- S48. The packets block of combined packets defining the interleave window is then decrypted using the session key.

Petitioner Apple Inc. - Exhibit 1026, p. 28

- S49. The decrypted block is then divided using the window sequence data and the IP_T headers are converted into normal IP_C headers. The window sequence numbers are integrated in the IP_C headers.
- S50. The packets are then handed up to the IP layer processes.

1. SCALABILITY ENHANCEMENTS

The IP agility feature described above relies on the ability to transmit IP address changes to all TARP routers. The embodiments including this feature will be referred to as "boutique" embodiments due to potential limitations in scaling these features up for a large network, such as the Internet. (The "boutique" embodiments would, however, be robust for use in smaller networks, such as small virtual private networks, for example). One problem with the boutique embodiments is that if IP address changes are to occur frequently, the message traffic required to update all routers sufficiently quickly creates a serious burden on the Internet when the TARP router and/or client population gets large. The bandwidth burden added to the networks, for example in ICMP packets, that would be used to update all the TARP routers could overwhelm the Internet for a large scale implementation that approached the scale of the Internet. In other words, the boutique system's scalability is limited.

A system can be constructed which trades some of the features of the above embodiments to provide the benefits of IP agility without the additional messaging burden. This is accomplished by IP address-hopping according to shared algorithms that govern IP addresses used between links participating in communications sessions between nodes such as TARP nodes. (Note that the IP hopping technique is also applicable to the boutique embodiment.) The IP agility feature discussed with respect to the boutique system can be modified so that it becomes decentralized under this scalable regime and governed by the above-described shared algorithm. Other features of the boutique system may be combined with this new type of IP-agility.

The new embodiment has the advantage of providing IP agility governed by a local algorithm and set of IP addresses exchanged by each communicating pair of nodes. This local governance is session-independent in that it may govern communications between a pair of nodes, irrespective of the session or end points being transferred between the directly communicating pair of nodes.

Petitioner Apple Inc. - Exhibit 1026, p. 29

In the scalable embodiments, blocks of IP addresses are allocated to each node in the network. (This scalability will increase in the future, when Internet Protocol addresses are increased to 128-bit fields, vastly increasing the number of distinctly addressable nodes). Each node can thus use any of the IP addresses assigned to that node to communicate with other nodes in the network. Indeed, each pair of communicating nodes can use a plurality of source IP addresses and destination IP addresses for communicating with each other.

Each communicating pair of nodes in a chain participating in any session stores two blocks of IP addresses, called netblocks, and an algorithm and randomization seed for selecting, from each netblock, the next pair of source/destination IP addresses that will be used to transmit the next message. In other words, the algorithm governs the sequential selection of IP-address pairs, one sender and one receiver IP address, from each netblock. The combination of algorithm, seed, and netblock (IP address block) will be called a "hopblock." A router issues separate transmit and receive hopblocks to its clients. The send address and the receive address of the IP header of each outgoing packet sent by the client are filled with the send and receive IP addresses generated by the algorithm. The algorithm is "clocked" (indexed) by a counter so that each time a pair is used, the algorithm turns out a new transmit pair for the next packet to be sent.

The router's receive hopblock is identical to the client's transmit hopblock. The router uses the receive hopblock to predict what the send and receive IP address pair for the next expected packet from that client will be. Since packets can be received out of order, it is not possible for the router to predict with certainty what IP address pair will be on the next sequential packet. To account for this problem, the router generates a range of predictions encompassing the number of possible transmitted packet send/receive addresses, of which the next packet received could leap ahead. Thus, if there is a vanishingly small probability that a given packet will arrive at the router ahead of 5 packets transmitted by the client before the given packet, then the router can generate a series of 6 send/receive IP address pairs (or "hop window") to compare with the next received packet. When a packet is received, it is marked in the hop window as such, so that a second packet with the same IP address pair will be discarded. If an out-of-sequence packet does not arrive within a predetermined timeout period, it can be requested for retransmission or simply discarded from the receive table, depending upon the protocol in use for that communications session, or possibly by convention.

Petitioner Apple Inc. - Exhibit 1026, p. 30

When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set. Received packets that do not have the predicted source/destination IP addresses falling with the window are rejected, thus thwarting possible hackers. (With the number of possible combinations, even a fairly large window would be hard to fall into at random.) If it is a member of this set, the router accepts the packet and processes it further. This link-based IP-hopping strategy, referred to as "IHOP," is a network element that stands on its own and is not necessarily accompanied by elements of the boutique system described above. If the routing agility feature described in connection with the boutique embodiment is combined with this link-based IP-hopping strategy, the router's next step would be to decrypt the TARP header to determine the destination TARP router for the packet and determine what should be the next hop for the packet. The TARP router would then forward the packet to a random TARP router or the destination TARP router with which the source TARP router has a link-based IP hopping communication established.

Figure 8 shows how a client computer 801 and a TARP router 811 can establish a secure session. When client 801 seeks to establish an IHOP session with TARP router 811, the client 801 sends "secure synchronization" request ("SSYN") packet 821 to the TARP router 811. This SYN packet 821 contains the client's 801 authentication token, and may be sent to the router 811 in an encrypted format. The source and destination IP numbers on the packet 821 are the client's 801 current fixed IP address, and a "known" fixed IP address for the router 811. (For security purposes, it may be desirable to reject any packets from outside of the local network that are destined for the router's known fixed IP address.) Upon receipt and validation of the client's 801 SSYN packet 821, the router 811 responds by sending an encrypted "secure synchronization acknowledgment" ("SSYN ACK") 822 to the client 801. This SSYN ACK 822 will contain the transmit and receive hopblocks that the client 801 will use when communicating with the TARP router 811. The client 801 will acknowledge the TARP router's 811 response packet 822 by generating an encrypted SSYN ACK ACK packet 823 which will be sent from the client's 801 fixed IP address and to the TARP router's 811 known fixed IP address. The client 801 will simultaneously generate a SSYN ACK ACK packet; this SSYN ACK packet, referred to as the Secure Session Initiation (SSI) packet 824, will be sent with the first {sender, receiver} IP pair in the client's transmit table 921 (FIG. 9), as specified in the transmit hopblock provided by the

Petitioner Apple Inc. - Exhibit 1026, p. 31

TARP router 811 in the SSYN ACK packet 822. The TARP router 811 will respond to the SSI packet 824 with an SSI ACK packet 825, which will be sent with the first {sender, receiver} IP pair in the TARP router's transmit table 923. Once these packets have been successfully exchanged, the secure communications session is established, and all further secure communications between the client 801 and the TARP router 811 will be conducted via this secure session, as long as synchronization is maintained. If synchronization is lost, then the client 801 and TARP router 802 may re-establish the secure session by the procedure outlined in Figure 8 and described above.

While the secure session is active, both the client 901 and TARP router 911 (FIG. 9) will maintain their respective transmit tables 921, 923 and receive tables 922, 924, as provided by the TARP router during session synchronization 822. It is important that the sequence of IP pairs in the client's transmit table 921 be identical to those in the TARP router's receive table 924; similarly, the sequence of IP pairs in the client's receive table 922 must be identical to those in the router's transmit table 923. This is required for the session synchronization to be maintained. The client 901 need maintain only one transmit table 921 and one receive table 922 during the course of the secure session. Each sequential packet sent by the client 901 will employ the next {send, receive} IP address pair in the transmit table, regardless of TCP or UDP session. The TARP router 911 will expect each packet arriving from the client 901 to bear the next IP address pair shown in its receive table.

Since packets can arrive out of order, however, the router 911 can maintain a "look ahead" buffer in its receive table, and will mark previously-received IP pairs as invalid for future packets; any future packet containing an IP pair that is in the look-ahead buffer but is marked as previously received will be discarded. Communications from the TARP router 911 to the client 901 are maintained in an identical manner; in particular, the router 911 will select the next IP address pair from its transmit table 923 when constructing a packet to send to the client 901, and the client 901 will maintain a look-ahead buffer of expected IP pairs on packets that it is receiving. Each TARP router will maintain separate pairs of transmit and receive tables for each client that is currently engaged in a secure session with or through that TARP router.

While clients receive their hopblocks from the first server linking them to the Internet, routers exchange hopblocks. When a router establishes a link-based IP-hopping communication regime with another router, each router of the pair exchanges its transmit hopblock. The transmit

Petitioner Apple Inc. - Exhibit 1026, p. 32

hopblock of each router becomes the receive hopblock of the other router. The communication between routers is governed as described by the example of a client sending a packet to the first router.

While the above strategy works fine in the IP milieu, many local networks that are connected to the Internet are Ethernet systems. In Ethernet, the IP addresses of the destination devices must be translated into hardware addresses, and vice versa, using known processes ("address resolution protocol," and "reverse address resolution protocol"). However, if the link-based IP-hopping strategy is employed, the correlation process would become explosive and burdensome. An alternative to the link-based IP hopping strategy may be employed within an Ethernet network. The solution is to provide that the node linking the Internet to the Ethernet (call it the border node) use the link-based IP-hopping communication regime to communicate with nodes outside the Ethernet LAN. Within the Ethernet LAN, each TARP node would have a single IP address which would be addressed in the conventional way. Instead of comparing the {sender, receiver} IP address pairs to authenticate a packet, the intra-LAN TARP node would use one of the IP header extension fields to do so. Thus, the border node uses an algorithm shared by the intra-LAN TARP node to generate a symbol that is stored in the free field in the IP header, and the intra-LAN TARP node generates a range of symbols based on its prediction of the next expected packet to be received from that particular source IP address. The packet is rejected if it does not fall into the set of predicted symbols (for example, numerical values) or is accepted if it does. Communications from the intra-LAN TARP node to the border node are accomplished in the same manner, though the algorithm will necessarily be different for security reasons. Thus, each of the communicating nodes will generate transmit and receive tables in a similar manner to that of Figure 9; the intra-LAN TARP nodes transmit table will be identical to the border node's receive table, and the intra-LAN TARP node's receive table will be identical to the border node's transmit table.

The algorithm used for IP address-hopping can be any desired algorithm. For example, the algorithm can be a given pseudo-random number generator that generates numbers of the range covering the allowed IP addresses with a given seed. Alternatively, the session participants can assume a certain type of algorithm and specify simply a parameter for applying the algorithm. For example the assumed algorithm could be a particular pseudo-random number generator and the session participants could simply exchange seed values.

Petitioner Apple Inc. - Exhibit 1026, p. 33

Note that there is no permanent physical distinction between the originating and destination terminal nodes. Either device at either end point can initiate a synchronization of the pair. Note also that the authentication/synchronization-request (and acknowledgment) and hopblock-exchange may all be served by a single message so that separate message exchanges may not be required.

As another extension to the stated architecture, multiple physical paths can be used by a client, in order to provide link redundancy and further thwart attempts at denial of service and traffic monitoring. As shown in Figure 10, for example, client 1001 can establish three simultaneous sessions with each of three TARP routers provided by different ISPs 1011, 1012, 1013. As an example, the client 1001 can use three different telephone lines 1021, 1022, 1023 to connect to the ISPs, or two telephone lines and a cable modem, etc. In this scheme, transmitted packets will be sent in a random fashion among the different physical paths. This architecture provides a high degree of communications redundancy, with improved immunity from denial-of-service attacks and traffic monitoring.

2. FURTHER EXTENSIONS

The following describes various extensions to the techniques, systems, and methods described above. As described above, the security of communications occurring between computers in a computer network (such as the Internet, an Ethernet, or others) can be enhanced by using seemingly random source and destination Internet Protocol (IP) addresses for data packets transmitted over the network. This feature prevents eavesdroppers from determining which computers in the network are communicating with each other while permitting the two communicating computers to easily recognize whether a given received data packet is legitimate or not. In one embodiment of the above-described systems, an IP header extension field is used to authenticate incoming packets on an Ethernet.

Various extensions to the previously described techniques described herein include: (1) use of hopped hardware or "MAC" addresses in broadcast type network; (2) a self-synchronization technique that permits a computer to automatically regain synchronization with a sender; (3) synchronization algorithms that allow transmitting and receiving computers to quickly re-establish synchronization in the event of lost packets or other events; and (4) a fast-packet rejection mechanism for rejecting invalid packets. Any or all of these extensions can be combined with the features described above in any of various ways.

Petitioner Apple Inc. - Exhibit 1026, p. 34

A. Hardware Address Hopping

Internet protocol-based communications techniques on a LAN—or across any dedicated physical medium—typically embed the IP packets within lower-level packets, often referred to as "frames." As shown in FIG. 11, for example, a first Ethernet frame 1150 comprises a frame header 1101 and two embedded IP packets IP1 and IP2, while a second Ethernet frame 1160 comprises a different frame header 1104 and a single IP packet IP3. Each frame header generally includes a source hardware address 1101A and a destination hardware address 1101B; other well-known fields in frame headers are omitted from FIG. 11 for clarity. Two hardware nodes communicating over a physical communication channel insert appropriate source and destination hardware addresses to indicate which nodes on the channel or network should receive the frame.

It may be possible for a nefarious listener to acquire information about the contents of a frame and/or its communicants by examining frames on a local network rather than (or in addition to) the IP packets themselves. This is especially true in broadcast media, such as Ethernet, where it is necessary to insert into the frame header the hardware address of the machine that generated the frame and the hardware address of the machine to which frame is being sent. All nodes on the network can potentially "see" all packets transmitted across the network. This can be a problem for secure communications, especially in cases where the communicants do not want for any third party to be able to identify who is engaging in the information exchange. One way to address this problem is to push the address-hopping scheme down to the hardware layer. In accordance with various embodiments of the invention, hardware addresses are "hopped" in a manner similar to that used to change IP addresses, such that a listener cannot determine which hardware node generated a particular message nor which node is the intended recipient.

FIG. 12A shows a system in which Media Access Control ("MAC") hardware addresses are "hopped" in order to increase security over a network such as an Ethernet. While the description refers to the exemplary case of an Ethernet environment, the inventive principles are equally applicable to other types of communications media. In the Ethernet case, the MAC address of the sender and receiver are inserted into the Ethernet frame and can be observed by anyone on the LAN who is within the broadcast range for that frame. For secure

Petitioner Apple Inc. - Exhibit 1026, p. 35

communications, it becomes desirable to generate frames with MAC addresses that are not attributable to any specific sender or receiver.

As shown in FIG. 12A, two computer nodes 1201 and 1202 communicate over a communication channel such as an Ethernet. Each node executes one or more application programs 1203 and 1218 that communicate by transmitting packets through communication software 1204 and 1217, respectively. Examples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like. Communication software 1204 and 1217 can comprise, for example, an OSI layered architecture or "stack" that standardizes various services provided at different levels of functionality.

The lowest levels of communication software 1204 and 1217 communicate with hardware components 1206 and 1214 respectively, each of which can include one or more registers 1207 and 1215 that allow the hardware to be reconfigured or controlled in accordance with various communication protocols. The hardware components (an Ethernet network interface card, for example) communicate with each other over the communication medium. Each hardware component is typically pre-assigned a fixed hardware address or MAC number that identifies the hardware component to other nodes on the network. One or more interface drivers control the operation of each card and can, for example, be configured to accept or reject packets from certain hardware addresses. As will be described in more detail below, various embodiments of the inventive principles provide for "hopping" different addresses using one or more algorithms and one or more moving windows that track a range of valid addresses to validate received packets. Packets transmitted according to one or more of the inventive principles will be generally referred to as "secure" packets or "secure communications" to differentiate them from ordinary data packets that are transmitted in the clear using ordinary, machine-correlated addresses.

One straightforward method of generating non-attributable MAC addresses is an extension of the IP hopping scheme. In this scenario, two machines on the same LAN that desire to communicate in a secure fashion exchange random-number generators and seeds, and create sequences of quasi-random MAC addresses for synchronized hopping. The implementation and synchronization issues are then similar to that of IP hopping.

This approach, however, runs the risk of using MAC addresses that are currently active on the LAN—which, in turn, could interrupt communications for those machines. Since an

Petitioner Apple Inc. - Exhibit 1026, p. 36

Ethernet MAC address is at present 48 bits in length, the chance of randomly misusing an active MAC address is actually quite small. However, if that figure is multiplied by a large number of nodes (as would be found on an extensive LAN), by a large number of frames (as might be the case with packet voice or streaming video), and by a large number of concurrent Virtual Private Networks (VPNs), then the chance that a non-secure machine's MAC address could be used in an address-hopped frame can become non-trivial. In short, any scheme that runs even a small risk of interrupting communications for other machines on the LAN is bound to receive resistance from prospective system administrators. Nevertheless, it is technically feasible, and can be implemented without risk on a LAN on which there is a small number of machines, or if all of the machines on the LAN are engaging in MAC-hopped communications.

Synchronized MAC address hopping may incur some overhead in the course of session establishment, especially if there are multiple sessions or multiple nodes involved in the communications. A simpler method of randomizing MAC addresses is to allow each node to receive and process *every* incident frame on the network. Typically, each network interface driver will check the destination MAC address in the header of every incident frame to see if it matches that machine's MAC address; if there is no match, then the frame is discarded. In one embodiment, however, these checks can be disabled, and every incident packet is passed to the TARP stack for processing. This will be referred to as "promiscuous" mode, since every incident frame is processed. Promiscuous mode allows the sender to use completely random, unsynchronized MAC addresses, since the destination machine is guaranteed to process the frame. The decision as to whether the packet was truly intended for that machine is handled by the TARP stack, which checks the source and destination IP addresses for a match in its IP synchronization tables. If no match is found, the packet is discarded; if there is a match, the packet is unwrapped, the inner header is evaluated, and if the inner header indicates that the packet is destined for that machine then the packet is forwarded to the IP stack—otherwise it is discarded.

One disadvantage of purely-random MAC address hopping is its impact on processing overhead; that is, since every incident frame must be processed, the machine's CPU is engaged considerably more often than if the network interface driver is discriminating and rejecting packets unilaterally. A compromise approach is to select either a single fixed MAC address or a small number of MAC addresses (e.g., one for each virtual private network on an Ethernet) to

Petitioner Apple Inc. - Exhibit 1026, p. 37

use for MAC-hopped communications, regardless of the actual recipient for which the message is intended. In this mode, the network interface driver can check each incident frame against one (or a few) pre-established MAC addresses, thereby freeing the CPU from the task of physical-layer packet discrimination. This scheme does not betray any useful information to an interloper on the LAN; in particular, every secure packet can already be identified by a unique packet type in the outer header. However, since all machines engaged in secure communications would either be using the same MAC address, or be selecting from a small pool of predetermined MAC addresses, the association between a specific machine and a specific MAC address is effectively broken.

In this scheme, the CPU will be engaged more often than it would be in non-secure communications (or in synchronized MAC address hopping), since the network interface driver cannot always unilaterally discriminate between secure packets that are destined for that machine, and secure packets from other VPNs. However, the non-secure traffic is easily eliminated at the network interface, thereby reducing the amount of processing required of the CPU. There are boundary conditions where these statements would not hold, of course—e.g., if *all* of the traffic on the LAN is secure traffic, then the CPU would be engaged to the same degree as it is in the purely-random address hopping case; alternatively, if each VPN on the LAN uses a different MAC address, then the network interface can perfectly discriminate secure frames destined for the local machine from those constituting other VPNs. These are engineering tradeoffs that might be best handled by providing administrative options for the users when installing the software and/or establishing VPNs.

Even in this scenario, however, there still remains a slight risk of selecting MAC addresses that are being used by one or more nodes on the LAN. One solution to this problem is to formally assign one address or a range of addresses for use in MAC-hopped communications. This is typically done via an assigned numbers registration authority; e.g., in the case of Ethernet, MAC address ranges are assigned to vendors by the Institute of Electrical and Electronics Engineers (IEEE). A formally-assigned range of addresses would ensure that secure frames do not conflict with any properly-configured and properly-functioning machines on the LAN.

Reference will now be made to FIGS. 12A and 12B in order to describe the many combinations and features that follow the inventive principles. As explained above, two

Petitioner Apple Inc. - Exhibit 1026, p. 38

computer nodes 1201 and 1202 are assumed to be communicating over a network or communication medium such as an Ethernet. A communication protocol in each node (1204 and 1217, respectively) contains a modified element 1205 and 1216 that performs certain functions that deviate from the standard communication protocols. In particular, computer node 1201 implements a first "hop" algorithm 1208X that selects seemingly random source and destination IP addresses (and, in one embodiment, seemingly random IP header discriminator fields) in order to transmit each packet to the other computer node. For example, node 1201 maintains a transmit table 1208 containing triplets of source (S), destination (D), and discriminator fields (DS) that are inserted into outgoing IP packet headers. The table is generated through the use of an appropriate algorithm (e.g., a random number generator that is seeded with an appropriate seed) that is known to the recipient node 1202. As each new IP packet is formed, the next sequential entry out of the sender's transmit table 1208 is used to populate the IP source, IP destination, and IP header extension field (e.g., discriminator field). It will be appreciated that the transmit table need not be created in advance but could instead be created on-the-fly by executing the algorithm when each packet is formed.

At the receiving node 1202, the same IP hop algorithm 1222X is maintained and used to generate a receive table 1222 that lists valid triplets of source IP address, destination IP address, and discriminator field. This is shown by virtue of the first five entries of transmit table 1208 matching the second five entries of receive table 1222. (The tables may be slightly offset at any particular time due to lost packets, misordered packets, or transmission delays). Additionally, node 1202 maintains a receive window W3 that represents a list of valid IP source, IP destination, and discriminator fields that will be accepted when received as part of an incoming IP packet. As packets are received, window W3 slides down the list of valid entries, such that the possible valid entries change over time. Two packets that arrive out of order but are nevertheless matched to entries within window W3 will be accepted; those falling outside of window W3 will be rejected as invalid. The length of window W3 can be adjusted as necessary to reflect network delays or other factors.

Node 1202 maintains a similar transmit table 1221 for creating IP packets and frames destined for node 1201 using a potentially different hopping algorithm 1221X, and node 1201 maintains a matching receive table 1209 using the same algorithm 1209X. As node 1202 transmits packets to node 1201 using seemingly random IP source, IP destination, and/or

Petitioner Apple Inc. - Exhibit 1026, p. 39

discriminator fields, node 1201 matches the incoming packet values to those falling within window W1 maintained in its receive table. In effect, transmit table 1208 of node 1201 is synchronized (i.e., entries are selected in the same order) to receive table 1222 of receiving node 1202. Similarly, transmit table 1221 of node 1202 is synchronized to receive table 1209 of node 1201. It will be appreciated that although a common algorithm is shown for the source, destination and discriminator fields in FIG. 12A (using, e.g., a different seed for each of the three fields), an entirely different algorithm could in fact be used to establish values for each of these fields. It will also be appreciated that one or two of the fields can be "hopped" rather than all three as illustrated.

In accordance with another aspect of the invention, hardware or "MAC" addresses are hopped instead of or in addition to IP addresses and/or the discriminator field in order to improve security in a local area or broadcast-type network. To that end, node 1201 further maintains a transmit table 1210 using a transmit algorithm 1210X to generate source and destination hardware addresses that are inserted into frame headers (e.g., fields 1101A and 1101B in FIG. 11) that are synchronized to a corresponding receive table 1224 at node 1202. Similarly, node 1202 maintains a different transmit table 1223 containing source and destination hardware addresses that is synchronized with a corresponding receive table 1211 at node 1201. In this manner, outgoing hardware frames appear to be originating from and going to completely random nodes on the network, even though each recipient can determine whether a given packet is intended for it or not. It will be appreciated that the hardware hopping feature can be implemented at a different level in the communications protocol than the IP hopping feature (e.g., in a card driver or in a hardware card itself to improve performance).

FIG. 12B shows three different embodiments or modes that can be employed using the aforementioned principles. In a first mode referred to as "promiscuous" mode, a common hardware address (e.g., a fixed address for source and another for destination) or else a completely random hardware address is used by all nodes on the network, such that a particular packet cannot be attributed to any one node. Each node must initially accept all packets containing the common (or random) hardware address and inspect the IP addresses or discriminator field to determine whether the packet is intended for that node. In this regard, either the IP addresses or the discriminator field or both can be varied in accordance with an algorithm as described above. As explained previously, this may increase each node's overhead

Petitioner Apple Inc. - Exhibit 1026, p. 40

since additional processing is involved to determine whether a given packet has valid source and destination hardware addresses.

In a second mode referred to as "promiscuous per VPN" mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over a virtual private network. For example, if there are six nodes on an Ethernet, and the network is to be split up into two private virtual networks such that nodes on one VPN can communicate with only the other two nodes on its own VPN, then two sets of hardware addresses could be used: one set for the first VPN and a second set for the second VPN. This would reduce the amount of overhead involved in checking for valid frames since only packets arriving from the designated VPN would need to be checked. IP addresses and one or more discriminator fields could still be hopped as before for secure communication within the VPN. Of course, this solution compromises the anonymity of the VPNs (i.e., an outsider can easily tell what traffic belongs in which VPN, though he cannot correlate it to a specific machine/person). It also requires the use of a discriminator field to mitigate the vulnerability to certain types of DoS attacks. (For example, without the discriminator field, an attacker on the LAN could stream frames containing the MAC addresses being used by the VPN; rejecting those frames could lead to excessive processing overhead. The discriminator field would provide a low-overhead means of rejecting the false packets.)

In a third mode referred to as "hardware hopping" mode, hardware addresses are varied as illustrated in FIG. 12A, such that hardware source and destination addresses are changed constantly in order to provide non-attributable addressing. Variations on these embodiments are of course possible, and the invention is not intended to be limited in any respect by these illustrative examples.

B. Extending the Address Space

Address hopping provides security and privacy. However, the level of protection is limited by the number of addresses in the blocks being hopped. A hopblock denotes a field or fields modulated on a packet-wise basis for the purpose of providing a VPN. For instance, if two nodes communicate with IP address hopping using hopblocks of 4 addresses (2 bits) each, there would be 16 possible address-pair combinations. A window of size 16 would result in most address pairs being accepted as valid most of the time. This limitation can be overcome by using a discriminator field in addition to or instead of the hopped address fields. The discriminator

Petitioner Apple Inc. - Exhibit 1026, p. 41

field would be hopped in exactly the same fashion as the address fields and it would be used to determine whether a packet should be processed by a receiver.

Suppose that two clients, each using four-bit hopblocks, would like the same level of protection afforded to clients communicating via IP hopping between two A blocks (24 address bits eligible for hopping). A discriminator field of 20 bits, used in conjunction with the 4 address bits eligible for hopping in the IP address field, provides this level of protection. A 24-bit discriminator field would provide a similar level of protection if the address fields were not hopped or ignored. Using a discriminator field offers the following advantages: (1) an arbitrarily high level of protection can be provided, and (2) address hopping is unnecessary to provide protection. This may be important in environments where address hopping would cause routing problems.

C. Synchronization Techniques

It is generally assumed that once a sending node and receiving node have exchanged algorithms and seeds (or similar information sufficient to generate quasi-random source and destination tables), subsequent communication between the two nodes will proceed smoothly. Realistically, however, two nodes may lose synchronization due to network delays or outages, or other problems. Consequently, it is desirable to provide means for re-establishing synchronization between nodes in a network that have lost synchronization.

One possible technique is to require that each node provide an acknowledgment upon successful receipt of each packet and, if no acknowledgment is received within a certain period of time, to re-send the unacknowledged packet. This approach, however, drives up overhead costs and may be prohibitive in high-throughput environments such as streaming video or audio, for example.

A different approach is to employ an automatic synchronizing technique that will be referred to herein as "self-synchronization." In this approach, synchronization information is embedded into each packet, thereby enabling the receiver to re-synchronize itself upon receipt of a single packet if it determines that is has lost synchronization with the sender. (If communications are already in progress, and the receiver determines that it is still in sync with the sender, then there is no need to re-synchronize.) A receiver could detect that it was out of synchronization by, for example, employing a "dead-man" timer that expires after a certain

Petitioner Apple Inc. - Exhibit 1026, p. 42

period of time, wherein the timer is reset with each valid packet. A time stamp could be hashed into the public sync field (see below) to preclude packet-retry attacks.

In one embodiment, a "sync field" is added to the header of each packet sent out by the sender. This sync field could appear in the clear or as part of an encrypted portion of the packet. Assuming that a sender and receiver have selected a random-number generator (RNG) and seed value, this combination of RNG and seed can be used to generate a random-number sequence (RNS). The RNS is then used to generate a sequence of source/destination IP pairs (and, if desired, discriminator fields and hardware source and destination addresses), as described above. It is not necessary, however, to generate the entire sequence (or the first N-1 values) in order to generate the Nth random number in the sequence; if the sequence index N is known, the random value corresponding to that index can be directly generated (see below). Different RNGs (and seeds) with different fundamental periods could be used to generate the source and destination IP sequences, but the basic concepts would still apply. For the sake of simplicity, the following discussion will assume that IP source and destination address pairs (only) are hopped using a single RNG sequencing mechanism.

In accordance with a "self-synchronization" feature, a sync field in each packet header provides an index (i.e., a sequence number) into the RNS that is being used to generate IP pairs. Plugging this index into the RNG that is being used to generate the RNS yields a specific random number value, which in turn yields a specific IP pair. That is, an IP pair can be generated directly from knowledge of the RNG, seed, and index number; it is not necessary, in this scheme, to generate the entire sequence of random numbers that precede the sequence value associated with the index number provided.

Since the communicants have presumably previously exchanged RNGs and seeds, the only new information that must be provided in order to generate an IP pair is the sequence number. If this number is provided by the sender in the packet header, then the receiver need only plug this number into the RNG in order to generate an IP pair – and thus verify that the IP pair appearing in the header of the packet is valid. In this scheme, if the sender and receiver lose synchronization, the receiver can immediately re-synchronize upon receipt of a single packet by simply comparing the IP pair in the packet header to the IP pair generated from the index number. Thus, synchronized communications can be resumed upon receipt of a single packet, making this scheme ideal for multicast communications. Taken to the extreme, it could obviate

Petitioner Apple Inc. - Exhibit 1026, p. 43

the need for synchronization tables entirely; that is, the sender and receiver could simply rely on the index number in the sync field to validate the IP pair on each packet, and thereby eliminate the tables entirely.

The aforementioned scheme may have some inherent security issues associated with it — namely, the placement of the sync field. If the field is placed in the outer header, then an interloper could observe the values of the field and their relationship to the IP stream. This could potentially compromise the algorithm that is being used to generate the IP-address sequence, which would compromise the security of the communications. If, however, the value is placed in the inner header, then the sender must decrypt the inner header before it can extract the sync value and validate the IP pair; this opens up the receiver to certain types of denial-of-service (DoS) attacks, such as packet replay. That is, if the receiver must decrypt a packet before it can validate the IP pair, then it could potentially be forced to expend a significant amount of processing on decryption if an attacker simply retransmits previously valid packets. Other attack methodologies are possible in this scenario.

A possible compromise between algorithm security and processing speed is to split up the sync value between an inner (encrypted) and outer (unencrypted) header. That is, if the sync value is sufficiently long, it could potentially be split into a rapidly-changing part that can be viewed in the clear, and a fixed (or very slowly changing) part that must be protected. The part that can be viewed in the clear will be called the "public sync" portion and the part that must be protected will be called the "private sync" portion.

Both the public sync and private sync portions are needed to generate the complete sync value. The private portion, however, can be selected such that it is fixed or will change only occasionally. Thus, the private sync value can be stored by the recipient, thereby obviating the need to decrypt the header in order to retrieve it. If the sender and receiver have previously agreed upon the frequency with which the private part of the sync will change, then the receiver can selectively decrypt a single header in order to extract the new private sync if the communications gap that has led to lost synchronization has exceeded the lifetime of the previous private sync. This should not represent a burdensome amount of decryption, and thus should not open up the receiver to denial-of-service attack simply based on the need to occasionally decrypt a single header.

Petitioner Apple Inc. - Exhibit 1026, p. 44

One implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value. This implementation is shown in FIG. 13, where (for example) a first ISP 1302 is the sender and a second ISP 1303 is the receiver. (Other alternatives are possible from FIG. 13.) A transmitted packet comprises a public or "outer" header 1305 that is not encrypted, and a private or "inner" header 1306 that is encrypted using for example a link key. Outer header 1305 includes a public sync portion while inner header 1306 contains the private sync portion. A receiving node decrypts the inner header using a decryption function 1307 in order to extract the private sync portion. This step is necessary only if the lifetime of the currently buffered private sync has expired. (If the currently-buffered private sync is still valid, then it is simply extracted from memory and "added" (which could be an inverse hash) to the public sync, as shown in step 1308.) The public and decrypted private sync portions are combined in function 1308 in order to generate the combined sync 1309. The combined sync (1309) is then fed into the RNG (1310) and compared to the IP address pair (1311) to validate or reject the packet.

An important consideration in this architecture is the concept of "future" and "past" where the public sync values are concerned. Though the sync values, themselves, should be random to prevent spoofing attacks, it may be important that the receiver be able to quickly identify a sync value that has already been sent — even if the packet containing that sync value was never actually received by the receiver. One solution is to hash a time stamp or sequence number into the public sync portion, which could be quickly extracted, checked, and discarded, thereby validating the public sync portion itself.

In one embodiment, packets can be checked by comparing the source/destination IP pair generated by the sync field with the pair appearing in the packet header. If (1) they match, (2) the time stamp is valid, and (3) the dead-man timer has expired, then re-synchronization occurs; otherwise, the packet is rejected. If enough processing power is available, the dead-man timer and synchronization tables can be avoided altogether, and the receiver would simply resynchronize (e.g., validate) on every packet.

The foregoing scheme may require large-integer (e.g., 160-bit) math, which may affect its implementation. Without such large-integer registers, processing throughput would be affected, thus potentially affecting security from a denial-of-service standpoint. Nevertheless, as large-

Petitioner Apple Inc. - Exhibit 1026, p. 45

integer math processing features become more prevalent, the costs of implementing such a feature will be reduced.

D. Other Synchronization Schemes

As explained above, if W or more consecutive packets are lost between a transmitter and receiver in a VPN (where W is the window size), the receiver's window will not have been updated and the transmitter will be transmitting packets not in the receiver's window. The sender and receiver will not recover synchronization until perhaps the random pairs in the window are repeated by chance. Therefore, there is a need to keep a transmitter and receiver in synchronization whenever possible and to re-establish synchronization whenever it is lost.

A "checkpoint" scheme can be used to regain synchronization between a sender and a receiver that have fallen out of synchronization. In this scheme, a checkpoint message comprising a random IP address pair is used for communicating synchronization information. In one embodiment, two messages are used to communicate synchronization information between a sender and a recipient:

1. SYNC_REQ is a message used by the sender to indicate that it wants to synchronize; and
2. SYNC_ACK is a message used by the receiver to inform the transmitter that it has been synchronized.

According to one variation of this approach, both the transmitter and receiver maintain three checkpoints (see FIG. 14):

1. In the transmitter, ckpt_o ("checkpoint old") is the IP pair that was used to re-send the last SYNC_REQ packet to the receiver. In the receiver, ckpt_o ("checkpoint old") is the IP pair that receives repeated SYNC_REQ packets from the transmitter.
2. In the transmitter, ckpt_n ("checkpoint new") is the IP pair that will be used to send the next SYNC_REQ packet to the receiver. In the receiver, ckpt_n ("checkpoint new") is the IP pair that receives a new SYNC_REQ packet from the transmitter and which causes the receiver's window to be re-aligned, ckpt_o set to ckpt_n, a new ckpt_n to be generated and a new ckpt_r to be generated.
3. In the transmitter, ckpt_r is the IP pair that will be used to send the next SYNC_ACK packet to the receiver. In the receiver, ckpt_r is the IP pair that receives a new SYNC_ACK packet from the transmitter and which causes a new ckpt_n to be

Petitioner Apple Inc. - Exhibit 1026, p. 46

generated. Since SYNC_ACK is transmitted from the receiver ISP to the sender ISP, the transmitter ckpt_r refers to the ckpt_r of the receiver and the receiver ckpt_r refers to the ckpt_r of the transmitter (see FIG. 14).

When a transmitter initiates synchronization, the IP pair it will use to transmit the next data packet is set to a predetermined value and when a receiver first receives a SYNC_REQ, the receiver window is updated to be centered on the transmitter's next IP pair. This is the primary mechanism for checkpoint synchronization.

Synchronization can be initiated by a packet counter (e.g., after every N packets transmitted, initiate a synchronization) or by a timer (every S seconds, initiate a synchronization) or a combination of both. See FIG. 15. From the transmitter's perspective, this technique operates as follows: (1) Each transmitter periodically transmits a "sync request" message to the receiver to make sure that it is in sync. (2) If the receiver is still in sync, it sends back a "sync ack" message. (If this works, no further action is necessary). (3) If no "sync ack" has been received within a period of time, the transmitter retransmits the sync request again. If the transmitter reaches the next checkpoint without receiving a "sync ack" response, then synchronization is broken, and the transmitter should stop transmitting. The transmitter will continue to send sync_reqs until it receives a sync_ack , at which point transmission is reestablished.

From the receiver's perspective, the scheme operates as follows: (1) when it receives a "sync request" request from the transmitter, it advances its window to the next checkpoint position (even skipping pairs if necessary), and sends a "sync ack" message to the transmitter. If sync was never lost, then the "jump ahead" really just advances to the next available pair of addresses in the table (i.e., normal advancement).

If an interloper intercepts the "sync request" messages and tries to interfere with communication by sending new ones, it will be ignored if the synchronization has been established or it will actually help to re-establish synchronization.

A window is realigned whenever a re-synchronization occurs. This realignment entails updating the receiver's window to straddle the address pairs used by the packet transmitted immediately after the transmission of the SYNC_REQ packet. Normally, the transmitter and receiver are in synchronization with one another. However, when network events occur, the receiver's window may have to be advanced by many steps during resynchronization. In this

Petitioner Apple Inc. - Exhibit 1026, p. 47

case, it is desirable to move the window ahead without having to step through the intervening random numbers sequentially. (This feature is also desirable for the auto-sync approach discussed above).

E. Random Number Generator with a Jump-Ahead capability

An attractive method for generating randomly hopped addresses is to use identical random number generators in the transmitter and receiver and advance them as packets are transmitted and received. There are many random number generation algorithms that could be used. Each one has strengths and weaknesses for address hopping applications.

Linear congruential random number generators (LCRs) are fast, simple and well characterized random number generators that can be made to jump ahead *n* steps efficiently. An LCR generates random numbers $X_1, X_2, X_3 \ldots X_k$ starting with seed X_0 using a recurrence

$$X_i=(a\ X_{i-1} + b) \bmod c, \qquad (1)$$

where a, b and c define a particular LCR. Another expression for X_i,

$$X_i=((a^i(X_0+b)-b)/(a-1)) \bmod c \quad (2)$$

enables the jump-ahead capability. The factor a^i can grow very large even for modest i if left unfettered. Therefore some special properties of the modulo operation can be used to control the size and processing time required to compute (2). (2) can be rewritten as:

$$X_i=(a^i\ (X_0(a-1)+b)-b)/(a-1) \bmod c. \quad (3)$$

It can be shown that:

$$(a^i(X_0(a-1)+b)-b)/(a-1) \bmod c =$$

$$((a^i \bmod((a-1)c)(X_0(a-1)+b) -b) /(a-1)) \bmod c \qquad (4).$$

$(X_0(a-1)+b)$ can be stored as $(X_0(a-1)+b) \bmod c$, b as b mod c and compute $a^i \bmod((a-1)c)$ (this requires O(log(i)) steps).

A practical implementation of this algorithm would jump a fixed distance, n, between synchronizations; this is tantamount to synchronizing every *n* packets. The window would commence *n* IP pairs from the start of the previous window. Using X_j^w, the random number at the j^{th} checkpoint, as X_0 and *n* as *i*, a node can store $a^n \bmod((a-1)c)$ once per LCR and set

$$X_{j+1}^w=X_{n(j+1)}=((a^n \bmod((a-1)c)\ (X_j^w\ (a-1)+b)-b)/(a-1))\bmod c, \quad (5)$$

to generate the random number for the $j+1^{th}$ synchronization. Using this construction, a node could jump ahead an arbitrary (but fixed) distance between synchronizations in a constant amount of time (independent of n).

Petitioner Apple Inc. - Exhibit 1026, p. 48

Pseudo-random number generators, in general, and LCRs, in particular, will eventually repeat their cycles. This repetition may present vulnerability in the IP hopping scheme. An adversary would simply have to wait for a repeat to predict future sequences. One way of coping with this vulnerability is to create a random number generator with a known long cycle. A random sequence can be replaced by a new random number generator before it repeats. LCRs can be constructed with known long cycles. This is not currently true of many random number generators.

Random number generators can be cryptographically insecure. An adversary can derive the RNG parameters by examining the output or part of the output. This is true of LCGs. This vulnerability can be mitigated by incorporating an encryptor, designed to scramble the output as part of the random number generator. The random number generator prevents an adversary from mounting an attack—e.g., a known plaintext attack—against the encryptor.

F. Random Number Generator Example

Consider a RNG where a=31,b=4 and c=15. For this case equation (1) becomes:

$X_i=(31\ X_{i-1} + 4) \bmod 15$. (6)

If one sets $X_0=1$, equation (6) will produce the sequence 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 0, 4, 8, 12. This sequence will repeat indefinitely. For a jump ahead of 3 numbers in this sequence $a^n= 31^3=29791$, $c*(a-1)=15*30=450$ and $a^n \bmod((a-1)c) = 31^3 \bmod(15*30)=29791 \bmod(450)=91$. Equation (5) becomes:

$((91\ (X_i30+4)-4)/30) \bmod 15$ (7).

Table 1 shows the jump ahead calculations from (7) . The calculations start at 5 and jump ahead 3.

TABLE 1

I	X_i	(X_i30+4)	$91\ (X_i30+4)-4$	$((91\ (X_i30+4)-4)/30$	X_{i+3}
1	5	154	14010	467	2
4	2	64	5820	194	14
7	14	424	38580	1286	11
10	11	334	30390	1013	8
13	8	244	22200	740	5

G. Fast Packet Filter

Petitioner Apple Inc. - Exhibit 1026, p. 49

Address hopping VPNs must rapidly determine whether a packet has a valid header and thus requires further processing, or has an invalid header (a hostile packet) and should be immediately rejected. Such rapid determinations will be referred to as "fast packet filtering." This capability protects the VPN from attacks by an adversary who streams hostile packets at the receiver at a high rate of speed in the hope of saturating the receiver's processor (a so-called "denial of service" attack). Fast packet filtering is an important feature for implementing VPNs on shared media such as Ethernet.

Assuming that all participants in a VPN share an unassigned "A" block of addresses, one possibility is to use an experimental "A" block that will never be assigned to any machine that is not address hopping on the shared medium. "A" blocks have a 24 bits of address that can be hopped as opposed to the 8 bits in "C" blocks. In this case a hopblock will be the "A" block. The use of the experimental "A" block is a likely option on an Ethernet because:

1. The addresses have no validity outside of the Ethernet and will not be routed out to a valid outside destination by a gateway.
2. There are 2^{24} (~16 million) addresses that can be hopped within each "A" block. This yields >280 trillion possible address pairs making it very unlikely that an adversary would guess a valid address. It also provides acceptably low probability of collision between separate VPNs (all VPNs on a shared medium independently generate random address pairs from the same "A" block).
3. The packets will not be received by someone on the Ethernet who is not on a VPN (unless the machine is in promiscuous mode) minimizing impact on non-VPN computers.

The Ethernet example will be used to describe one implementation of fast packet filtering. The ideal algorithm would quickly examine a packet header, determine whether the packet is hostile, and reject any hostile packets or determine which active IP pair the packet header matches. The problem is a classical associative memory problem. A variety of techniques have been developed to solve this problem (hashing, B–trees etc). Each of these approaches has its strengths and weaknesses. For instance, hash tables can be made to operate quite fast in a statistical sense, but can occasionally degenerate into a much slower algorithm. This slowness can persist for a period of time. Since there is a need to discard hostile packets quickly at all times, hashing would be unacceptable.

H. Presence Vector Algorithm

Petitioner Apple Inc. - Exhibit 1026, p. 50

A presence vector is a bit vector of length 2^n that can be indexed by n-bit numbers (each ranging from 0 to 2^n-1). One can indicate the presence of k n-bit numbers (not necessarily unique), by setting the bits in the presence vector indexed by each number to 1. Otherwise, the bits in the presence vector are 0. An n-bit number, x, is one of the k numbers if and only if the x^{th} bit of the presence vector is 1. A fast packet filter can be implemented by indexing the presence vector and looking for a 1, which will be referred to as the "test."

For example, suppose one wanted to represent the number 135 using a presence vector. The 135^{th} bit of the vector would be set. Consequently, one could very quickly determine whether an address of 135 was valid by checking only one bit: the 135^{th} bit. The presence vectors could be created in advance corresponding to the table entries for the IP addresses. In effect, the incoming addresses can be used as indices into a long vector, making comparisons very fast. As each RNG generates a new address, the presence vector is updated to reflect the information. As the window moves, the presence vector is updated to zero out addresses that are no longer valid.

There is a trade-off between efficiency of the test and the amount of memory required for storing the presence vector(s). For instance, if one were to use the 48 bits of hopping addresses as an index, the presence vector would have to be 35 terabytes. Clearly, this is too large for practical purposes. Instead, the 48 bits can be divided into several smaller fields. For instance, one could subdivide the 48 bits into four 12-bit fields (see FIG. 16). This reduces the storage requirement to 2048 bytes at the expense of occasionally having to process a hostile packet. In effect, instead of one long presence vector, the decomposed address portions must match all four shorter presence vectors before further processing is allowed. (If the first part of the address portion doesn't match the first presence vector, there is no need to check the remaining three presence vectors).

A presence vector will have a 1 in the y^{th} bit if and only if one or more addresses with a corresponding field of y are active. An address is active only if each presence vector indexed by the appropriate sub-field of the address is 1.

Consider a window of 32 active addresses and 3 checkpoints. A hostile packet will be rejected by the indexing of one presence vector more than 99% of the time. A hostile packet will be rejected by the indexing of all 4 presence vectors more than 99.9999995% of the time. On average, hostile packets will be rejected in less than 1.02 presence vector index operations.

Petitioner Apple Inc. - Exhibit 1026, p. 51

The small percentage of hostile packets that pass the fast packet filter will be rejected when matching pairs are not found in the active window or are active checkpoints. Hostile packets that serendipitously match a header will be rejected when the VPN software attempts to decrypt the header. However, these cases will be extremely rare. There are many other ways this method can be configured to arbitrate the space/speed tradeoffs.

I. Further Synchronization Enhancements

A slightly modified form of the synchronization techniques described above can be employed. The basic principles of the previously described checkpoint synchronization scheme remain unchanged. The actions resulting from the reception of the checkpoints are, however, slightly different. In this variation, the receiver will maintain between OoO ("Out of Order") and 2×WINDOW_SIZE+OoO active addresses (1 ≤OoO ≤WINDOW_SIZE and WINDOW_SIZE ≥1). OoO and WINDOW_SIZE are engineerable parameters, where OoO is the minimum number of addresses needed to accommodate lost packets due to events in the network or out of order arrivals and WINDOW_SIZE is the number of packets transmitted before a SYNC_REQ is issued. FIG. 17 depicts a storage array for a receiver's active addresses.

The receiver starts with the first 2×WINDOW_SIZE addresses loaded and active (ready to receive data). As packets are received, the corresponding entries are marked as "used" and are no longer eligible to receive packets. The transmitter maintains a packet counter, initially set to 0, containing the number of data packets transmitted since the last *initial* transmission of a SYNC_REQ for which SYNC_ACK has been received. When the transmitter packet counter equals WINDOW_SIZE, the transmitter generates a SYNC_REQ and does its initial transmission. When the receiver receives a SYNC_REQ corresponding to its current CKPT_N, it generates the next WINDOW_SIZE addresses and starts loading them in order starting at the first location after the last active address wrapping around to the beginning of the array after the end of the array has been reached. The receiver's array might look like FIG. 18 when a SYNC_REQ has been received. In this case a couple of packets have been either lost or will be received out of order when the SYNC_REQ is received.

FIG. 19 shows the receiver's array after the new addresses have been generated. If the transmitter does not receive a SYNC_ACK, it will re-issue the SYNC_REQ at regular intervals. When the transmitter receives a SYNC_ACK, the packet counter is decremented by WINDOW_SIZE. If the packet counter reaches 2×WINDOW_SIZE – OoO then the transmitter

Petitioner Apple Inc. - Exhibit 1026, p. 52

ceases sending data packets until the appropriate SYNC_ACK is finally received. The transmitter then resumes sending data packets. Future behavior is essentially a repetition of this initial cycle. The advantages of this approach are:

1. There is no need for an efficient jump ahead in the random number generator,
2. No packet is ever transmitted that does not have a corresponding entry in the receiver side
3. No timer based re-synchronization is necessary. This is a consequence of 2.
4. The receiver will always have the ability to accept data messages transmitted within OoO messages of the most recently transmitted message.

J. Distributed Transmission Path Variant

Another embodiment incorporating various inventive principles is shown in FIG. 20. In this embodiment, a message transmission system includes a first computer 2001 in communication with a second computer 2002 through a network 2011 of intermediary computers. In one variant of this embodiment, the network includes two edge routers 2003 and 2004 each of which is linked to a plurality of Internet Service Providers (ISPs) 2005 through 2010. Each ISP is coupled to a plurality of other ISPs in an arrangement as shown in FIG. 20, which is a representative configuration only and is not intended to be limiting. Each connection between ISPs is labeled in FIG. 20 to indicate a specific physical transmission path (e.g., AD is a physical path that links ISP A (element 2005) to ISP D (element 2008)). Packets arriving at each edge router are selectively transmitted to one of the ISPs to which the router is attached on the basis of a randomly or quasi-randomly selected basis.

As shown in FIG. 21, computer 2001 or edge router 2003 incorporates a plurality of link transmission tables 2100 that identify, for each potential transmission path through the network, valid sets of IP addresses that can be used to transmit the packet. For example, AD table 2101 contains a plurality of IP source/destination pairs that are randomly or quasi-randomly generated. When a packet is to be transmitted from first computer 2001 to second computer 2002, one of the link tables is randomly (or quasi-randomly) selected, and the next valid source/destination address pair from that table is used to transmit the packet through the network. If path AD is randomly selected, for example, the next source/destination IP address pair (which is pre-determined to transmit between ISP A (element 2005) and ISP B (element 2008)) is used to transmit the packet. If one of the transmission paths becomes degraded or inoperative, that link

Petitioner Apple Inc. - Exhibit 1026, p. 53

table can be set to a "down" condition as shown in table 2105, thus preventing addresses from being selected from that table. Other transmission paths would be unaffected by this broken link.

3. CONTINUATION-IN-PART IMPROVEMENTS

The following describes various improvements and features that can be applied to the embodiments described above. The improvements include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities. Each is discussed separately below.

A. Load Balancer

Various embodiments described above include a system in which a transmitting node and a receiving node are coupled through a plurality of transmission paths, and wherein successive packets are distributed quasi-randomly over the plurality of paths. See, for example, FIGS. 20 and 21 and accompanying description. The improvement extends this basic concept to encompass distributing packets across different paths in such a manner that the loads on the paths are generally balanced according to transmission link quality.

In one embodiment, a system includes a transmitting node and a receiving node that are linked via a plurality of transmission paths having potentially varying transmission quality. Successive packets are transmitted over the paths based on a weight value distribution function for each path. The rate that packets will be transmitted over a given path can be different for each path. The relative "health" of each transmission path is monitored in order to identify paths that have become degraded. In one embodiment, the health of each path is monitored in the transmitter by comparing the number of packets transmitted to the number of packet acknowledgements received. Each transmission path may comprise a physically separate path (e.g., via dial-up phone line, computer network, router, bridge, or the like), or may comprise logically separate paths contained within a broadband communication medium (e.g., separate channels in an FDM, TDM, CDMA, or other type of modulated or unmodulated transmission link).

Petitioner Apple Inc. - Exhibit 1026, p. 54

When the transmission quality of a path falls below a predetermined threshold and there are other paths that can transmit packets, the transmitter changes the weight value used for that path, making it less likely that a given packet will be transmitted over that path. The weight will preferably be set no lower than a minimum value that keeps nominal traffic on the path. The weights of the other available paths are altered to compensate for the change in the affected path. When the quality of a path degrades to where the transmitter is turned off by the synchronization function (i.e., no packets are arriving at the destination), the weight is set to zero. If all transmitters are turned off, no packets are sent.

Conventional TCP/IP protocols include a "throttling" feature that reduces the transmission rate of packets when it is determined that delays or errors are occurring in transmission. In this respect, timers are sometimes used to determine whether packets have been received. These conventional techniques for limiting transmission of packets, however, do not involve multiple transmission paths between two nodes wherein transmission across a particular path relative to the others is changed based on link quality.

According to certain embodiments, in order to damp oscillations that might otherwise occur if weight distributions are changed drastically (e.g., according to a step function), a linear or an exponential decay formula can be applied to gradually decrease the weight value over time that a degrading path will be used. Similarly, if the health of a degraded path improves, the weight value for that path is gradually increased.

Transmission link health can be evaluated by comparing the number of packets that are acknowledged within the transmission window (see embodiments discussed above) to the number of packets transmitted within that window and by the state of the transmitter (i.e., on or off). In other words, rather than accumulating general transmission statistics over time for a path, one specific implementation uses the "windowing" concepts described above to evaluate transmission path health.

The same scheme can be used to shift virtual circuit paths from an "unhealthy" path to a "healthy" one, and to select a path for a new virtual circuit.

FIG. 22A shows a flowchart for adjusting weight values associated with a plurality of transmission links. It is assumed that software executing in one or more computer nodes executes the steps shown in FIG. 22A. It is also assumed that the software can be stored on a computer-readable medium such as a magnetic or optical disk for execution by a computer.

Petitioner Apple Inc. - Exhibit 1026, p. 55

Beginning in step 2201, the transmission quality of a given transmission path is measured. As described above, this measurement can be based on a comparison between the number of packets transmitted over a particular link to the number of packet acknowledgements received over the link (e.g., per unit time, or in absolute terms). Alternatively, the quality can be evaluated by comparing the number of packets that are acknowledged within the transmission window to the number of packets that were transmitted within that window. In yet another variation, the number of missed synchronization messages can be used to indicate link quality. Many other variations are of course possible.

In step 2202, a check is made to determine whether more than one transmitter (e.g., transmission path) is turned on. If not, the process is terminated and resumes at step 2201.

In step 2203, the link quality is compared to a given threshold (e.g., 50%, or any arbitrary number). If the quality falls below the threshold, then in step 2207 a check is made to determine whether the weight is above a minimum level (e.g., 1%). If not, then in step 2209 the weight is set to the minimum level and processing resumes at step 2201. If the weight is above the minimum level, then in step 2208 the weight is gradually decreased for the path, then in step 2206 the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are increased).

If in step 2203 the quality of the path was greater than or equal to the threshold, then in step 2204 a check is made to determine whether the weight is less than a steady-state value for that path. If so, then in step 2205 the weight is increased toward the steady-state value, and in step 2206 the weights for the remaining paths are adjusted accordingly to compensate (e.g., they are decreased). If in step 2204 the weight is not less than the steady-state value, then processing resumes at step 2201 without adjusting the weights.

The weights can be adjusted incrementally according to various functions, preferably by changing the value gradually. In one embodiment, a linearly decreasing function is used to adjust the weights; according to another embodiment, an exponential decay function is used. Gradually changing the weights helps to damp oscillators that might otherwise occur if the probabilities were abruptly.

Although not explicitly shown in FIG. 22A the process can be performed only periodically (e.g., according to a time schedule), or it can be continuously run, such as in a background mode of operation. In one embodiment, the combined weights of all potential paths

Petitioner Apple Inc. - Exhibit 1026, p. 56

should add up to unity (e.g., when the weighting for one path is decreased, the corresponding weights that the other paths will be selected will increase).

Adjustments to weight values for other paths can be prorated. For example, a decrease of 10% in weight value for one path could result in an evenly distributed increase in the weights for the remaining paths. Alternatively, weightings could be adjusted according to a weighted formula as desired (e.g., favoring healthy paths over less healthy paths). In yet another variation, the difference in weight value can be amortized over the remaining links in a manner that is proportional to their traffic weighting.

FIG. 22B shows steps that can be executed to shut down transmission links where a transmitter turns off. In step 2210, a transmitter shut-down event occurs. In step 2211, a test is made to determine whether at least one transmitter is still turned on. If not, then in step 2215 all packets are dropped until a transmitter turns on. If in step 2211 at least one transmitter is turned on, then in step 2212 the weight for the path is set to zero, and the weights for the remaining paths are adjusted accordingly.

FIG. 23 shows a computer node 2301 employing various principles of the above-described embodiments. It is assumed that two computer nodes of the type shown in FIG. 23 communicate over a plurality of separate physical transmission paths. As shown in FIG. 23, four transmission paths X1 through X4 are defined for communicating between the two nodes. Each node includes a packet transmitter 2302 that operates in accordance with a transmit table 2308 as described above. (The packet transmitter could also operate without using the IP-hopping features described above, but the following description assumes that some form of hopping is employed in conjunction with the path selection mechanism.). The computer node also includes a packet receiver 2303 that operates in accordance with a receive table 2309, including a moving window W that moves as valid packets are received. Invalid packets having source and destination addresses that do not fall within window W are rejected.

As each packet is readied for transmission, source and destination IP addresses (or other discriminator values) are selected from transmit table 2308 according to any of the various algorithms described above, and packets containing these source/destination address pairs, which correspond to the node to which the four transmission paths are linked, are generated to a transmission path switch 2307. Switch 2307, which can comprise a software function, selects from one of the available transmission paths according to a weight distribution table 2306. For

Petitioner Apple Inc. - Exhibit 1026, p. 57

example, if the weight for path X1 is 0.2, then every fifth packet will be transmitted on path X1. A similar regime holds true for the other paths as shown. Initially, each link's weight value can be set such that it is proportional to its bandwidth, which will be referred to as its "steady-state" value.

Packet receiver 2303 generates an output to a link quality measurement function 2304 that operates as described above to determine the quality of each transmission path. (The input to packet receiver 2303 for receiving incoming packets is omitted for clarity). Link quality measurement function 2304 compares the link quality to a threshold for each transmission link and, if necessary, generates an output to weight adjustment function 2305. If a weight adjustment is required, then the weights in table 2306 are adjusted accordingly, preferably according to a gradual (e.g., linearly or exponentially declining) function. In one embodiment, the weight values for all available paths are initially set to the same value, and only when paths degrade in quality are the weights changed to reflect differences.

Link quality measurement function 2304 can be made to operate as part of a synchronizer function as described above. That is, if resynchronization occurs and the receiver detects that synchronization has been lost (e.g., resulting in the synchronization window W being advanced out of sequence), that fact can be used to drive link quality measurement function 2304. According to one embodiment, load balancing is performed using information garnered during the normal synchronization, augmented slightly to communicate link health from the receiver to the transmitter. The receiver maintains a count, MESS_R(W), of the messages received in synchronization window W. When it receives a synchronization request (SYNC_REQ) corresponding to the end of window W, the receiver includes counter MESS_R in the resulting synchronization acknowledgement (SYNC_ACK) sent back to the transmitter. This allows the transmitter to compare messages sent to messages received in order to asses the health of the link.

If synchronization is completely lost, weight adjustment function 2305 decreases the weight value on the affected path to zero. When synchronization is regained, the weight value for the affected path is gradually increased to its original value. Alternatively, link quality can be measured by evaluating the length of time required for the receiver to acknowledge a synchronization request. In one embodiment, separate transmit and receive tables are used for each transmission path.

Petitioner Apple Inc. - Exhibit 1026, p. 58

When the transmitter receives a SYNC_ACK, the MESS_R is compared with the number of messages transmitted in a window (MESS_T). When the transmitter receives a SYNC_ACK, the traffic probabilities will be examined and adjusted if necessary. MESS_R is compared with the number of messages transmitted in a window (MESS_T). There are two possibilities:

1. If MESS_R is less than a threshold value, THRESH, then the link will be deemed to be unhealthy. If the transmitter was turned off, the transmitter is turned on and the weight P for that link will be set to a minimum value MIN. This will keep a trickle of traffic on the link for monitoring purposes until it recovers. If the transmitter was turned on, the weight P for that link will be set to:

$$P' = \alpha \times MIN + (1 - \alpha) \times P \quad (1)$$

Equation 1 will exponentially damp the traffic weight value to MIN during sustained periods of degraded service.

2. If MESS_R for a link is greater than or equal to THRESH, the link will be deemed healthy. If the weight P for that link is greater than or equal to the steady state value S for that link, then P is left unaltered. If the weight P for that link is less than THRESH then P will be set to:

$$P' = \beta \times S + (1 - \beta) \times P \quad (2)$$

where β is a parameter such that $0 <= \beta <= 1$ that determines the damping rate of P.

Equation 2 will increase the traffic weight to S during sustained periods of acceptable service in a damped exponential fashion.

A detailed example will now be provided with reference to FIG. 24. As shown in FIG. 24, a first computer 2401 communicates with a second computer 2402 through two routers 2403 and 2404. Each router is coupled to the other router through three transmission links. As described above, these may be physically diverse links or logical links (including virtual private networks).

Suppose that a first link L1 can sustain a transmission bandwidth of 100 Mb/s and has a window size of 32; link L2 can sustain 75 Mb/s and has a window size of 24; and link L3 can sustain 25 Mb/s and has a window size of 8. The combined links can thus sustain 200Mb/s. The steady state traffic weights are 0.5 for link L1; 0.375 for link L2, and 0.125 for link L3. MIN=1Mb/s, THRESH =0.8 MESS_T for each link, α=.75 and β=.5. These traffic weights will

Petitioner Apple Inc. - Exhibit 1026, p. 59

remain stable until a link stops for synchronization or reports a number of packets received less than its THRESH. Consider the following sequence of events:

1. Link L1 receives a SYNC_ACK containing a MESS_R of 24, indicating that only 75% of the MESS_T (32) messages transmitted in the last window were successfully received. Link 1 would be below THRESH (0.8). Consequently, link L1's traffic weight value would be reduced to 0.12825, while link L2's traffic weight value would be increased to 0.65812 and link L3's traffic weight value would be increased to 0.217938.

2. Link L2 and L3 remained healthy and link L1 stopped to synchronize. Then link L1's traffic weight value would be set to 0, link L2's traffic weight value would be set to 0.75, and link L33's traffic weight value would be set to 0.25.

3. Link L1 finally received a SYNC_ACK containing a MESS_R of 0 indicating that none of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be below THRESH. Link L1's traffic weight value would be increased to .005, link L2's traffic weight value would be decreased to 0.74625, and link L3's traffic weight value would be decreased to 0.24875.

4. Link L1 received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be above THRESH. Link L1's traffic weight value would be increased to 0.2525, while link L2's traffic weight value would be decreased to 0.560625 and link L3's traffic weight value would be decreased to .186875.

5. Link L1 received a SYNC_ACK containing a MESS_R of 32 indicating that 100% of the MESS_T (32) messages transmitted in the last window were successfully received. Link L1 would be above THRESH. Link L1's traffic weight value would be increased to 0.37625; link L2's traffic weight value would be decreased to 0.4678125, and link L3's traffic weight value would be decreased to 0.1559375.

6. Link L1 remains healthy and the traffic probabilities approach their steady state traffic probabilities.

B. Use of a DNS Proxy to Transparently Create Virtual Private Networks

A second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.

Petitioner Apple Inc. - Exhibit 1026, p. 60

Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser and then used by the browser to contact the destination web site.

This conventional scheme is shown in FIG. 25. A user's computer 2501 includes a client application 2504 (for example, a web browser) and an IP protocol stack 2505. When the user enters the name of a destination host, a request DNS REQ is made (through IP protocol stack 2505) to a DNS 2502 to look up the IP address associated with the name. The DNS returns the IP address DNS RESP to client application 2504, which is then able to use the IP address to communicate with the host 2503 through separate transactions such as PAGE REQ and PAGE RESP.

In the conventional architecture shown in FIG. 25, nefarious listeners on the Internet could intercept the DNS REQ and DNS RESP packets and thus learn what IP addresses the user was contacting. For example, if a user wanted to set up a secure communication path with a web site having the name "Target.com," when the user's browser contacted a DNS to find the IP address for that web site, the true IP address of that web site would be revealed over the Internet as part of the DNS inquiry. This would hamper anonymous communications on the Internet.

One conventional scheme that provides secure virtual private networks over the Internet provides the DNS server with the public keys of the machines that the DNS server has the addresses for. This allows hosts to retrieve automatically the public keys of a host that the host is to communicate with so that the host can set up a VPN without having the user enter the public key of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project(RFC 2535).

The conventional scheme suffers from certain drawbacks. For example, any user can perform a DNS request. Moreover, DNS requests resolve to the same value for all users.

According to certain aspects of the invention, a specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user. The VPN is preferably implemented using the IP address "hopping" features of the basic

Petitioner Apple Inc. - Exhibit 1026, p. 61

invention described above, such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted. For DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently "passes through" the request to provide a normal look-up function and return the IP address of the target web server, provided that the requesting host has permissions to resolve unsecured sites. Different users who make an identical DNS request could be provided with different results.

FIG. 26 shows a system employing various principles summarized above. A user's computer 2601 includes a conventional client (e.g., a web browser) 2605 and an IP protocol stack 2606 that preferably operates in accordance with an IP hopping function 2607 as outlined above. A modified DNS server 2602 includes a conventional DNS server function 2609 and a DNS proxy 2610. A gatekeeper server 2603 is interposed between the modified DNS server and a secure target site 2704. An "unsecure" target site 2611 is also accessible via conventional IP protocols.

According to one embodiment, DNS proxy 2610 intercepts all DNS lookup functions from client 2605 and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy 2610 determines whether the user has sufficient security privileges to access the site. If so, DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604. In one embodiment, gatekeeper 2603 creates "hopblocks" to be used by computer 2601 and secure target site 2604 for secure communication. Then, gatekeeper 2603 communicates these to user computer 2601. Thereafter, DNS proxy 2610 returns to user computer 2601 the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) 2604, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

Had the user requested lookup of a non-secure web site such as site 2611, DNS proxy would merely pass through to conventional DNS server 2609 the look-up request, which would be handled in a conventional manner, returning the IP address of non-secure web site 2611. If the user had requested lookup of a secure web site but lacked credentials to create such a connection, DNS proxy 2610 would return a "host unknown" error to the user. In this manner,

Petitioner Apple Inc. - Exhibit 1026, p. 62

different users requesting access to the same DNS name could be provided with different look-up results.

Gatekeeper 2603 can be implemented on a separate computer (as shown in FIG. 26) or as a function within modified DNS server 2602. In general, it is anticipated that gatekeeper 2703 facilitates the allocation and exchange of information needed to communicate securely, such as using "hopped" IP addresses. Secure hosts such as site 2604 are assumed to be equipped with a secure communication function such as an IP hopping function 2608.

It will be appreciated that the functions of DNS proxy 2610 and DNS server 2609 can be combined into a single server for convenience. Moreover, although element 2602 is shown as combining the functions of two servers, the two servers can be made to operate independently.

FIG. 27 shows steps that can be executed by DNS proxy server 2610 to handle requests for DNS look-up for secure hosts. In step 2701, a DNS look-up request is received for a target host. In step 2702, a check is made to determine whether access to a secure host was requested. If not, then in step 2703 the DNS request is passed to conventional DNS server 2609, which looks up the IP address of the target site and returns it to the user's application for further processing.

In step 2702, if access to a secure host was requested, then in step 2704 a further check is made to determine whether the user is authorized to connect to the secure host. Such a check can be made with reference to an internally stored list of authorized IP addresses, or can be made by communicating with gatekeeper 2603 (e.g., over an "administrative" VPN that is secure). It will be appreciated that different levels of security can also be provided for different categories of hosts. For example, some sites may be designated as having a certain security level, and the security level of the user requesting access must match that security level. The user's security level can also be determined by transmitting a request message back to the user's computer requiring that it prove that it has sufficient privileges.

If the user is not authorized to access the secure site, then a "host unknown" message is returned (step 2705). If the user has sufficient security privileges, then in step 2706 a secure VPN is established between the user's computer and the secure target site. As described above, this is preferably done by allocating a hopping regime that will be carried out between the user's computer and the secure target site, and is preferably performed transparently to the user (i.e., the user need not be involved in creating the secure link). As described in various embodiments of

Petitioner Apple Inc. - Exhibit 1026, p. 63

this application, any of various fields can be "hopped" (e.g., IP source/destination addresses; a field in the header; etc.) in order to communicate securely.

Some or all of the security functions can be embedded in gatekeeper 2603, such that it handles all requests to connect to secure sites. In this embodiment, DNS proxy 2610 communicates with gatekeeper 2603 to determine (preferably over a secure administrative VPN) whether the user has access to a particular web site. Various scenarios for implementing these features are described by way of example below:

Scenario #1: Client has permission to access target computer, and gatekeeper has a rule to make a VPN for the client. In this scenario, the client's DNS request would be received by the DNS proxy server 2610, which would forward the request to gatekeeper 2603. The gatekeeper would establish a VPN between the client and the requested target. The gatekeeper would provide the address of the destination to the DNS proxy, which would then return the resolved name as a result. The resolved address can be transmitted back to the client in a secure administrative VPN.

Scenario #2: Client does not have permission to access target computer. In this scenario, the client's DNS request would be received by the DNS proxy server 2610, which would forward the request to gatekeeper 2603. The gatekeeper would reject the request, informing DNS proxy server 2610 that it was unable to find the target computer. The DNS proxy 2610 would then return a "host unknown" error message to the client.

Scenario #3: Client has permission to connect using a normal non-VPN link, and the gatekeeper does not have a rule to set up a VPN for the client to the target site. In this scenario, the client's DNS request is received by DNS proxy server 2610, which would check its rules and determine that no VPN is needed. Gatekeeper 2603 would then inform the DNS proxy server to forward the request to conventional DNS server 2609, which would resolve the request and return the result to the DNS proxy server and then back to the client.

Scenario #4: Client does not have permission to establish a normal/non-VPN link, and the gatekeeper does not have a rule to make a VPN for the client to the target site. In this scenario, the DNS proxy server would receive the client's DNS request and forward it to gatekeeper 2603. Gatekeeper 2603 would determine that no special VPN was needed, but that the client is not authorized to communicate with non-VPN members. The gatekeeper would reject the request, causing DNS proxy server 2610 to return an error message to the client.

Petitioner Apple Inc. - Exhibit 1026, p. 64

C. Large Link to Small Link Bandwidth Management

One feature of the basic architecture is the ability to prevent so-called "denial of service" attacks that can occur if a computer hacker floods a known Internet node with packets, thus preventing the node from communicating with other nodes. Because IP addresses or other fields are "hopped" and packets arriving with invalid addresses are quickly discarded, Internet nodes are protected against flooding targeted at a single IP address.

In a system in which a computer is coupled through a link having a limited bandwidth (e.g., an edge router) to a node that can support a much higher-bandwidth link (e.g., an Internet Service Provider), a potential weakness could be exploited by a determined hacker. Referring to FIG. 28, suppose that a first host computer 2801 is communicating with a second host computer 2804 using the IP address hopping principles described above. The first host computer is coupled through an edge router 2802 to an Internet Service Provider (ISP) 2803 through a low bandwidth link (LOW BW), and is in turn coupled to second host computer 2804 through parts of the Internet through a high bandwidth link (HIGH BW). In this architecture, the ISP is able to support a high bandwidth to the internet, but a much lower bandwidth to the edge router 2802.

Suppose that a computer hacker is able to transmit a large quantity of dummy packets addressed to first host computer 2801 across high bandwidth link HIGH BW. Normally, host computer 2801 would be able to quickly reject the packets since they would not fall within the acceptance window permitted by the IP address hopping scheme. However, because the packets must travel across low bandwidth link LOW BW, the packets overwhelm the lower bandwidth link before they are received by host computer 2801. Consequently, the link to host computer 2801 is effectively flooded before the packets can be discarded.

According to one inventive improvement, a "link guard" function 2805 is inserted into the high-bandwidth node (e.g., ISP 2803) that quickly discards packets destined for a low-bandwidth target node if they are not valid packets. Each packet destined for a low-bandwidth node is cryptographically authenticated to determine whether it belongs to a VPN. If it is not a valid VPN packet, the packet is discarded at the high-bandwidth node. If the packet is authenticated as belonging to a VPN, the packet is passed with high preference. If the packet is a valid non-VPN packet, it is passed with a lower quality of service (e.g., lower priority).

In one embodiment, the ISP distinguishes between VPN and non-VPN packets using the protocol of the packet. In the case of IPSEC [rfc 2401], the packets have IP protocols 420 and

Petitioner Apple Inc. - Exhibit 1026, p. 65

421. In the case of the TARP VPN, the packets will have an IP protocol that is not yet defined. The ISP's link guard, 2805, maintains a table of valid VPNs which it uses to validate whether VPN packets are cryptographically valid. According to one embodiment, packets that do not fall within any hop windows used by nodes on the low-bandwidth link are rejected, or are sent with a lower quality of service. One approach for doing this is to provide a copy of the IP hopping tables used by the low-bandwidth nodes to the high-bandwidth node, such that both the high-bandwidth and low-bandwidth nodes track hopped packets (e.g., the high-bandwidth node moves its hopping window as valid packets are received). In such a scenario, the high-bandwidth node discards packets that do not fall within the hopping window before they are transmitted over the low-bandwidth link. Thus, for example, ISP 2903 maintains a copy 2910 of the receive table used by host computer 2901. Incoming packets that do not fall within this receive table are discarded. According to a different embodiment, link guard 2805 validates each VPN packet using a keyed hashed message authentication code (HMAC) [rfc 2104].

According to another embodiment, separate VPNs (using, for example, hopblocks) can be established for communicating between the low-bandwidth node and the high-bandwidth node (i.e., packets arriving at the high-bandwidth node are converted into different packets before being transmitted to the low-bandwidth node).

As shown in FIG. 29, for example, suppose that a first host computer 2900 is communicating with a second host computer 2902 over the Internet, and the path includes a high bandwidth link HIGH BW to an ISP 2901 and a low bandwidth link LOW BW through an edge router 2904. In accordance with the basic architecture described above, first host computer 2900 and second host computer 2902 would exchange hopblocks (or a hopblock algorithm) and would be able to create matching transmit and receive tables 2905, 2906, 2912 and 2913. Then in accordance with the basic architecture, the two computers would transmit packets having seemingly random IP source and destination addresses, and each would move a corresponding hopping window in its receive table as valid packets were received.

Suppose that a nefarious computer hacker 2903 was able to deduce that packets having a certain range of IP addresses (e.g., addresses 100 to 200 for the sake of simplicity) are being transmitted to ISP 2901, and that these packets are being forwarded over a low-bandwidth link. Hacker computer 2903 could thus "flood" packets having addresses falling into the range 100 to 200, expecting that they would be forwarded along low bandwidth link LOW BW, thus causing

Petitioner Apple Inc. - Exhibit 1026, p. 66

the low bandwidth link to become overwhelmed. The fast packet reject mechanism in first host computer 3000 would be of little use in rejecting these packets, since the low bandwidth link was effectively jammed before the packets could be rejected. In accordance with one aspect of the improvement, however, VPN link guard 2911 would prevent the attack from impacting the performance of VPN traffic because the packets would either be rejected as invalid VPN packets or given a lower quality of service than VPN traffic over the lower bandwidth link. A denial-of-service flood attack could, however, still disrupt non-VPN traffic.

According to one embodiment of the improvement, ISP 2901 maintains a separate VPN with first host computer 2900, and thus translates packets arriving at the ISP into packets having a different IP header before they are transmitted to host computer 2900. The cryptographic keys used to authenticate VPN packets at the link guard 2911 and the cryptographic keys used to encrypt and decrypt the VPN packets at host 2902 and host 2901 can be different, so that link guard 2911 does not have access to the private host data; it only has the capability to authenticate those packets.

According to yet a third embodiment, the low-bandwidth node can transmit a special message to the high-bandwidth node instructing it to shut down all transmissions on a particular IP address, such that only hopped packets will pass through to the low-bandwidth node. This embodiment would prevent a hacker from flooding packets using a single IP address. According to yet a fourth embodiment, the high-bandwidth node can be configured to discard packets transmitted to the low-bandwidth node if the transmission rate exceeds a certain predetermined threshold for any given IP address; this would allow hopped packets to go through. In this respect, link guard 2911 can be used to detect that the rate of packets on a given IP address are exceeding a threshold rate; further packets addressed to that same IP address would be dropped or transmitted at a lower priority (e.g., delayed).

D. Traffic Limiter

In a system in which multiple nodes are communicating using "hopping" technology, a treasonous insider could internally flood the system with packets. In order to prevent this possibility, one inventive improvement involves setting up "contracts" between nodes in the system, such that a receiver can impose a bandwidth limitation on each packet sender. One technique for doing this is to delay acceptance of a checkpoint synchronization request from a sender until a certain time period (e.g., one minute) has elapsed. Each receiver can effectively

Petitioner Apple Inc. - Exhibit 1026, p. 67

control the rate at which its hopping window moves by delaying "SYNC ACK" responses to "SYNC_REQ" messages.

A simple modification to the checkpoint synchronizer will serve to protect a receiver from accidental or deliberate overload from an internally treasonous client. This modification is based on the observation that a receiver will not update its tables until a SYNC_REQ is received on hopped address CKPT_N. It is a simple matter of deferring the generation of a new CKPT_N until an appropriate interval after previous checkpoints.

Suppose a receiver wished to restrict reception from a transmitter to 100 packets a second, and that checkpoint synchronization messages were triggered every 50 packets. A compliant transmitter would not issue new SYNC_REQ messages more often than every 0.5 seconds. The receiver could delay a non-compliant transmitter from synchronizing by delaying the issuance of CKPT_N for 0.5 second after the last SYNC_REQ was accepted.

In general, if M receivers need to restrict N transmitters issuing new SYNC_REQ messages after every W messages to sending R messages a second in aggregate, each receiver could defer issuing a new CKPT_N until MxNxW/R seconds have elapsed since the last SYNC_REQ has been received and accepted. If the transmitter exceeds this rate between a pair of checkpoints, it will issue the new checkpoint before the receiver is ready to receive it, and the SYNC_REQ will be discarded by the receiver. After this, the transmitter will re-issue the SYNC_REQ every T1 seconds until it receives a SYNC_ACK. The receiver will eventually update CKPT_N and the SYNC_REQ will be acknowledged. If the transmission rate greatly exceeds the allowed rate, the transmitter will stop until it is compliant. If the transmitter exceeds the allowed rate by a little, it will eventually stop after several rounds of delayed synchronization until it is in compliance. Hacking the transmitter's code to not shut off only permits the transmitter to lose the acceptance window. In this case it can recover the window and proceed only after it is compliant again.

Two practical issues should be considered when implementing the above scheme:

1. The receiver rate should be slightly higher than the permitted rate in order to allow for statistical fluctuations in traffic arrival times and non-uniform load balancing.

2. Since a transmitter will rightfully continue to transmit for a period after a SYNC_REQ is transmitted, the algorithm above can artificially reduce the transmitter's bandwidth. If events prevent a compliant transmitter from synchronizing for a period (e.g. the network dropping a

Petitioner Apple Inc. - Exhibit 1026, p. 68

SYNC_REQ or a SYNC_ACK) a SYNC_REQ will be accepted later than expected. After this, the transmitter will transmit fewer than expected messages before encountering the next checkpoint. The new checkpoint will not have been activated and the transmitter will have to retransmit the SYNC_REQ. This will appear to the receiver as if the transmitter is not compliant. Therefore, the next checkpoint will be accepted late from the transmitter's perspective. This has the effect of reducing the transmitter's allowed packet rate until the transmitter transmits at a packet rate below the agreed upon rate for a period of time.

To guard against this, the receiver should keep track of the times that the last C SYNC_REQs were received and accepted and use the minimum of MxNxW/R seconds after the last SYNC_REQ has been received and accepted, 2xMxNxW/R seconds after next to the last SYNC_REQ has been received and accepted, CxMxNxW/R seconds after $(C-1)^{th}$ to the last SYNC_REQ has been received, as the time to activate CKPT_N. This prevents the receiver from inappropriately limiting the transmitter's packet rate if at least one out of the last C SYNC_REQs was processed on the first attempt.

FIG. 30 shows a system employing the above-described principles. In FIG. 30, two computers 3000 and 3001 are assumed to be communicating over a network N in accordance with the "hopping" principles described above (e.g., hopped IP addresses, discriminator values, etc.). For the sake of simplicity, computer 3000 will be referred to as the receiving computer and computer 3001 will be referred to as the transmitting computer, although full duplex operation is of course contemplated. Moreover, although only a single transmitter is shown, multiple transmitters can transmit to receiver 3000.

As described above, receiving computer 3000 maintains a receive table 3002 including a window W that defines valid IP address pairs that will be accepted when appearing in incoming data packets. Transmitting computer 3001 maintains a transmit table 3003 from which the next IP address pairs will be selected when transmitting a packet to receiving computer 3000. (For the sake of illustration, window W is also illustrated with reference to transmit table 3003). As transmitting computer moves through its table, it will eventually generate a SYNC_REQ message as illustrated in function 3010. This is a request to receiver 3000 to synchronize the receive table 3002, from which transmitter 3001 expects a response in the form of a CKPT_N (included as part of a SYNC_ACK message). If transmitting computer 3001 transmits more messages than its allotment, it will prematurely generate the SYNC_REQ message. (If it has

Petitioner Apple Inc. - Exhibit 1026, p. 69

been altered to remove the SYNC_REQ message generation altogether, it will fall out of synchronization since receiver 3000 will quickly reject packets that fall outside of window W, and the extra packets generated by transmitter 3001 will be discarded).

In accordance with the improvements described above, receiving computer 3000 performs certain steps when a SYNC_REQ message is received, as illustrated in FIG. 30. In step 3004, receiving computer 3000 receives the SYNC_REQ message. In step 3005, a check is made to determine whether the request is a duplicate. If so, it is discarded in step 3006. In step 3007, a check is made to determine whether the SYNC_REQ received from transmitter 3001 was received at a rate that exceeds the allowable rate R (i.e., the period between the time of the last SYNC_REQ message). The value R can be a constant, or it can be made to fluctuate as desired. If the rate exceeds R, then in step 3008 the next activation of the next CKPT_N hopping table entry is delayed by W/R seconds after the last SYNC_REQ has been accepted.

Otherwise, if the rate has not been exceeded, then in step 3109 the next CKPT_N value is calculated and inserted into the receiver's hopping table prior to the next SYNC_REQ from thetransmitter 3101. Transmitter 3101 then processes the SYNC_REQ in the normal manner.

E. Signaling Synchronizer

In a system in which a large number of users communicate with a central node using secure hopping technology, a large amount of memory must be set aside for hopping tables and their supporting data structures. For example, if one million subscribers to a web site occasionally communicate with the web site, the site must maintain one million hopping tables, thus using up valuable computer resources, even though only a small percentage of the users may actually be using the system at any one time. A desirable solution would be a system that permits a certain maximum number of simultaneous links to be maintained, but which would "recognize" millions of registered users at any one time. In other words, out of a population of a million registered users, a few thousand at a time could simultaneously communicate with a central server, without requiring that the server maintain one million hopping tables of appreciable size.

One solution is to partition the central node into two nodes: a signaling server that performs session initiation for user log-on and log-off (and requires only minimally sized tables), and a transport server that contains larger hopping tables for the users. The signaling server listens for the millions of known users and performs a fast-packet reject of other (bogus) packets.

Petitioner Apple Inc. - Exhibit 1026, p. 70

When a packet is received from a known user, the signaling server activates a virtual private link (VPL) between the user and the transport server, where hopping tables are allocated and maintained. When the user logs onto the signaling server, the user's computer is provided with hop tables for communicating with the transport server, thus activating the VPL. The VPLs can be torn down when they become inactive for a time period, or they can be torn down upon user log-out. Communication with the signaling server to allow user log-on and log-off can be accomplished using a specialized version of the checkpoint scheme described above.

FIG. 31 shows a system employing certain of the above-described principles. In FIG. 31, a signaling server 3101 and a transport server 3102 communicate over a link. Signaling server 3101 contains a large number of small tables 3106 and 3107 that contain enough information to authenticate a communication request with one or more clients 3103 and 3104. As described in more detail below, these small tables may advantageously be constructed as a special case of the synchronizing checkpoint tables described previously. Transport server 3102, which is preferably a separate computer in communication with signaling server 3101, contains a smaller number of larger hopping tables 3108, 3109, and 3110 that can be allocated to create a VPN with one of the client computers.

According to one embodiment, a client that has previously registered with the system (e.g., via a system administration function, a user registration procedure, or some other method) transmits a request for information from a computer (e.g., a web site). In one variation, the request is made using a "hopped" packet, such that signaling server 3101 will quickly reject invalid packets from unauthorized computers such as hacker computer 3105. An "administrative" VPN can be established between all of the clients and the signaling server in order to ensure that a hacker cannot flood signaling server 3101 with bogus packets. Details of this scheme are provided below.

Signaling server 3101 receives the request 3111 and uses it to determine that client 3103 is a validly registered user. Next, signaling server 3101 issues a request to transport server 3102 to allocate a hopping table (or hopping algorithm or other regime) for the purpose of creating a VPN with client 3103. The allocated hopping parameters are returned to signaling server 3101 (path 3113), which then supplies the hopping parameters to client 3103 via path 3114, preferably in encrypted form.

Petitioner Apple Inc. - Exhibit 1026, p. 71

Thereafter, client 3103 communicates with transport server 3102 using the normal hopping techniques described above. It will be appreciated that although signaling server 3101 and transport server 3102 are illustrated as being two separate computers, they could of course be combined into a single computer and their functions performed on the single computer. Alternatively, it is possible to partition the functions shown in FIG. 31 differently from as shown without departing from the inventive principles.

One advantage of the above-described architecture is that signaling server 3101 need only maintain a small amount of information on a large number of potential users, yet it retains the capability of quickly rejecting packets from unauthorized users such as hacker computer 3105. Larger data tables needed to perform the hopping and synchronization functions are instead maintained in a transport server 3102, and a smaller number of these tables are needed since they are only allocated for "active" links. After a VPN has become inactive for a certain time period (e.g., one hour), the VPN can be automatically torn down by transport server 3102 or signaling server 3101.

A more detailed description will now be provided regarding how a special case of the checkpoint synchronization feature can be used to implement the signaling scheme described above.

The signaling synchronizer may be required to support many (millions) of standing, low bandwidth connections. It therefore should minimize per-VPL memory usage while providing the security offered by hopping technology. In order to reduce memory usage in the signaling server, the data hopping tables can be completely eliminated and data can be carried as part of the SYNC_REQ message. The table used by the server side (receiver) and client side (transmitter) is shown schematically as element 3106 in FIG. 31.

The meaning and behaviors of CKPT_N, CKPT_O and CKPT_R remain the same from the previous description, except that CKPT_N can receive a combined data and SYNC_REQ message or a SYNC_REQ message without the data.

The protocol is a straightforward extension of the earlier synchronizer. Assume that a client transmitter is on and the tables are synchronized. The initial tables can be generated "out of band." For example, a client can log into a web server to establish an account over the Internet. The client will receive keys etc encrypted over the Internet. Meanwhile, the server will set up the signaling VPN on the signaling server.

Petitioner Apple Inc. - Exhibit 1026, p. 72

Assuming that a client application wishes to send a packet to the server on the client's standing signaling VPL:

1. The client sends the message marked as a data message on the inner header using the transmitter's CKPT_N address. It turns the transmitter off and starts a timer T1 noting CKPT_O. Messages can be one of three types: DATA, SYNC_REQ and SYNC_ACK. In the normal algorithm, some potential problems can be prevented by identifying each message type as part of the encrypted inner header field. In this algorithm, it is important to distinguish a data packet and a SYNC_REQ in the signaling synchronizer since the data and the SYNC_REQ come in on the same address.

2. When the server receives a data message on its CKPT_N, it verifies the message and passes it up the stack. The message can be verified by checking message type and and other information (i.e., user credentials) contained in the inner header It replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

3. When the client side receiver receives a SYNC_ACK on its CKPT_R with a payload matching its transmitter side CKPT_O and the transmitter is off, the transmitter is turned on and the receiver side CKPT_R is updated. If the SYNC_ACK's payload does not match the transmitter side CKPT_O or the transmitter is on, the SYNC_ACK is simply discarded.

4. T1 expires: If the transmitter is off and the client's transmitter side CKPT_O matches the CKPT_O associated with the timer, it starts timer T1 noting CKPT_O again, and a SYNC_REQ is sent using the transmitter's CKPT_O address. Otherwise, no action is taken.

5. When the server receives a SYNC_REQ on its CKPT_N, it replaces its CKPT_O with CKPT_N and generates the next CKPT_N. It updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

6. When the server receives a SYNC_REQ on its CKPT_O, it updates its transmitter side CKPT_R to correspond to the client's receiver side CKPT_R and transmits a SYNC_ACK containing CKPT_O in its payload.

FIG. 32 shows message flows to highlight the protocol. Reading from top to bottom, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is

Petitioner Apple Inc. - Exhibit 1026, p. 73

turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is successfully received and a passed up the stack. It also synchronizes the receiver i.e., the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates a new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned on and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

Next, the client sends data to the server using its transmitter side CKPT_N. The client side transmitter is turned off and a retry timer is turned off. The transmitter will not transmit messages as long as the transmitter is turned off. The client side transmitter then loads CKPT_N into CKPT_O and updates CKPT_N. This message is lost. The client side timer expires and as a result a SYNC_REQ is transmitted on the client side transmitter's CKPT_O (this will keep happening until the SYNC_ACK has been received at the client). The SYNC_REQ is successfully received at the server. It synchronizes the receiver i.e., the server loads CKPT_N into CKPT_O and generates a new CKPT_N, it generates an new CKPT_R in the server side transmitter and transmits a SYNC_ACK containing the server side receiver's CKPT_O the server. The SYNC_ACK is successfully received at the client. The client side receiver's CKPT_R is updated, the transmitter is turned off and the retry timer is killed. The client side transmitter is ready to transmit a new data message.

There are numerous other scenarios that follow this flow. For example, the SYNC_ACK could be lost. The transmitter would continue to re-send the SYNC_REQ until the receiver synchronizes and responds.

The above-described procedures allow a client to be authenticated at signaling server 3201 while maintaining the ability of signaling server 3201 to quickly reject invalid packets, such as might be generated by hacker computer 3205. In various embodiments, the signaling synchronizer is really a derivative of the synchronizer. It provides the same protection as the hopping protocol, and it does so for a large number of low bandwidth connections.

F. One-Click Secure On-line Communications and Secure Domain Name Service

The present invention provides a technique for establishing a secure communication link between a first computer and a second computer over a computer network. Preferably, a user

Petitioner Apple Inc. - Exhibit 1026, p. 74

enables a secure communication link using a single click of a mouse, or a corresponding minimal input from another input device, such as a keystroke entered on a keyboard or a click entered through a trackball. Alternatively, the secure link is automatically established as a default setting at boot-up of the computer (i.e., no click). FIG. 33 shows a system block diagram 3300 of a computer network in which the one-click secure communication method of the present invention is suitable. In FIG. 33, a computer terminal or client computer 3301, such as a personal computer (PC), is connected to a computer network 3302, such as the Internet, through an ISP 3303. Alternatively, computer 3301 can be connected to computer network 3302 through an edge router. Computer 3301 includes an input device, such as a keyboard and/or mouse, and a display device, such as a monitor. Computer 3301 can communicate conventionally with another computer 3304 connected to computer network 3302 over a communication link 3305 using a browser 3306 that is installed and operates on computer 3301 in a well-known manner.

Computer 3304 can be, for example, a server computer that is used for conducting e-commerce. In the situation when computer network 3302 is the Internet, computer 3304 typically will have a standard top-level domain name such as .com, .net, .org, .edu, .mil or .gov.

FIG. 34 shows a flow diagram 3400 for installing and establishing a "one-click" secure communication link over a computer network according to the present invention. At step 3401, computer 3301 is connected to server computer 3304 over a non-VPN communication link 3305. Web browser 3306 displays a web page associated with server 3304 in a well-known manner. According to one variation of the invention, the display of computer 3301 contains a hyperlink, or an icon representing a hyperlink, for selecting a virtual private network (VPN) communication link ("go secure" hyperlink) through computer network 3302 between terminal 3301 and server 3304. Preferably, the "go secure" hyperlink is displayed as part of the web page downloaded from server computer 3304, thereby indicating that the entity providing server 3304 also provides VPN capability.

By displaying the "go secure" hyperlink, a user at computer 3301 is informed that the current communication link between computer 3301 and server computer 3304 is a non-secure, non-VPN communication link. At step 3402, it is determined whether a user of computer 3301 has selected the "go secure" hyperlink. If not, processing resumes using a non-secure (conventional) communication method (not shown). If, at step 3402, it is determined that the user has selected the "go secure" hyperlink, flow continues to step 3403 where an object

Petitioner Apple Inc. - Exhibit 1026, p. 75

associated with the hyperlink determines whether a VPN communication software module has already been installed on computer 3301. Alternatively, a user can enter a command into computer 3301 to "go secure."

If, at step 3403, the object determines that the software module has been installed, flow continues to step 3407. If, at step 3403, the object determines that the software module has not been installed, flow continues to step 3404 where a non-VPN communication link 3307 is launched between computer 3301 and a website 3308 over computer network 3302 in a well-known manner. Website 3308 is accessible by all computer terminals connected to computer network 3302 through a non-VPN communication link. Once connected to website 3308, a software module for establishing a secure communication link over computer network 3302 can be downloaded and installed. Flow continues to step 3405 where, after computer 3301 connects to website 3308, the software module for establishing a communication link is downloaded and installed in a well-known manner on computer terminal 3301 as software module 3309. At step 3405, a user can optionally select parameters for the software module, such as enabling a secure communication link mode of communication for all communication links over computer network 3302. At step 3406, the -communication link between computer 3301 and website 3308 is then terminated in a well-known manner.

By clicking on the "go secure" hyperlink, a user at computer 3301 has enabled a secure communication mode of communication between computer 3301 and server computer 3304. According to one variation of the invention, the user is not required to do anything more than merely click the "go secure" hyperlink. The user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link. All procedures required for establishing a secure communication link between computer 3301 and server computer 3304 are performed transparently to a user at computer 3301.

At step 3407, a secure VPN communications mode of operation has been enabled and software module 3309 begins to establish a VPN communication link. In one embodiment, software module 3309 automatically replaces the top-level domain name for server 3304 within browser 3406 with a secure top-level domain name for server computer 3304. For example, if the top-level domain name for server 3304 is .com, software module 3309 replaces the .com top-level domain name with a .scom top-level domain name, where the "s" stands for secure. Alternatively, software module 3409 can replace the top-level domain name of server 3304 with

Petitioner Apple Inc. - Exhibit 1026, p. 76

any other non-standard top-level domain name.

Because the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown. According to the invention, software module 3409 contains the URL for querying a secure domain name service (SDNS) for obtaining the URL for a secure top-level domain name. In this regard, software module 3309 accesses a secure portal 3310 that interfaces a secure network 3311 to computer network 3302. Secure network 3311 includes an internal router 3312, a secure domain name service (SDNS) 3313, a VPN gatekeeper 3314 and a secure proxy 3315. The secure network can include other network services, such as e-mail 3316, a plurality of chatrooms (of which only one chatroom 3317 is shown), and a standard domain name service (STD DNS) 3318. Of course, secure network 3311 can include other resources and services that are not shown in FIG. 33.

When software module 3309 replaces the standard top-level domain name for server 3304 with the secure top-level domain name, software module 3309 sends a query to SDNS 3313 at step 3408 through secure portal 3310 preferably using an administrative VPN communication link 3319. In this configuration, secure portal 3310 can only be accessed using a VPN communication link. Preferably, such a VPN communication link can be based on a technique of inserting a source and destination IP address pair into each data packet that is selected according to a pseudo-random sequence; an IP address hopping regime that pseudorandomly changes IP addresses in packets transmitted between a client computer and a secure target computer; periodically changing at least one field in a series of data packets according to a known sequence; an Internet Protocol (IP) address in a header of each data packet that is compared to a table of valid IP addresses maintained in a table in the second computer; and/or a comparison of the IP address in the header of each data packet to a moving window of valid IP addresses, and rejecting data packets having IP addresses that do not fall within the moving window. Other types of VPNs can alternatively be used. Secure portal 3310 authenticates the query from software module 3309 based on the particular information hopping technique used for VPN communication link 3319.

SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS 3313 stores a computer network address corresponding to the secure domain name. An entity can

Petitioner Apple Inc. - Exhibit 1026, p. 77

register a secure domain name in SDNS 3313 so that a user who desires a secure communication link to the website of the entity can automatically obtain the secure computer network address for the secure website. Moreover, an entity can register several secure domain names, with each respective secure domain name representing a different priority level of access in a hierarchy of access levels to a secure website. For example, a securities trading website can provide users secure access so that a denial of service attack on the website will be ineffectual with respect to users subscribing to the secure website service. Different levels of subscription can be arranged based on, for example, an escalating fee, so that a user can select a desired level of guarantee for connecting to the secure securities trading website. When a user queries SDNS 3313 for the secure computer network address for the securities trading website, SDNS 3313 determines the particular secure computer network address based on the user's identity and the user's subscription level.

At step 3409, SDNS 3313 accesses VPN gatekeeper 3314 for establishing a VPN communication link between software module 3309 and secure server 3320. Server 3320 can only be accessed through a VPN communication link. VPN gatekeeper 3314 provisions computer 3301 and secure web server computer 3320, or a secure edge router for server computer 3320, thereby creating the VPN. Secure server computer 3320 can be a separate server computer from server computer 3304, or can be the same server computer having both non-VPN and VPN communication link capability, such as shown by server computer 3322. Returning to FIG. 34, in step 3410, SDNS 3313 returns a secure URL to software module 3309 for the .scom server address for a secure server 3320 corresponding to server 3304.

Alternatively, SDNS 3313 can be accessed through secure portal 3310 "in the clear", that is, without using an administrative VPN communication link. In this situation, secure portal 3310 preferably authenticates the query using any well-known technique, such as a cryptographic technique, before allowing the query to proceed to SDNS 3319. Because the initial communication link in this situation is not a VPN communication link, the reply to the query can be "in the clear." The querying computer can use the clear reply for establishing a VPN link to the desired domain name. Alternatively, the query to SDNS 3313 can be in the clear, and SDNS 3313 and gatekeeper 3314 can operate to establish a VPN communication link to the querying computer for sending the reply.

At step 3411, software module 3309 accesses secure server 3320 through VPN

Petitioner Apple Inc. - Exhibit 1026, p. 78

communication link 3321 based on the VPN resources allocated by VPN gatekeeper 3314. At step 3412, web browser 3306 displays a secure icon indicating that the current communication link to server 3320 is a secure VPN communication link. Further communication between computers 3301 and 3320 occurs via the VPN, e.g., using a "hopping" regime as discussed above. When VPN link 3321 is terminated at step 3413, flow continues to step 3414 where software module 3309 automatically replaces the secure top-level domain name with the corresponding non-secure top-level domain name for server 3304. Browser 3306 accesses a standard DNS 3325 for obtaining the non-secure URL for server 3304. Browser 3306 then connects to server 3304 in a well-known manner. At step 3415, browser 3306 displays the "go secure" hyperlink or icon for selecting a VPN communication link between terminal 3301 and server 3304. By again displaying the "go secure" hyperlink, a user is informed that the current communication link is a non-secure, non-VPN communication link.

When software module 3309 is being installed or when the user is off-line, the user can optionally specify that all communication links established over computer network 3302 are secure communication links. Thus, anytime that a communication link is established, the link is a VPN link. Consequently, software module 3309 transparently accesses SDNS 3313 for obtaining the URL for a selected secure website. In other words, in one embodiment, the user need not "click" on the secure option each time secure communication is to be effected.

Additionally, a user at computer 3301 can optionally select a secure communication link through proxy computer 3315. Accordingly, computer 3301 can establish a VPN communication link 3323 with secure server computer 3320 through proxy computer 3315. Alternatively, computer 3301 can establish a non-VPN communication link 3324 to a non-secure website, such as non-secure server computer 3304.

FIG. 35 shows a flow diagram 3500 for registering a secure domain name according to the present invention. At step 3501, a requester accesses website 3308 and logs into a secure domain name registry service that is available through website 3308. At step 3502, the requestor completes an online registration form for registering a secure domain name having a top-level domain name, such as .com, .net, .org, .edu, .mil or .gov. Of course, other secure top-level domain names can also be used. Preferably, the requestor must have previously registered a non-secure domain name corresponding to the equivalent secure domain name that is being

Petitioner Apple Inc. - Exhibit 1026, p. 79

requested. For example, a requestor attempting to register secure domain name "website.scom" must have previously registered the corresponding non-secure domain name "website.com".

At step 3503, the secure domain name registry service at website 3308 queries a non-secure domain name server database, such as standard DNS 3322, using, for example, a whois query, for determining ownership information relating to the non-secure domain name corresponding to the requested secure domain name. At step 3504, the secure domain name registry service at website 3308 receives a reply from standard DNS 3322 and at step 3505 determines whether there is conflicting ownership information for the corresponding non-secure domain name. If there is no conflicting ownership information, flow continues to step 3507, otherwise flow continues to step 3506 where the requestor is informed of the conflicting ownership information. Flow returns to step 3502.

When there is no conflicting ownership information at step 3505, the secure domain name registry service (website 3308) informs the requestor that there is no conflicting ownership information and prompts the requestor to verify the information entered into the online form and select an approved form of payment. After confirmation of the entered information and appropriate payment information, flow continues to step 3508 where the newly registered secure domain name sent to SDNS 3313 over communication link 3326.

If, at step 3505, the requested secure domain name does not have a corresponding equivalent non-secure domain name, the present invention informs the requestor of the situation and prompts the requestor for acquiring the corresponding equivalent non-secure domain name for an increased fee. By accepting the offer, the present invention automatically registers the corresponding equivalent non-secure domain name with standard DNS 3325 in a well-known manner. Flow then continues to step 3508.

G. Tunneling Secure Address Hopping Protocol Through Existing Protocol Using Web Proxy

The present invention also provides a technique for implementing the field hopping schemes described above in an application program on the client side of a firewall between two computer networks, and in the network stack on the server side of the firewall. The present invention uses a new secure connectionless protocol that provides good denial of service rejection capabilities by layering the new protocol on top of an existing IP protocol, such as the ICMP, UDP or TCP protocols. Thus, this aspect of the present invention does not require

Petitioner Apple Inc. - Exhibit 1026, p. 80

changes in the Internet infrastructure.

According to the invention, communications are protected by a client-side proxy application program that accepts unencrypted, unprotected communication packets from a local browser application. The client-side proxy application program tunnels the unencrypted, unprotected communication packets through a new protocol, thereby protecting the communications from a denial of service at the server side. Of course, the unencrypted, unprotected communication packets can be encrypted prior to tunneling.

The client-side proxy application program is not an operating system extension and does not involve any modifications to the operating system network stack and drivers. Consequently, the client is easier to install, remove and support in comparison to a VPN. Moreover, the client-side proxy application can be allowed through a corporate firewall using a much smaller "hole" in the firewall and is less of a security risk in comparison to allowing a protocol layer VPN through a corporate firewall.

The server-side implementation of the present invention authenticates valid field-hopped packets as valid or invalid very early in the server packet processing, similar to a standard virtual private network, for greatly minimizing the impact of a denial of service attempt in comparison to normal TCP/IP and HTTP communications, thereby protecting the server from invalid communications.

FIG. 36 shows a system block diagram of a computer network 3600 in which a virtual private connection according to the present invention can be configured to more easily traverse a firewall between two computer networks. FIG. 37 shows a flow diagram 3700 for establishing a virtual private connection that is encapsulated using an existing network protocol.

In FIG. 36 a local area network (LAN) 3601 is connected to another computer network 3602, such as the Internet, through a firewall arrangement 3603. Firewall arrangement operates in a well-known manner to interface LAN 3601 to computer network 3602 and to protect LAN 3601 from attacks initiated outside of LAN 3601.

A client computer 3604 is connected to LAN 3601 in a well-known manner. Client computer 3604 includes an operating system 3605 and a web browser 3606. Operating system 3605 provides kernel mode functions for operating client computer 3604. Browser 3606 is an application program for accessing computer network resources connected to LAN 3601 and computer network 3602 in a well-known manner. According to the present invention, a proxy

Petitioner Apple Inc. - Exhibit 1026, p. 81

application 3607 is also stored on client computer 3604 and operates at an application layer in conjunction with browser 3606. Proxy application 3607 operates at the application layer within client computer 3604 and when enabled, modifies unprotected, unencrypted message packets generated by browser 3606 by inserting data into the message packets that are used for forming a virtual private connection between client computer 3604 and a server computer connected to LAN 3601 or computer network 3602. According to the invention, a virtual private connection does not provide the same level of security to the client computer as a virtual private network. A virtual private connection can be conveniently authenticated so that, for example, a denial of service attack can be rapidly rejected, thereby providing different levels of service that can be subscribed to by a user.

Proxy application 3607 is conveniently installed and uninstalled by a user because proxy application 3607 operates at the application layer within client computer 3604. On installation, proxy application 3607 preferably configures browser 3606 to use proxy application for all web communications. That is, the payload portion of all message packets is modified with the data for forming a virtual private connection between client computer 3604 and a server computer. Preferably, the data for forming the virtual private connection contains field-hopping data, such as described above in connection with VPNs. Also, the modified message packets preferably conform to the UDP protocol. Alternatively, the modified message packets can conform to the TCP/IP protocol or the ICMP protocol. Alternatively, proxy application 3606 can be selected and enabled through, for example, an option provided by browser 3606. Additionally, proxy application 3607 can be enabled so that only the payload portion of specially designated message packets is modified with the data for forming a virtual private connection between client computer 3604 and a designated host computer. Specially designated message packets can be, for example, selected predetermined domain names.

Referring to FIG. 37, at step 3701, unprotected and unencrypted message packets are generated by browser 3606. At step 3702, proxy application 3607 modifies the payload portion of all message packets by tunneling the data for forming a virtual private connection between client computer 3604 and a destination server computer into the payload portion. At step, 3703, the modified message packets are sent from client computer 3604 to, for example, website (server computer) 3608 over computer network 3602.

Petitioner Apple Inc. - Exhibit 1026, p. 82

Website 3608 includes a VPN guard portion 3609, a server proxy portion 3610 and a web server portion 3611. VPN guard portion 3609 is embedded within the kernel layer of the operating system of website 3608 so that large bandwidth attacks on website 3608 are rapidly rejected. When client computer 3604 initiates an authenticated connection to website 3608, VPN guard portion 3609 is keyed with the hopping sequence contained in the message packets from client computer 3604, thereby performing a strong authentication of the client packet streams entering website 3608 at step 3704. VPN guard portion 3609 can be configured for providing different levels of authentication and, hence, quality of service, depending upon a subscribed level of service. That is, VPN guard portion 3609 can be configured to let all message packets through until a denial of service attack is detected, in which case VPN guard portion 3609 would allow only client packet streams conforming to a keyed hopping sequence, such as that of the present invention.

Server proxy portion 3610 also operates at the kernel layer within website 3608 and catches incoming message packets from client computer 3604 at the VPN level. At step 3705, server proxy portion 3610 authenticates the message packets at the kernel level within host computer 3604 using the destination IP address, UDP ports and discriminator fields. The authenticated message packets are then forwarded to the authenticated message packets to web server portion 3611 as normal TCP web transactions.

At step 3705, web server portion 3611 responds to message packets received from client computer 3604 in accordance with the particular nature of the message packets by generating reply message packets. For example, when a client computer requests a webpage, web server portion 3611 generates message packets corresponding to the requested webpage. At step 3706, the reply message packets pass through server proxy portion 3610, which inserts data into the payload portion of the message packets that are used for forming the virtual private connection between host computer 3608 and client computer 3604 over computer network 3602. Preferably, the data for forming the virtual private connection is contains field-hopping data, such as described above in connection with VPNs. Server proxy portion 3610 operates at the kernel layer within host computer 3608 to insert the virtual private connection data into the payload portion of the reply message packets. Preferably, the modified message packets sent by host computer 3608 to client computer 3604 conform to the UDP protocol. Alternatively, the modified message packets can conform to the TCP/IP protocol or the ICMP protocol.

Petitioner Apple Inc. - Exhibit 1026, p. 83

At step 3707, the modified packets are sent from host computer 3608 over computer network 3602 and pass through firewall 3603. Once through firewall 3603, the modified packets are directed to client computer 3604 over LAN 3601 and are received at step 3708 by proxy application 3607 at the application layer within client computer 3604. Proxy application 3607 operates to rapidly evaluate the modified message packets for determining whether the received packets should be accepted or dropped. If the virtual private connection data inserted into the received information packets conforms to expected virtual private connection data, then the received packets are accepted. Otherwise, the received packets are dropped.

While the present invention has been described in connection with the illustrated embodiments, it will be appreciated and understood that modifications may be made without departing from the true spirit and scope of the invention.

Petitioner Apple Inc. - Exhibit 1026, p. 84

CLAIMS

What is claimed is:

1. A method for accessing a secure computer network address, comprising steps of:

receiving a secure domain;

sending a query message to a secure domain service, the query message requesting a secure computer network address corresponding to the secure domain;

receiving a response message containing the secure computer network address corresponding to the secure domain; and

sending an access request message to the secure computer network address using a virtual private network communication link.

Petitioner Apple Inc. - Exhibit 1026, p. 85

ABSTRACT

A technique is disclosed for establishing a secure communication link between a first computer and a second computer over a computer network. Initially, a secure communication mode of communication is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. The secure communication link is a virtual private network communication link over the computer network in which one or more data values that vary according to a pseudo-random sequence are inserted into each data packet.

Petitioner Apple Inc. - Exhibit 1026, p. 86

Banner & Witcoff Ref. No. 000479.00112
Client Ref. No. 10006-Div. (1)

JOINT DECLARATION FOR PATENT APPLICATION

As the below named inventors, we hereby declare that:

Our residence, post office address and citizenship are as stated below next to our names;

We believe we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK, the specification of which

- ☒ is attached hereto.
- ☐ was filed on _____as Application Serial Number _____and was amended on _____ (if applicable).
- ☐ was filed under the Patent Cooperation Treaty (PCT) and accorded International Application No. _____, filed _____, and amended on _____ (if any).

We hereby state that we have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

We hereby acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Prior Foreign Application(s)

We hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Country	Application No.	Date of Filing (day month year)	Date of Issue (day month year)	Priority Claimed Under 35 U.S.C. §119

Prior United States Provisional Application(s)

We hereby claim priority benefits under Title 35, United States Code, §119(e)(1) of any U.S. provisional application listed below:

U.S. Provisional Application No.	Date of Filing (day month year)	Priority Claimed Under 35 U.S.C. §119(e)(1)
60/106,261	30 October 1998	Yes
60/137,704	7 June 1999	Yes

Prior United States Application(s)

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Petitioner Apple Inc. - Exhibit 1026, p. 87

Banner & Witcoff Ref. No. 000479.00112
Client Ref. No. 10006-Div. (1)

Application Serial No.	Date of Filing (Day, Month, Year)	Status — Patented, Pending, Abandoned
09/558,209	26 April 2000	Pending
09/504,783	15 February 2000	Patented
09/429,643	29 October 1999	Pending

Power of Attorney

And we hereby appoint, both jointly and severally, as our attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the practitioners at:

Customer Number: 22907 (WDC)

Please address all correspondence and telephone communications to the address and telephone number for this Customer Number.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature Victor Larson Date 11/6/03
Full Name of First Inventor Larson (Family Name) Victor (First Given Name) (Second Given Name)
Residence Fairfax, Virginia Citizenship USA
Post Office Address 12026 Lisa Marie Court, Fairfax, Virginia 22033

Signature Robert D. Short, III Date 10/27/03
Full Name of Second Inventor Short, III (Family Name) Robert (First Given Name) Dunham (Second Given Name)
Residence Leesburg, Virginia Citizenship USA
Post Office Address 38710 Goose Creek Lane, Leesburg, Virginia 20175

Signature Edmund Colby Monger Date 11/5/03
Full Name of Third Inventor Monger (Family Name) Edmund (First Given Name) Colby (Second Given Name)
Residence Crownsville, Maryland Citizenship USA
Post Office Address 1101 Opaca Court, Crownsville, Maryland 21032

Signature Michael Williamson Date 11/5/03
Full Name of Fourth Inventor Williamson (Family Name) Michael (First Given Name) (Second Given Name)
Residence South Riding, Virginia Citizenship USA
Post Office Address 26203 Ocala Circle, South Riding, Virginia 20152

Petitioner Apple Inc. - Exhibit 1026, p. 88

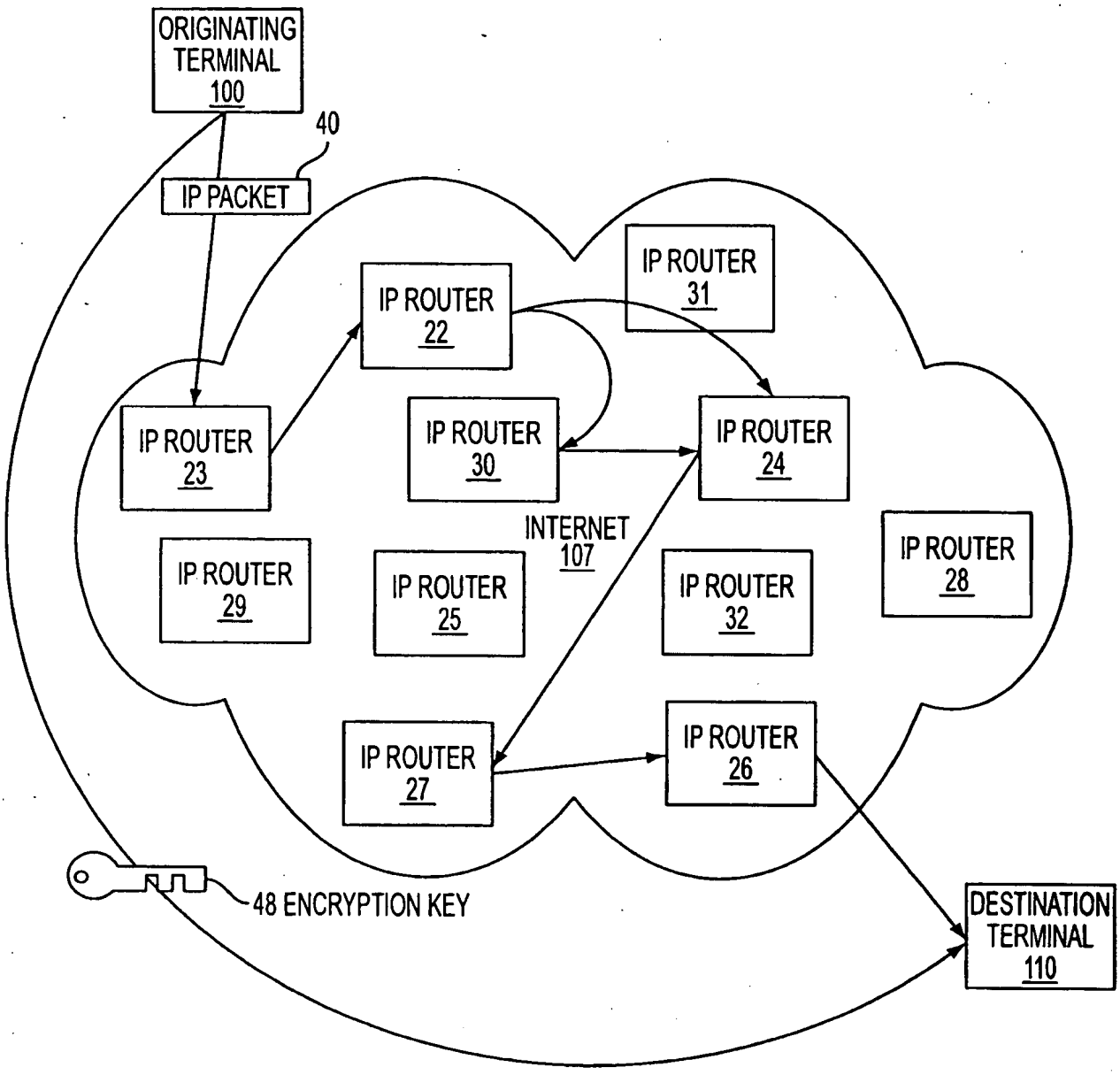

ORIGINATING TERMINAL 100
40
IP PACKET
IP ROUTER 22
IP ROUTER 31
IP ROUTER 23
IP ROUTER 30
IP ROUTER 24
INTERNET 107
IP ROUTER 29
IP ROUTER 25
IP ROUTER 32
IP ROUTER 28
IP ROUTER 27
IP ROUTER 26
48 ENCRYPTION KEY
DESTINATION TERMINAL 110

FIG. 1

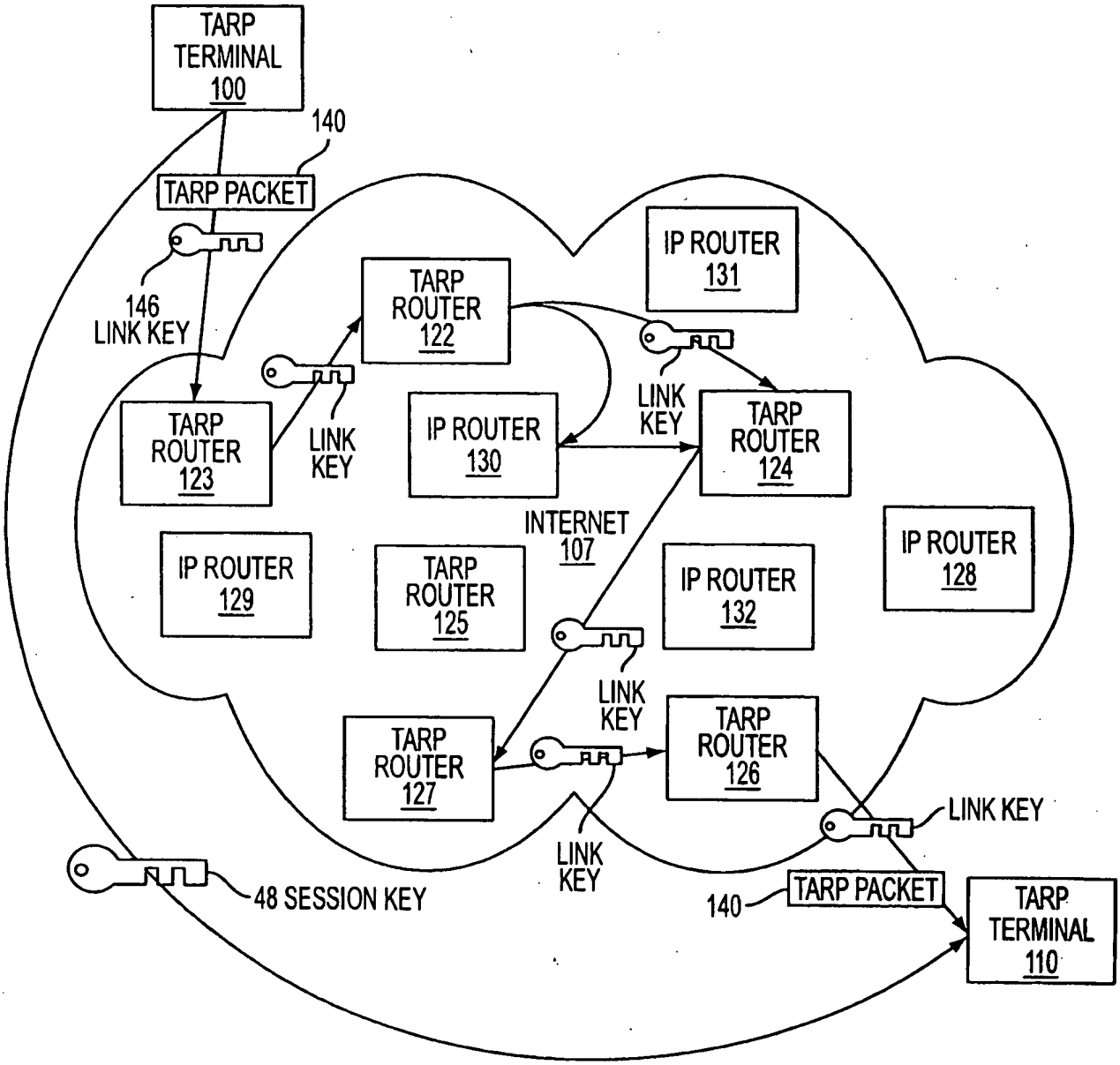

TARP TERMINAL 100
140
TARP PACKET
146 LINK KEY
TARP ROUTER 122
IP ROUTER 131
LINK KEY
TARP ROUTER 123
LINK KEY
IP ROUTER 130
TARP ROUTER 124
INTERNET 107
IP ROUTER 129
TARP ROUTER 125
IP ROUTER 132
IP ROUTER 128
LINK KEY
TARP ROUTER 127
TARP ROUTER 126
LINK KEY
LINK KEY
48 SESSION KEY
140
TARP PACKET
TARP TERMINAL 110

FIG. 2

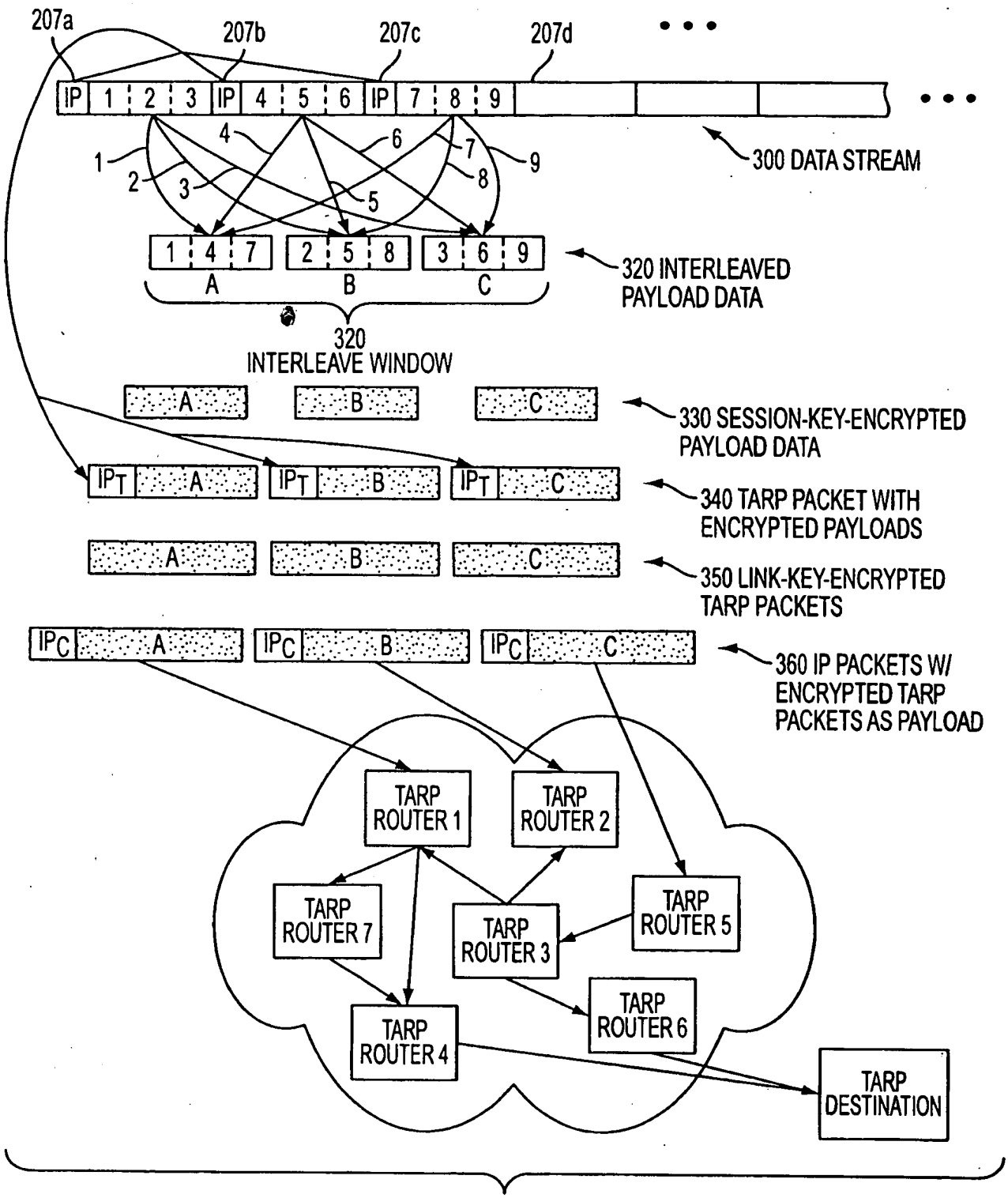

207a
207b
207c
207d
IP 1 2 3 IP 4 5 6 IP 7 8 9
300 DATA STREAM
1 4 7
2 5 8
3 6 9
A
B
C
320 INTERLEAVED PAYLOAD DATA
320 INTERLEAVE WINDOW
330 SESSION-KEY-ENCRYPTED PAYLOAD DATA
IPT A
IPT B
IPT C
340 TARP PACKET WITH ENCRYPTED PAYLOADS
350 LINK-KEY-ENCRYPTED TARP PACKETS
IPC A
IPC B
IPC C
360 IP PACKETS W/ ENCRYPTED TARP PACKETS AS PAYLOAD
TARP ROUTER 1
TARP ROUTER 2
TARP ROUTER 7
TARP ROUTER 3
TARP ROUTER 5
TARP ROUTER 4
TARP ROUTER 6
TARP DESTINATION

FIG. 3A

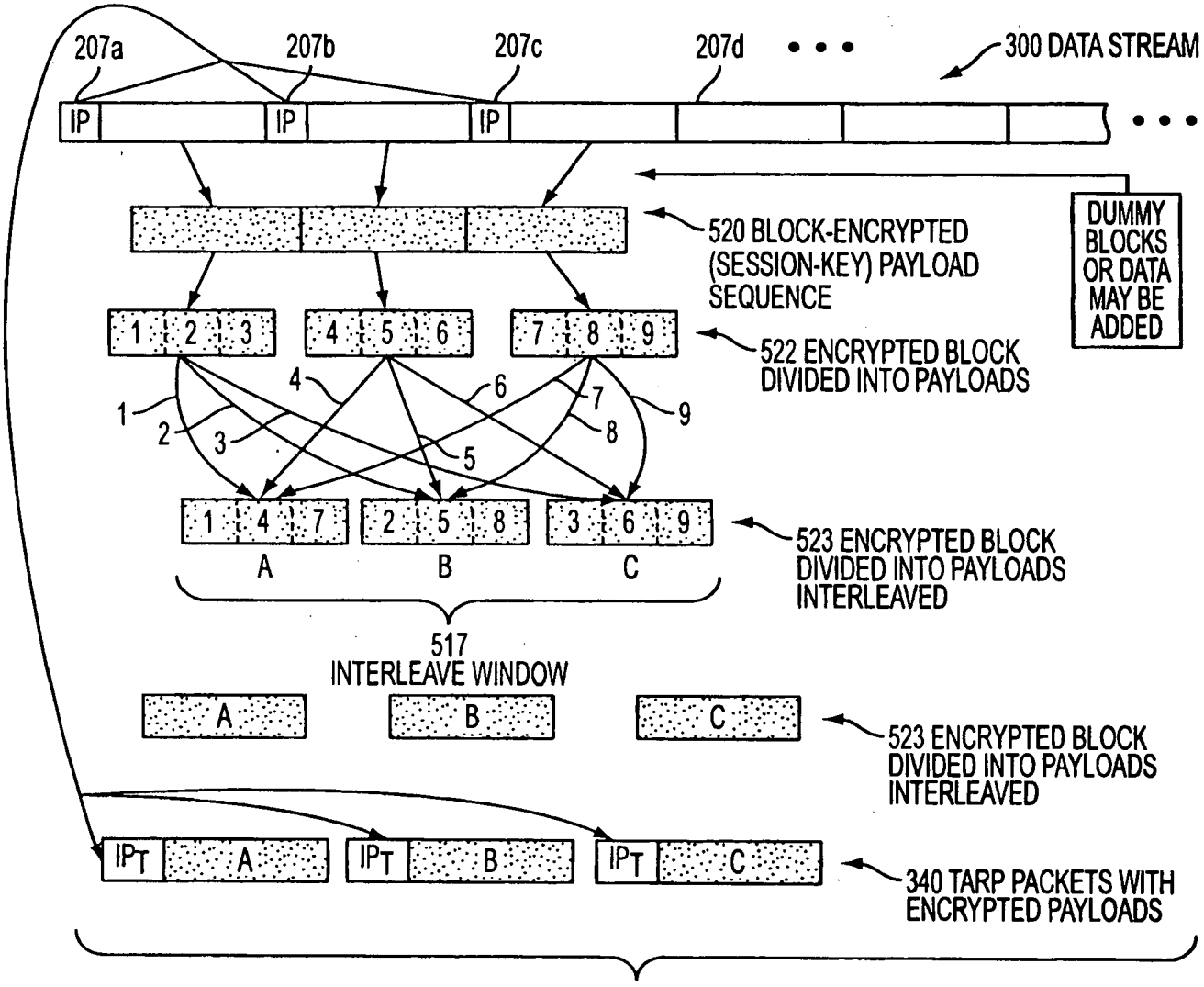

207a
207b
207c
207d
300 DATA STREAM
IP
IP
IP
520 BLOCK-ENCRYPTED (SESSION-KEY) PAYLOAD SEQUENCE
DUMMY BLOCKS OR DATA MAY BE ADDED
1 2 3
4 5 6
7 8 9
522 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS
1 4 7
2 5 8
3 6 9
A
B
C
523 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED
517
INTERLEAVE WINDOW
523 ENCRYPTED BLOCK DIVIDED INTO PAYLOADS INTERLEAVED
IPT
340 TARP PACKETS WITH ENCRYPTED PAYLOADS

FIG. 3B

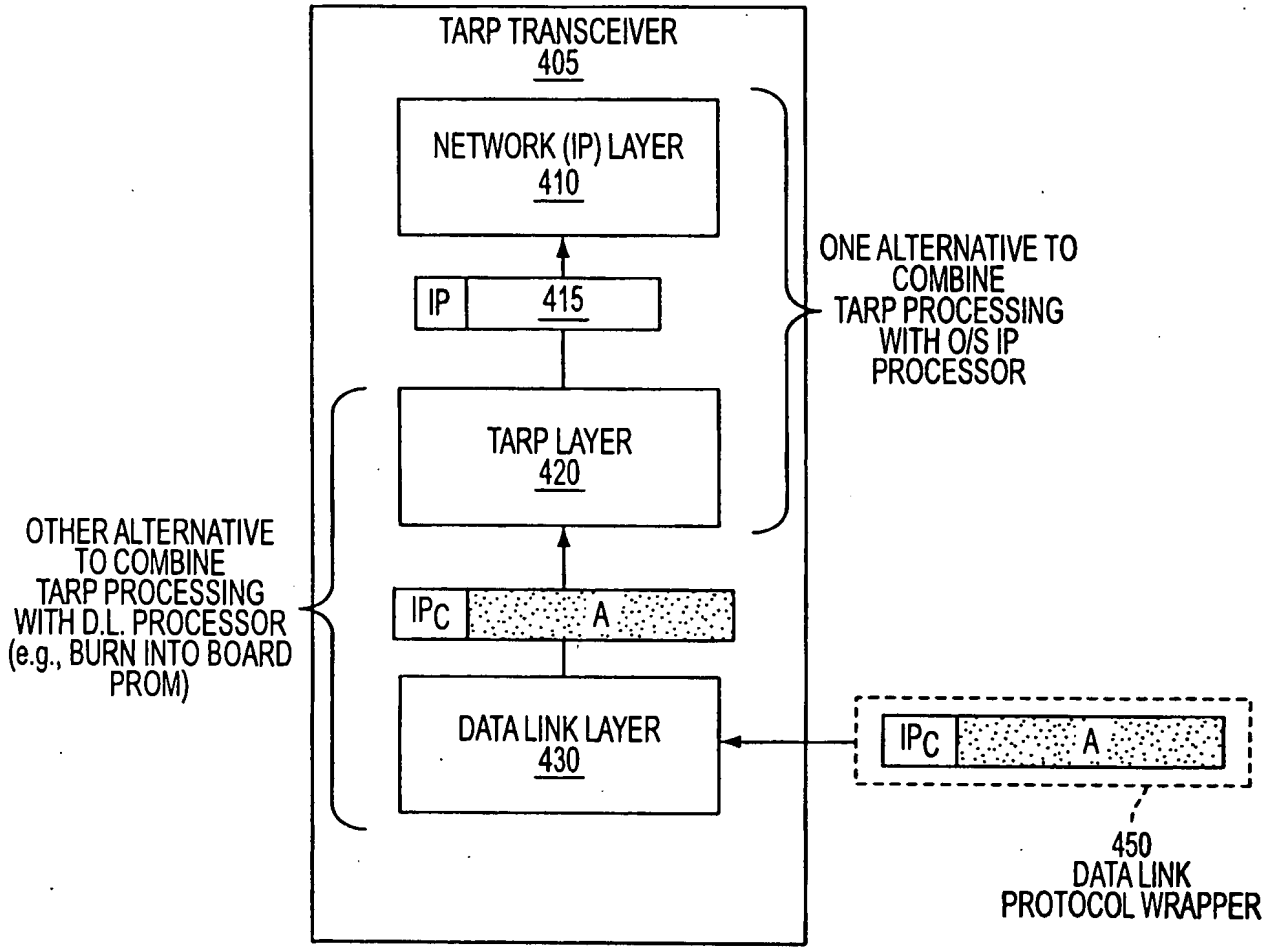

TARP TRANSCEIVER
405
NETWORK (IP) LAYER
410
IP
415
TARP LAYER
420
IPC
A
DATA LINK LAYER
430
ONE ALTERNATIVE TO COMBINE TARP PROCESSING WITH O/S IP PROCESSOR
OTHER ALTERNATIVE TO COMBINE TARP PROCESSING WITH D.L. PROCESSOR (e.g., BURN INTO BOARD PROM)
IPC
A
450
DATA LINK PROTOCOL WRAPPER

FIG. 4

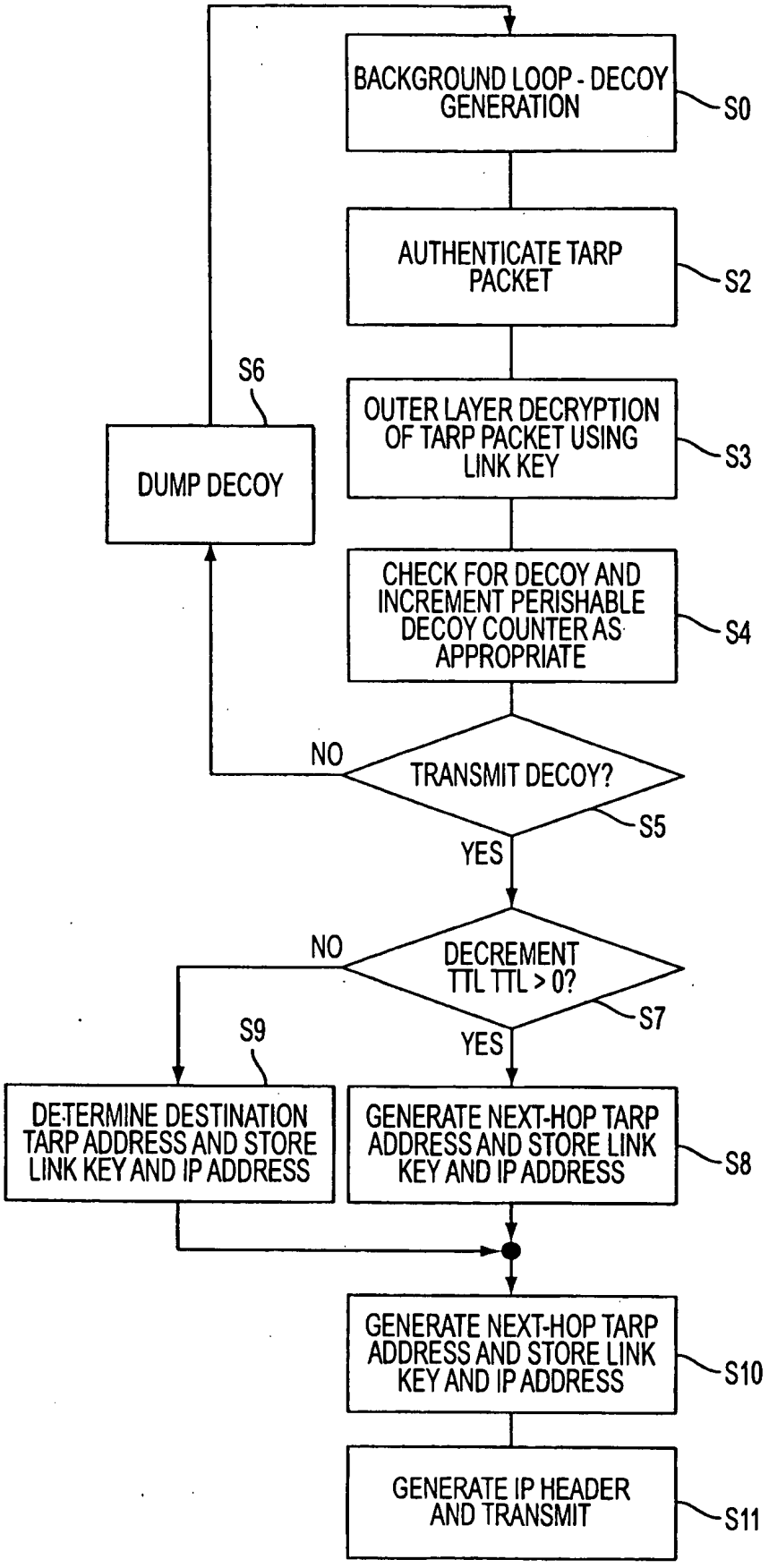

BACKGROUND LOOP - DECOY GENERATION
S0
AUTHENTICATE TARP PACKET
S2
OUTER LAYER DECRYPTION OF TARP PACKET USING LINK KEY
S3
CHECK FOR DECOY AND INCREMENT PERISHABLE DECOY COUNTER AS APPROPRIATE
S4
TRANSMIT DECOY?
S5
NO
YES
DUMP DECOY
S6
DECREMENT TTL TTL > 0?
S7
NO
YES
DETERMINE DESTINATION TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S9
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S8
GENERATE NEXT-HOP TARP ADDRESS AND STORE LINK KEY AND IP ADDRESS
S10
GENERATE IP HEADER AND TRANSMIT
S11

FIG. 5

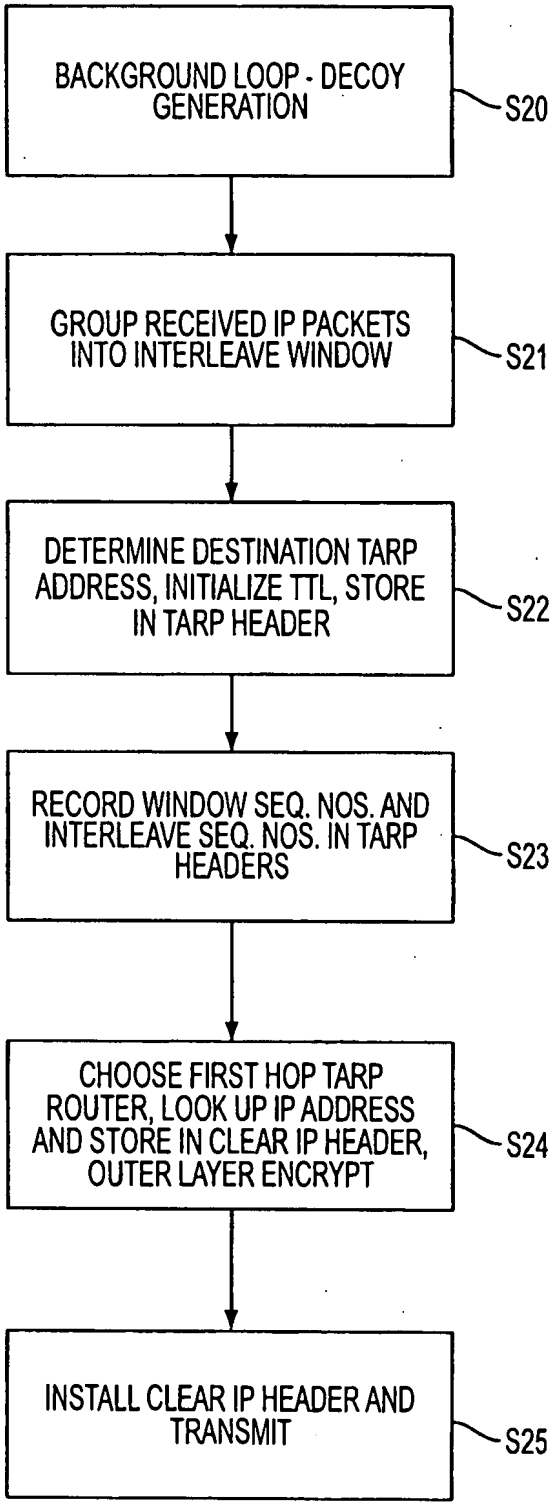

BACKGROUND LOOP - DECOY GENERATION
S20
GROUP RECEIVED IP PACKETS INTO INTERLEAVE WINDOW
S21
DETERMINE DESTINATION TARP ADDRESS, INITIALIZE TTL, STORE IN TARP HEADER
S22
RECORD WINDOW SEQ. NOS. AND INTERLEAVE SEQ. NOS. IN TARP HEADERS
S23
CHOOSE FIRST HOP TARP ROUTER, LOOK UP IP ADDRESS AND STORE IN CLEAR IP HEADER, OUTER LAYER ENCRYPT
S24
INSTALL CLEAR IP HEADER AND TRANSMIT
S25

FIG. 6

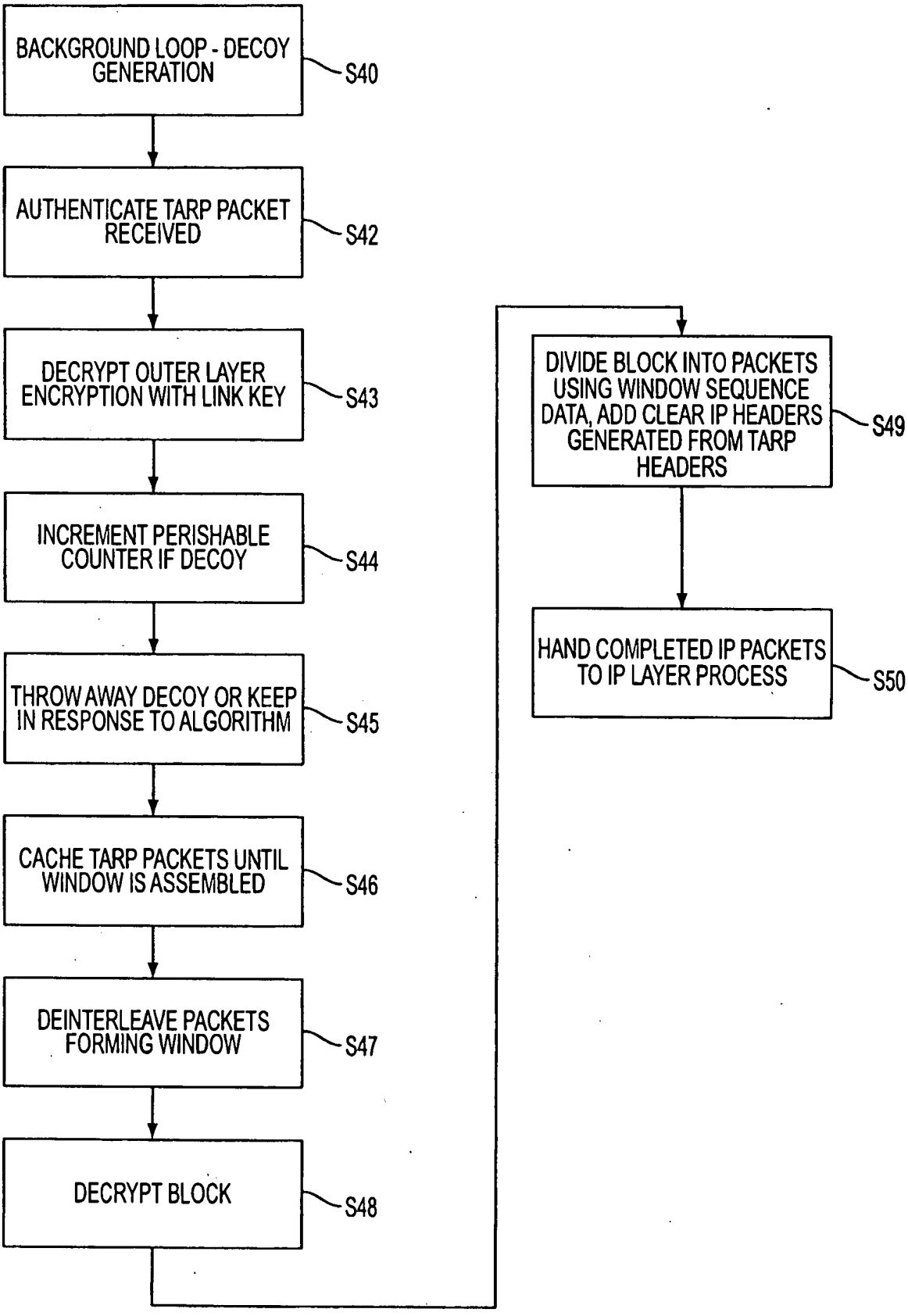

BACKGROUND LOOP - DECOY GENERATION
S40
AUTHENTICATE TARP PACKET RECEIVED
S42
DECRYPT OUTER LAYER ENCRYPTION WITH LINK KEY
S43
INCREMENT PERISHABLE COUNTER IF DECOY
S44
THROW AWAY DECOY OR KEEP IN RESPONSE TO ALGORITHM
S45
CACHE TARP PACKETS UNTIL WINDOW IS ASSEMBLED
S46
DEINTERLEAVE PACKETS FORMING WINDOW
S47
DECRYPT BLOCK
S48
DIVIDE BLOCK INTO PACKETS USING WINDOW SEQUENCE DATA, ADD CLEAR IP HEADERS GENERATED FROM TARP HEADERS
S49
HAND COMPLETED IP PACKETS TO IP LAYER PROCESS
S50

FIG. 7

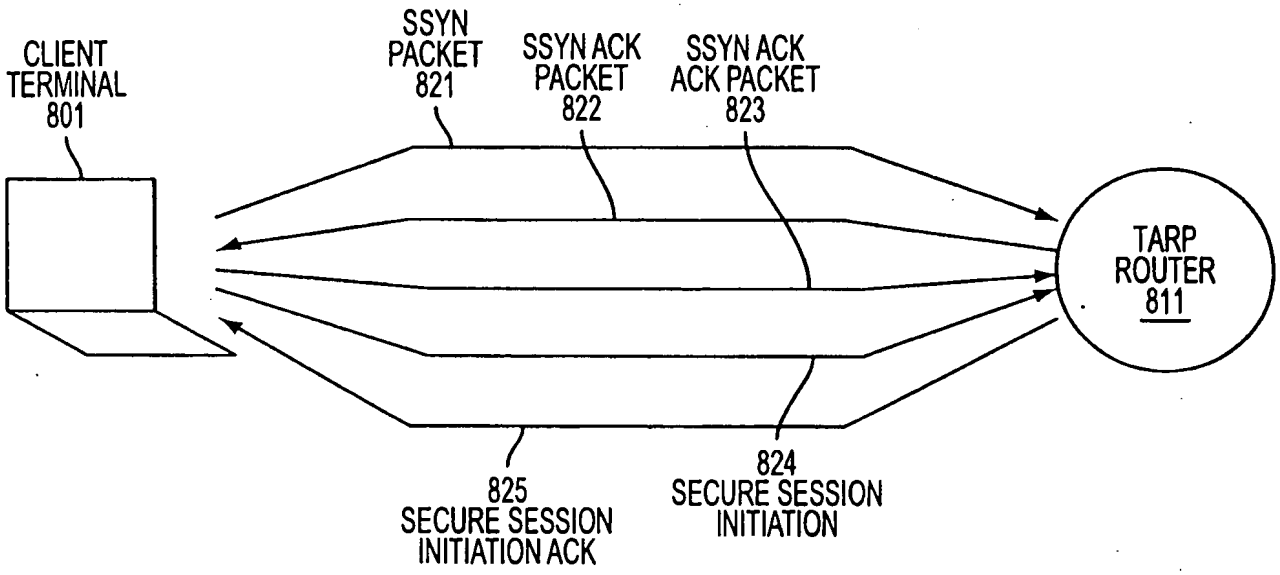

CLIENT TERMINAL 801
SSYN PACKET 821
SSYN ACK PACKET 822
SSYN ACK ACK PACKET 823
TARP ROUTER 811
825 SECURE SESSION INITIATION ACK
824 SECURE SESSION INITIATION

FIG. 8

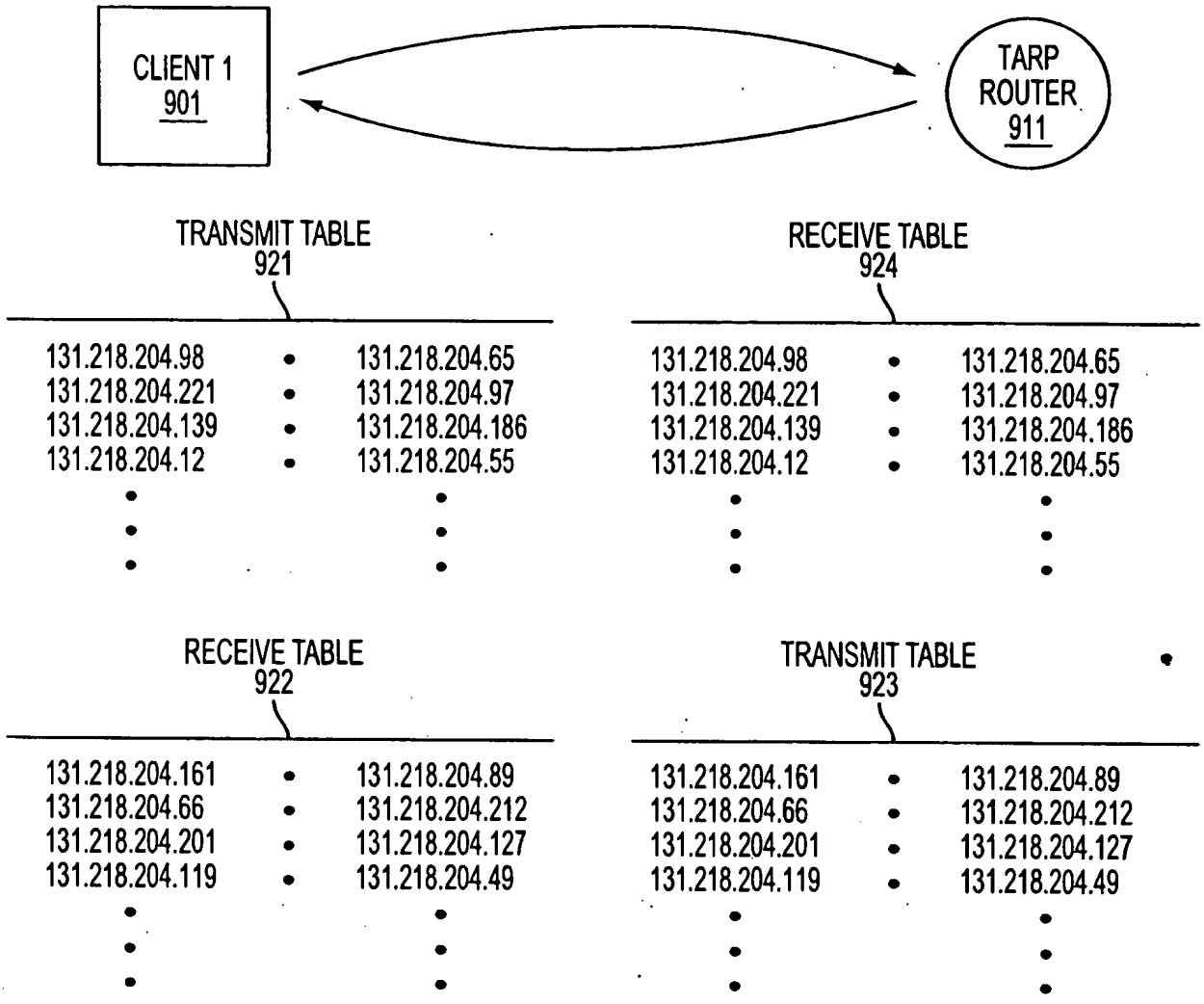

CLIENT 1
901
TARP
ROUTER
911
TRANSMIT TABLE
921
131.218.204.98 • 131.218.204.65
131.218.204.221 • 131.218.204.97
131.218.204.139 • 131.218.204.186
131.218.204.12 • 131.218.204.55
RECEIVE TABLE
924
131.218.204.98 • 131.218.204.65
131.218.204.221 • 131.218.204.97
131.218.204.139 • 131.218.204.186
131.218.204.12 • 131.218.204.55
RECEIVE TABLE
922
131.218.204.161 • 131.218.204.89
131.218.204.66 • 131.218.204.212
131.218.204.201 • 131.218.204.127
131.218.204.119 • 131.218.204.49
TRANSMIT TABLE
923
131.218.204.161 • 131.218.204.89
131.218.204.66 • 131.218.204.212
131.218.204.201 • 131.218.204.127
131.218.204.119 • 131.218.204.49

FIG. 9

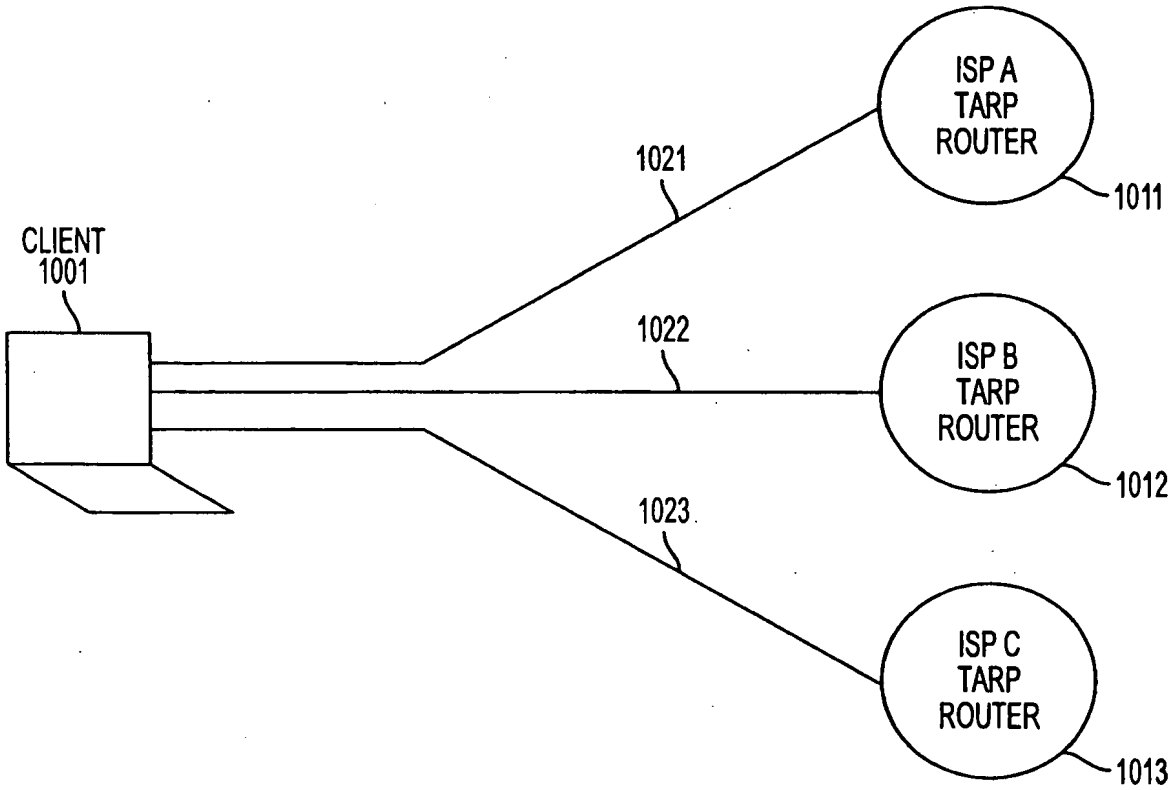

ISP A
TARP
ROUTER
1011
1021
CLIENT
1001
1022
ISP B
TARP
ROUTER
1012
1023
ISP C
TARP
ROUTER
1013

FIG. 10

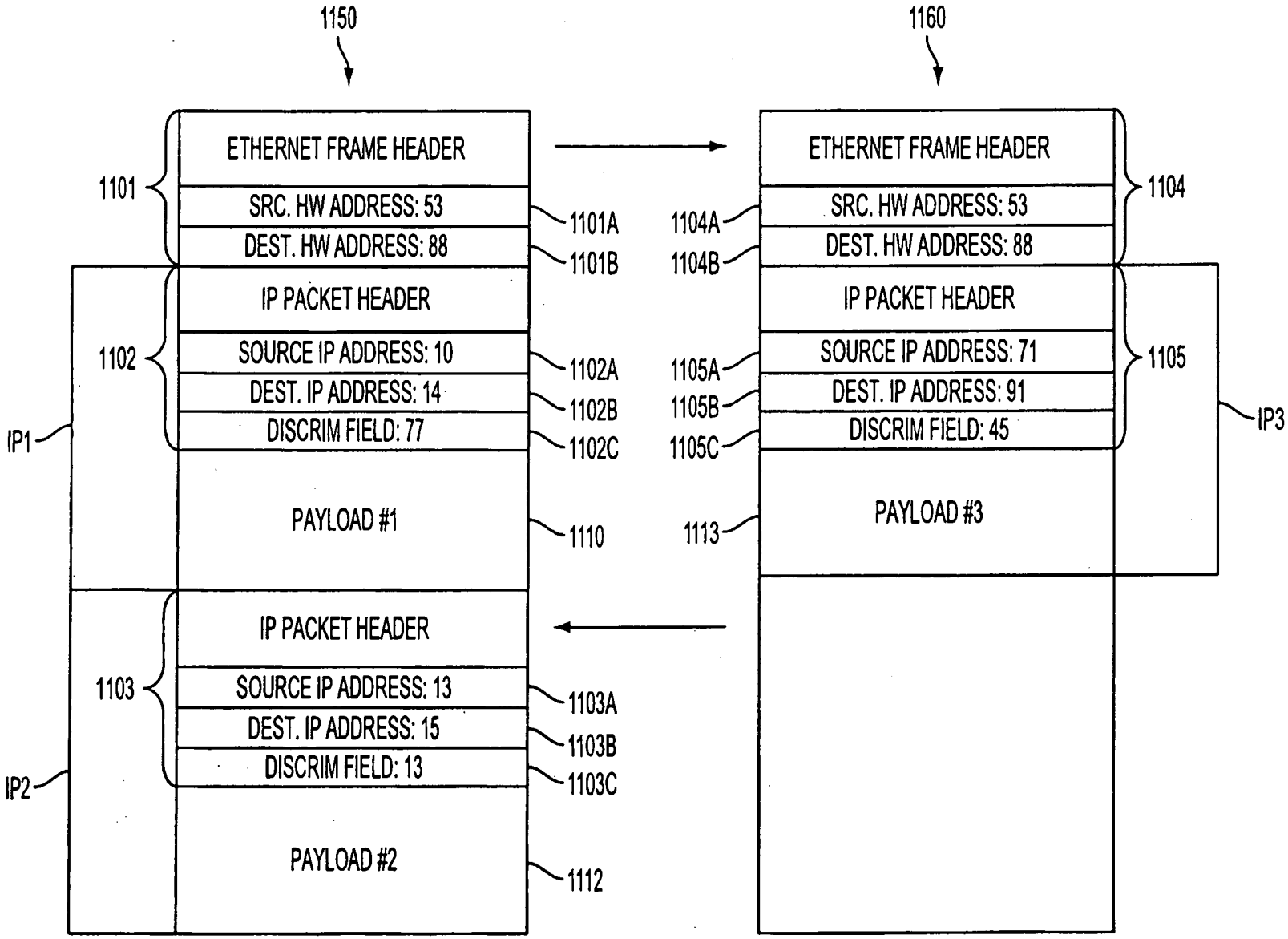


FIG. 11

Petitioner Apple Inc. - Exhibit 1026, p. 100

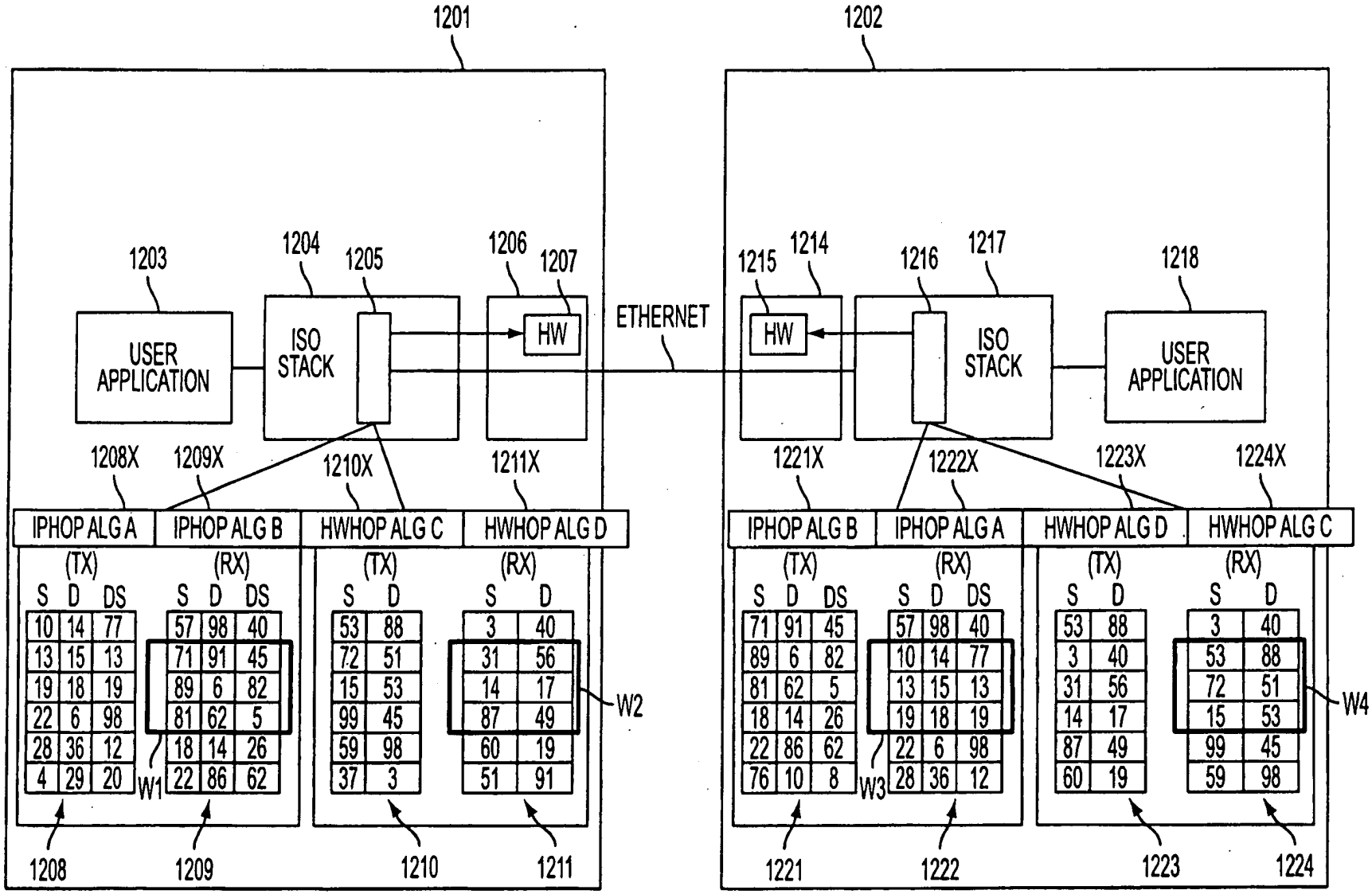


FIG. 12A

Petitioner Apple Inc. - Exhibit 1026, p. 101

MODE OR EMBODIMENT	HARDWARE ADDRESSES	IP ADDRESSES	DISCRIMINATOR FIELD VALUES
1. PROMISCUOUS	SAME FOR ALL NODES OR COMPLETELY RANDOM	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
2. PROMISCUOUS PER VPN	FIXED FOR EACH VPN	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC
3. HARDWARE HOPPING	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC	CAN BE VARIED IN SYNC

FIG. 12B

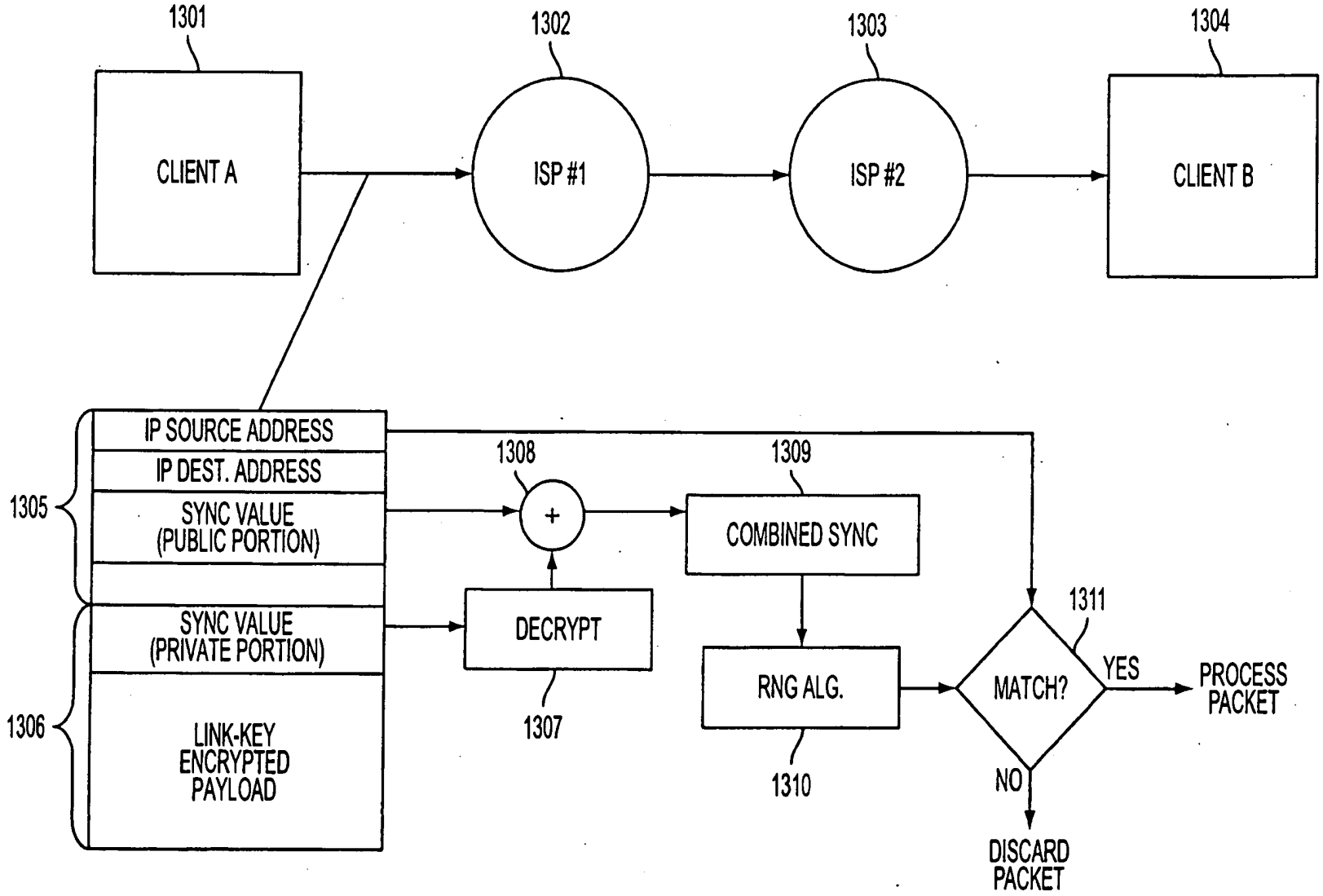


FIG. 13

Petitioner Apple Inc. - Exhibit 1026, p. 103

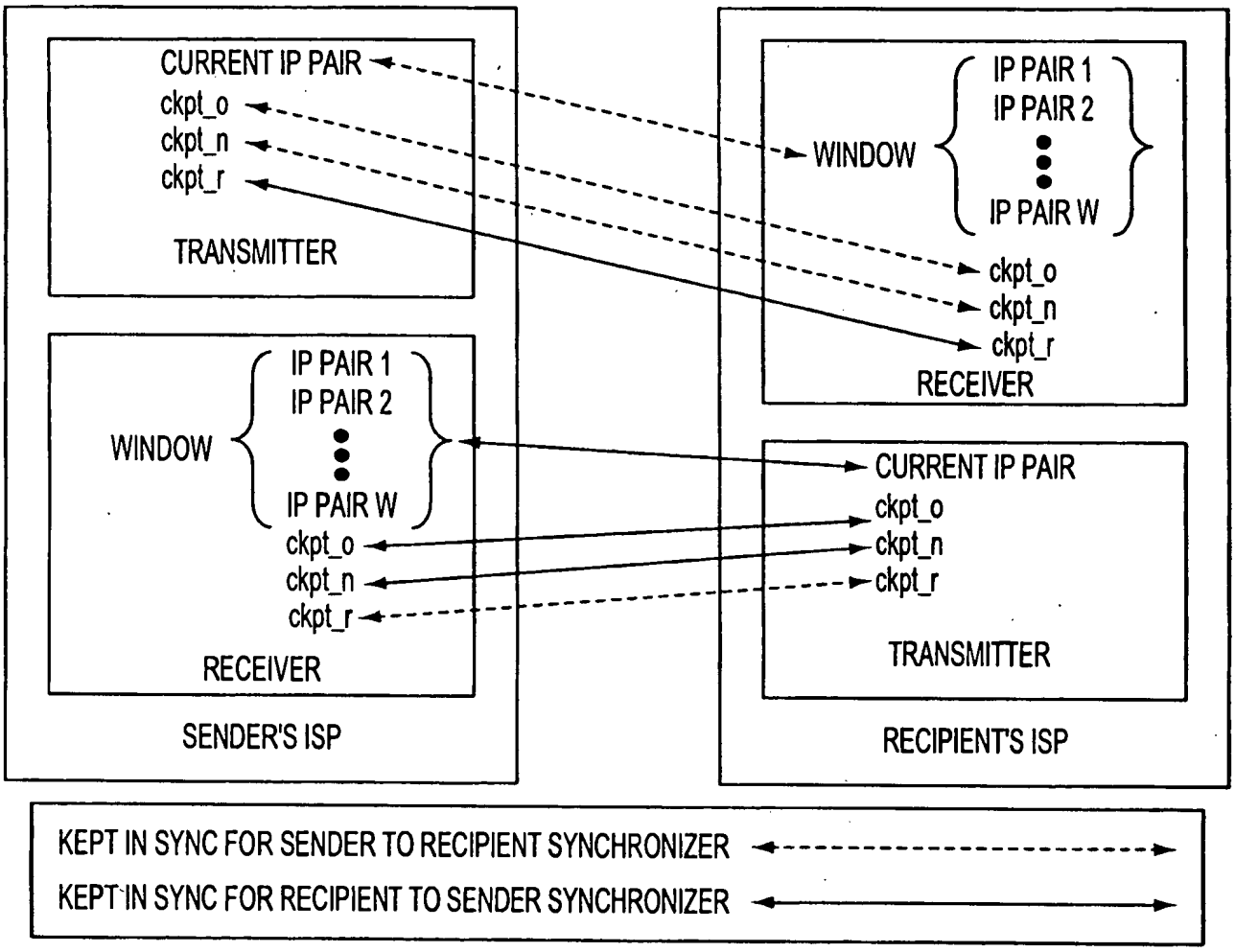

CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
SENDER'S ISP
WINDOW
IP PAIR 1
IP PAIR 2
IP PAIR W
ckpt_o
ckpt_n
ckpt_r
RECEIVER
CURRENT IP PAIR
ckpt_o
ckpt_n
ckpt_r
TRANSMITTER
RECIPIENT'S ISP
KEPT IN SYNC FOR SENDER TO RECIPIENT SYNCHRONIZER
KEPT IN SYNC FOR RECIPIENT TO SENDER SYNCHRONIZER

FIG. 14

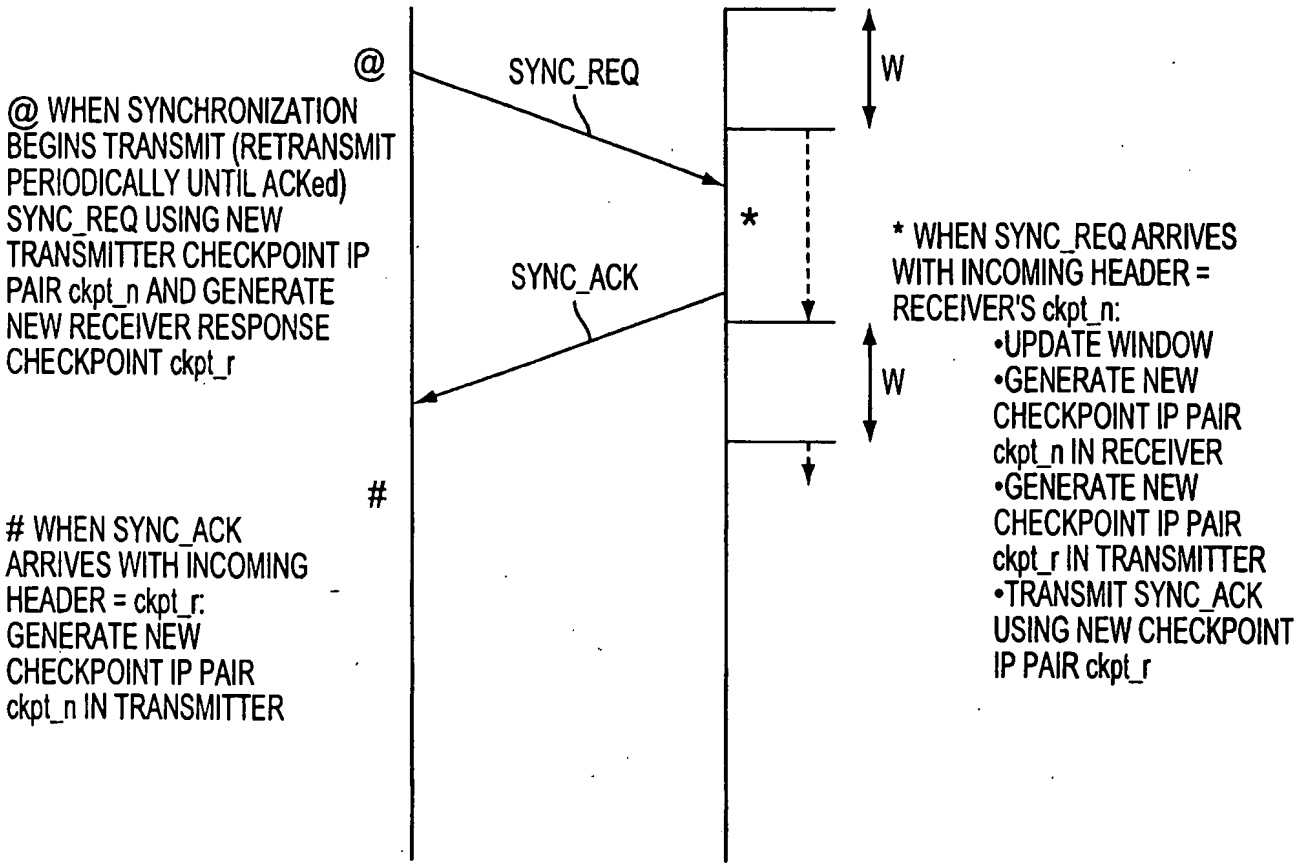

@
@ WHEN SYNCHRONIZATION BEGINS TRANSMIT (RETRANSMIT PERIODICALLY UNTIL ACKed) SYNC_REQ USING NEW TRANSMITTER CHECKPOINT IP PAIR ckpt_n AND GENERATE NEW RECEIVER RESPONSE CHECKPOINT ckpt_r
SYNC_REQ
W
*
* WHEN SYNC_REQ ARRIVES WITH INCOMING HEADER = RECEIVER'S ckpt_n:
•UPDATE WINDOW
•GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN RECEIVER
•GENERATE NEW CHECKPOINT IP PAIR ckpt_r IN TRANSMITTER
•TRANSMIT SYNC_ACK USING NEW CHECKPOINT IP PAIR ckpt_r
SYNC_ACK
W
#
WHEN SYNC_ACK ARRIVES WITH INCOMING HEADER = ckpt_r: GENERATE NEW CHECKPOINT IP PAIR ckpt_n IN TRANSMITTER

FIG. 15

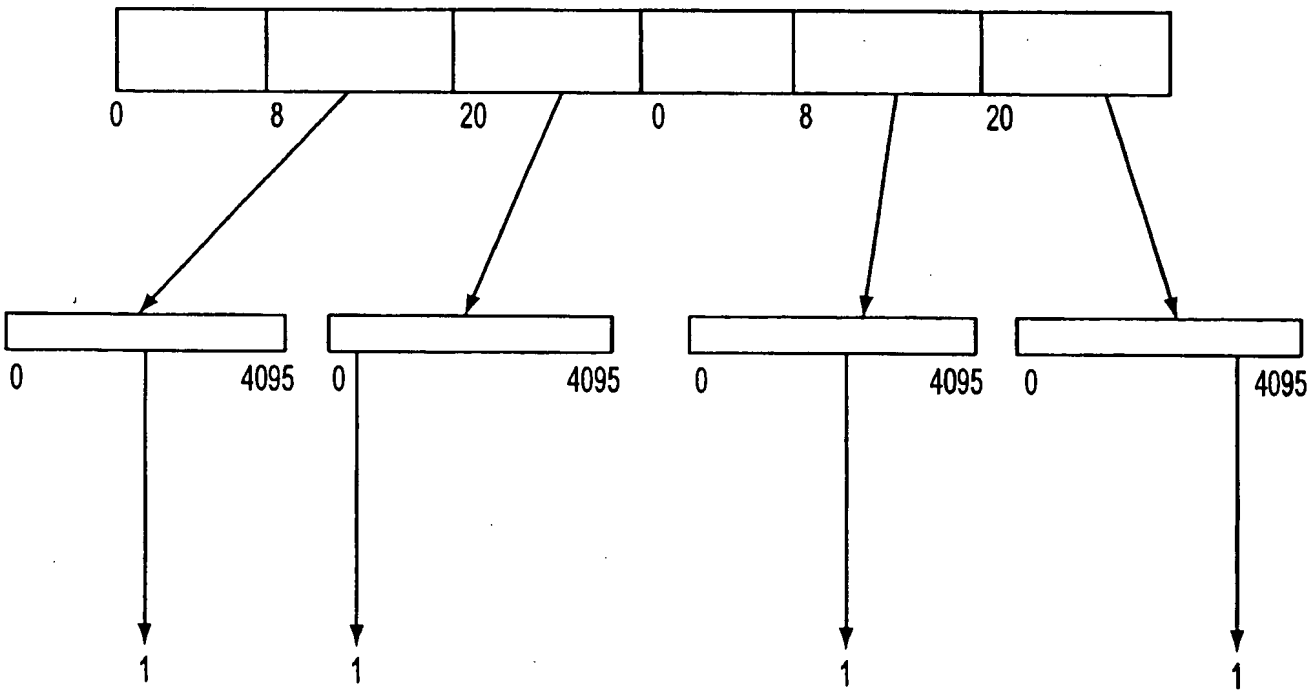


FIG. 16

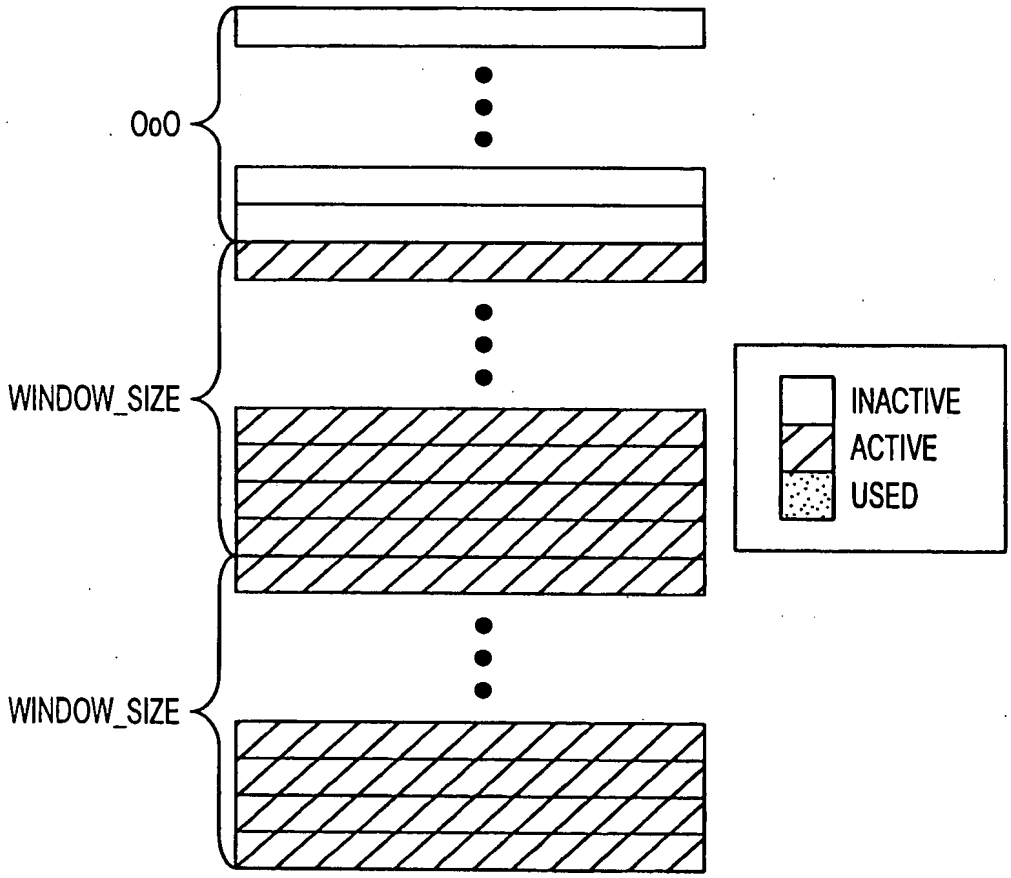


FIG. 17

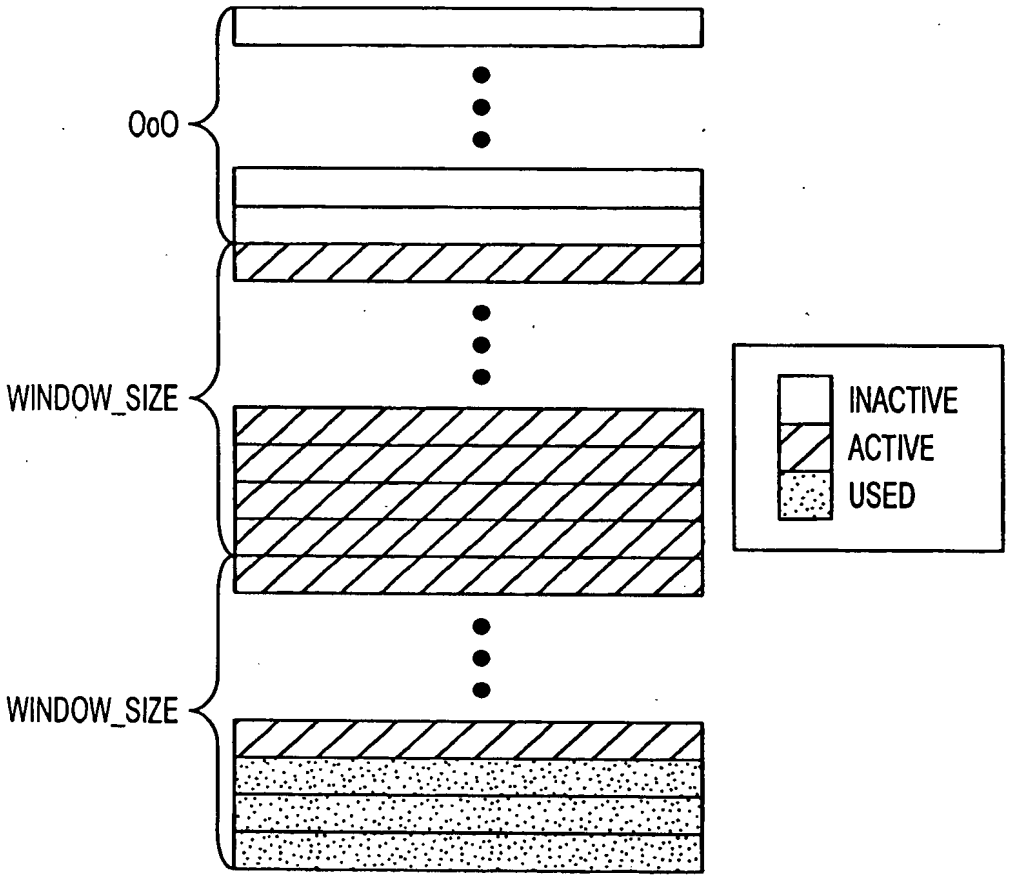


FIG. 18

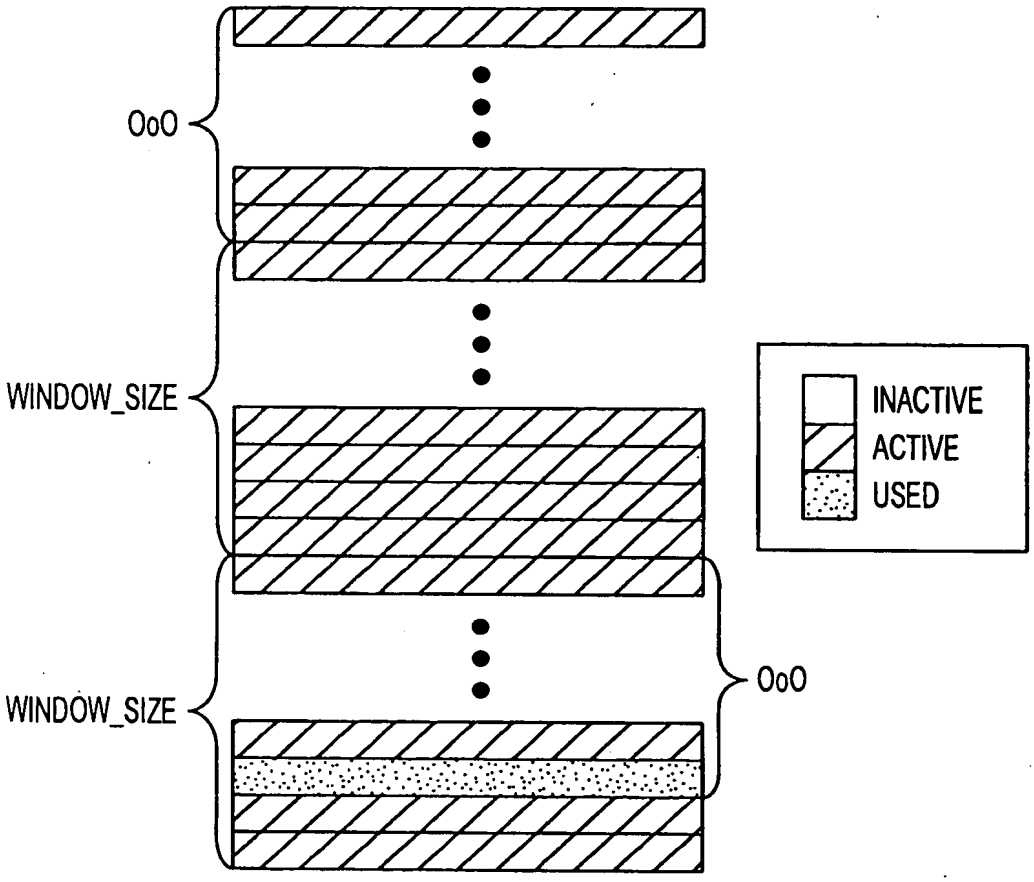


FIG. 19

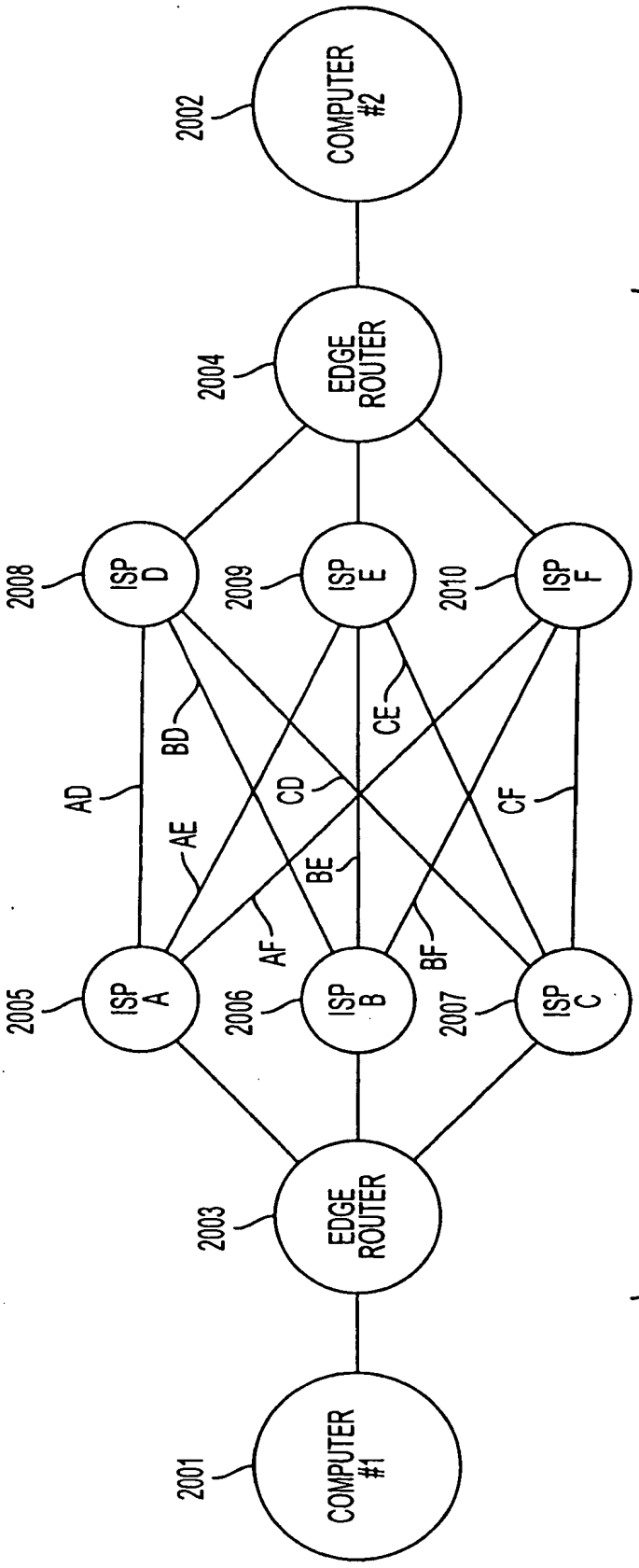

COMPUTER #1
2001
EDGE ROUTER
2003
ISP A
2005
ISP B
2006
ISP C
2007
ISP D
2008
ISP E
2009
ISP F
2010
EDGE ROUTER
2004
COMPUTER #2
2002
AD
AE
AF
BD
BE
BF
CD
CE
CF
2011

FIG. 20

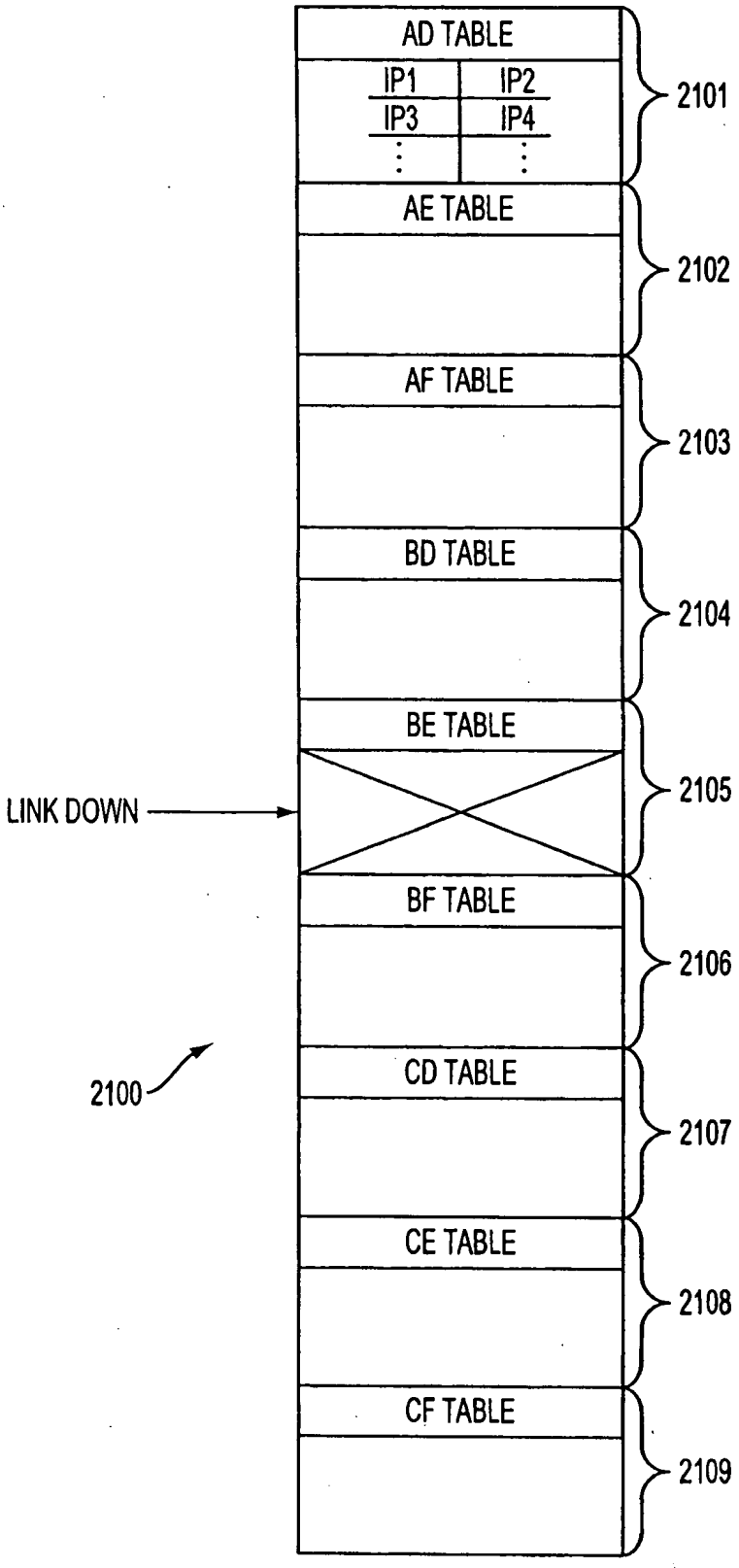

AD TABLE
IP1
IP2
IP3
IP4
2101
AE TABLE
2102
AF TABLE
2103
BD TABLE
2104
BE TABLE
LINK DOWN
2105
BF TABLE
2106
2100
CD TABLE
2107
CE TABLE
2108
CF TABLE
2109

FIG. 21

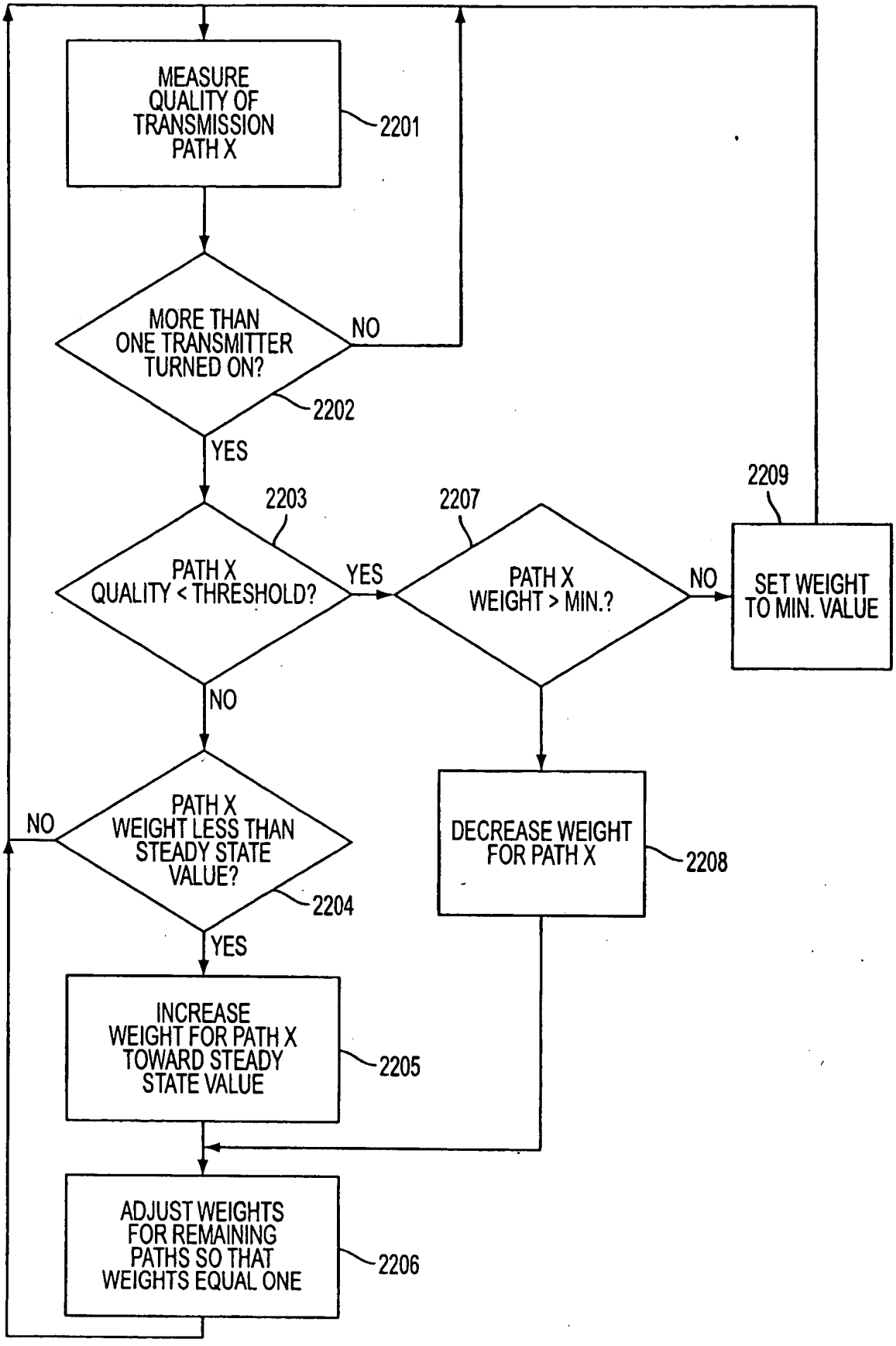

MEASURE QUALITY OF TRANSMISSION PATH X
2201
MORE THAN ONE TRANSMITTER TURNED ON?
NO
2202
YES
2203
PATH X QUALITY < THRESHOLD?
YES
2207
PATH X WEIGHT > MIN.?
NO
2209
SET WEIGHT TO MIN. VALUE
NO
PATH X WEIGHT LESS THAN STEADY STATE VALUE?
NO
2204
YES
DECREASE WEIGHT FOR PATH X
2208
INCREASE WEIGHT FOR PATH X TOWARD STEADY STATE VALUE
2205
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2206

FIG. 22A

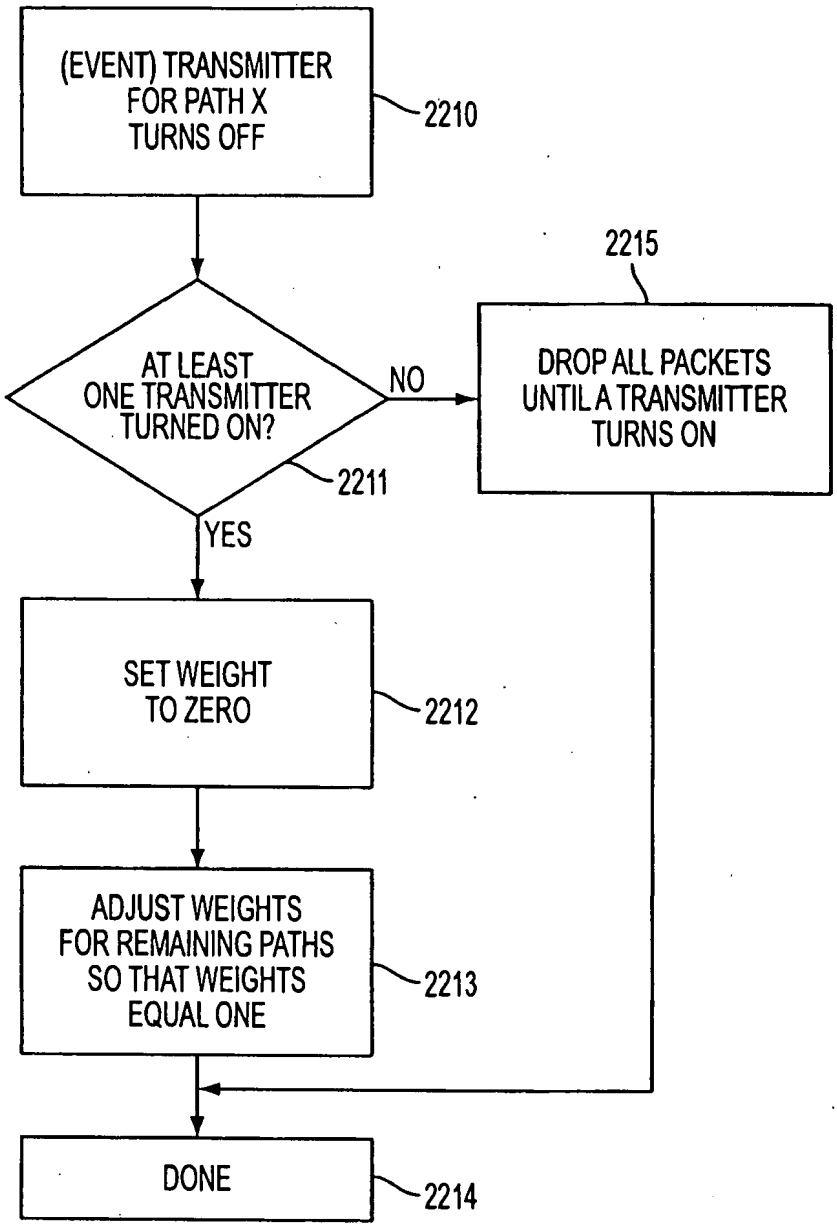

(EVENT) TRANSMITTER FOR PATH X TURNS OFF
2210
AT LEAST ONE TRANSMITTER TURNED ON?
2211
NO
2215
DROP ALL PACKETS UNTIL A TRANSMITTER TURNS ON
YES
SET WEIGHT TO ZERO
2212
ADJUST WEIGHTS FOR REMAINING PATHS SO THAT WEIGHTS EQUAL ONE
2213
DONE
2214

FIG. 22B

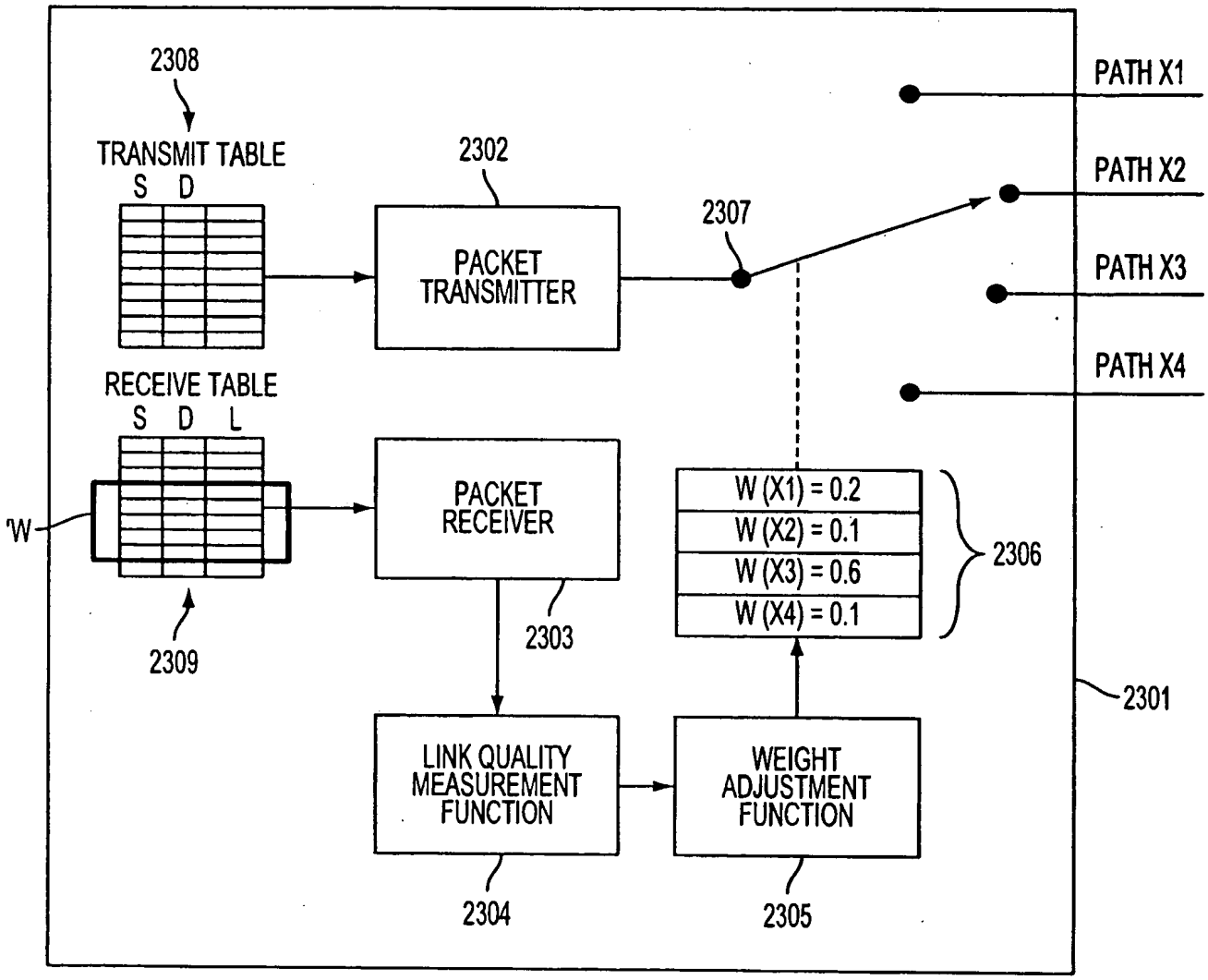

2308
TRANSMIT TABLE
S D
2302
PACKET TRANSMITTER
2307
PATH X1
PATH X2
PATH X3
PATH X4
RECEIVE TABLE
S D L
W
PACKET RECEIVER
W (X1) = 0.2
W (X2) = 0.1
W (X3) = 0.6
W (X4) = 0.1
2306
2309
2303
2301
LINK QUALITY MEASUREMENT FUNCTION
WEIGHT ADJUSTMENT FUNCTION
2304
2305

FIG. 23

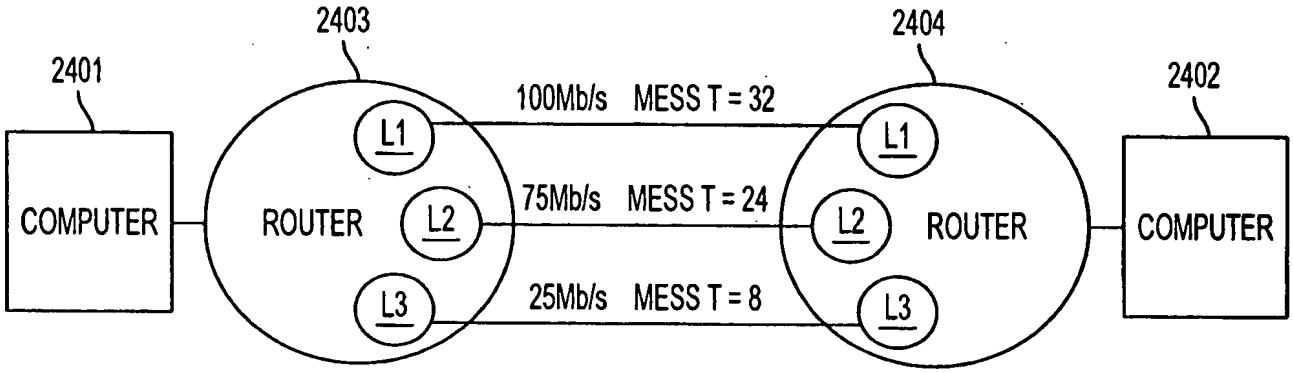

2401
2403
2404
2402
COMPUTER
ROUTER
L1
L2
L3
100Mb/s MESS T = 32
75Mb/s MESS T = 24
25Mb/s MESS T = 8
L1
L2
L3
ROUTER
COMPUTER

FIG. 24

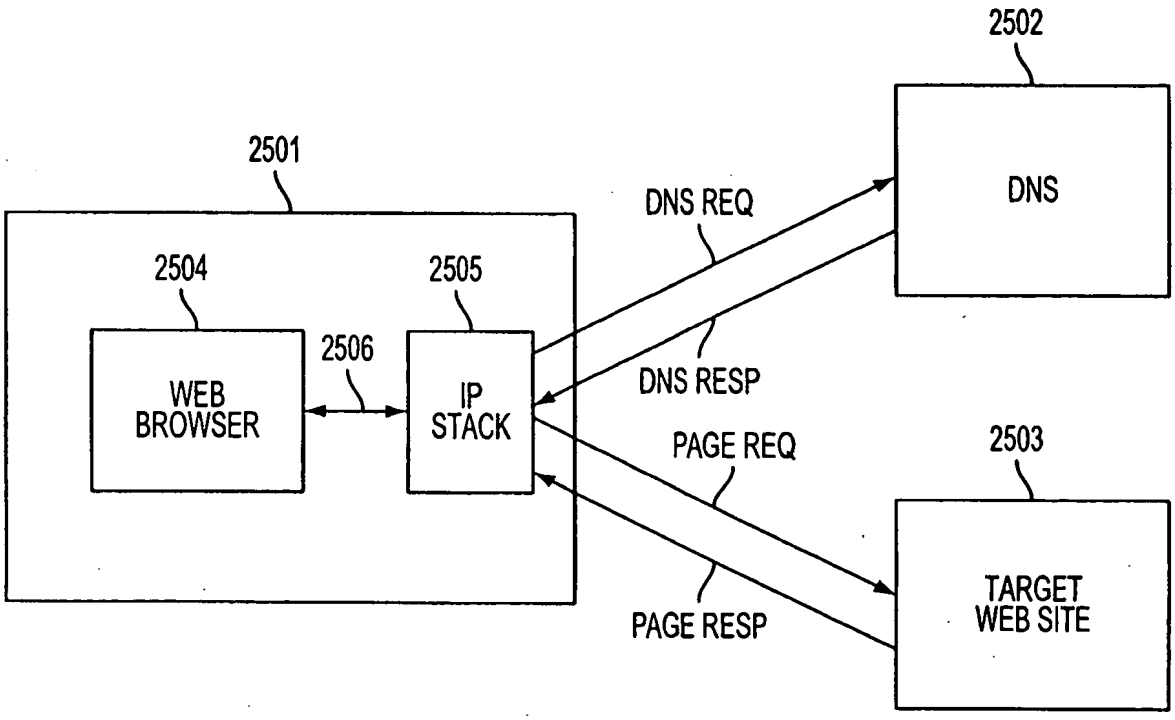


FIG. 25
(PRIOR ART)

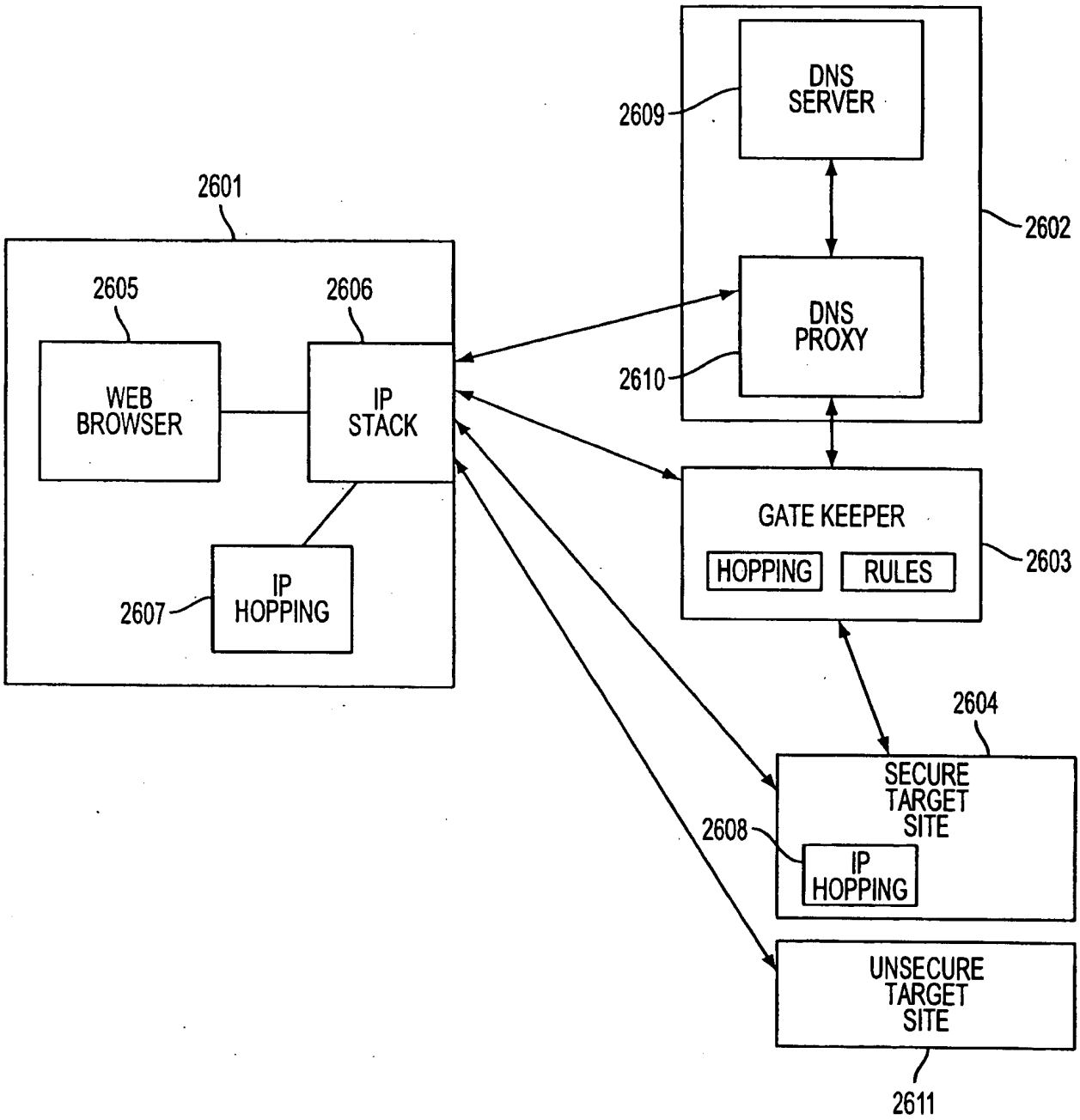

2601
2605
2606
WEB BROWSER
IP STACK
IP HOPPING
2607
2609
DNS SERVER
2602
DNS PROXY
2610
GATE KEEPER
HOPPING
RULES
2603
2604
SECURE TARGET SITE
2608
IP HOPPING
UNSECURE TARGET SITE
2611

FIG. 26

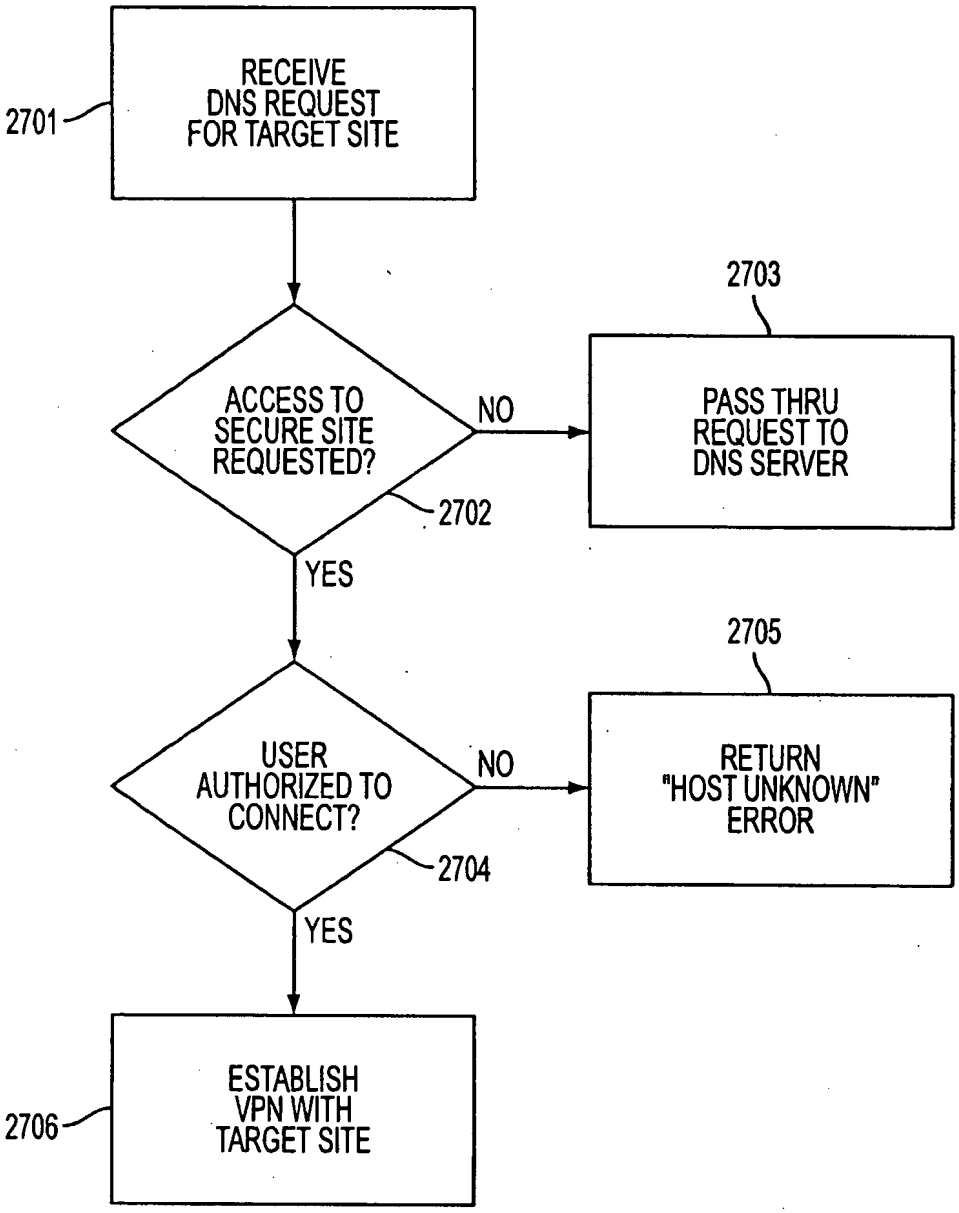

RECEIVE DNS REQUEST FOR TARGET SITE
2701
ACCESS TO SECURE SITE REQUESTED?
2702
NO
2703
PASS THRU REQUEST TO DNS SERVER
YES
USER AUTHORIZED TO CONNECT?
2704
NO
2705
RETURN "HOST UNKNOWN" ERROR
YES
ESTABLISH VPN WITH TARGET SITE
2706

FIG. 27

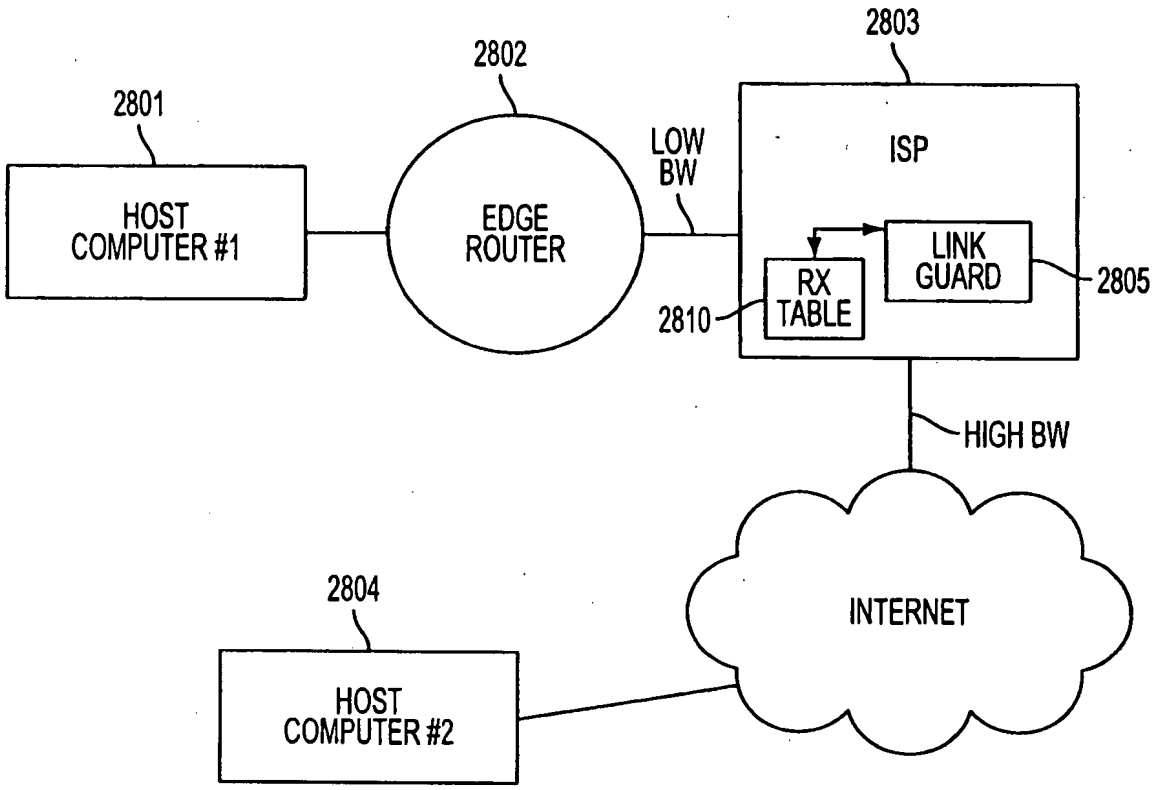

2803
2802
2801
ISP
LOW
BW
HOST
COMPUTER #1
EDGE
ROUTER
LINK
GUARD
2805
RX
TABLE
2810
HIGH BW
INTERNET
2804
HOST
COMPUTER #2

FIG. 28

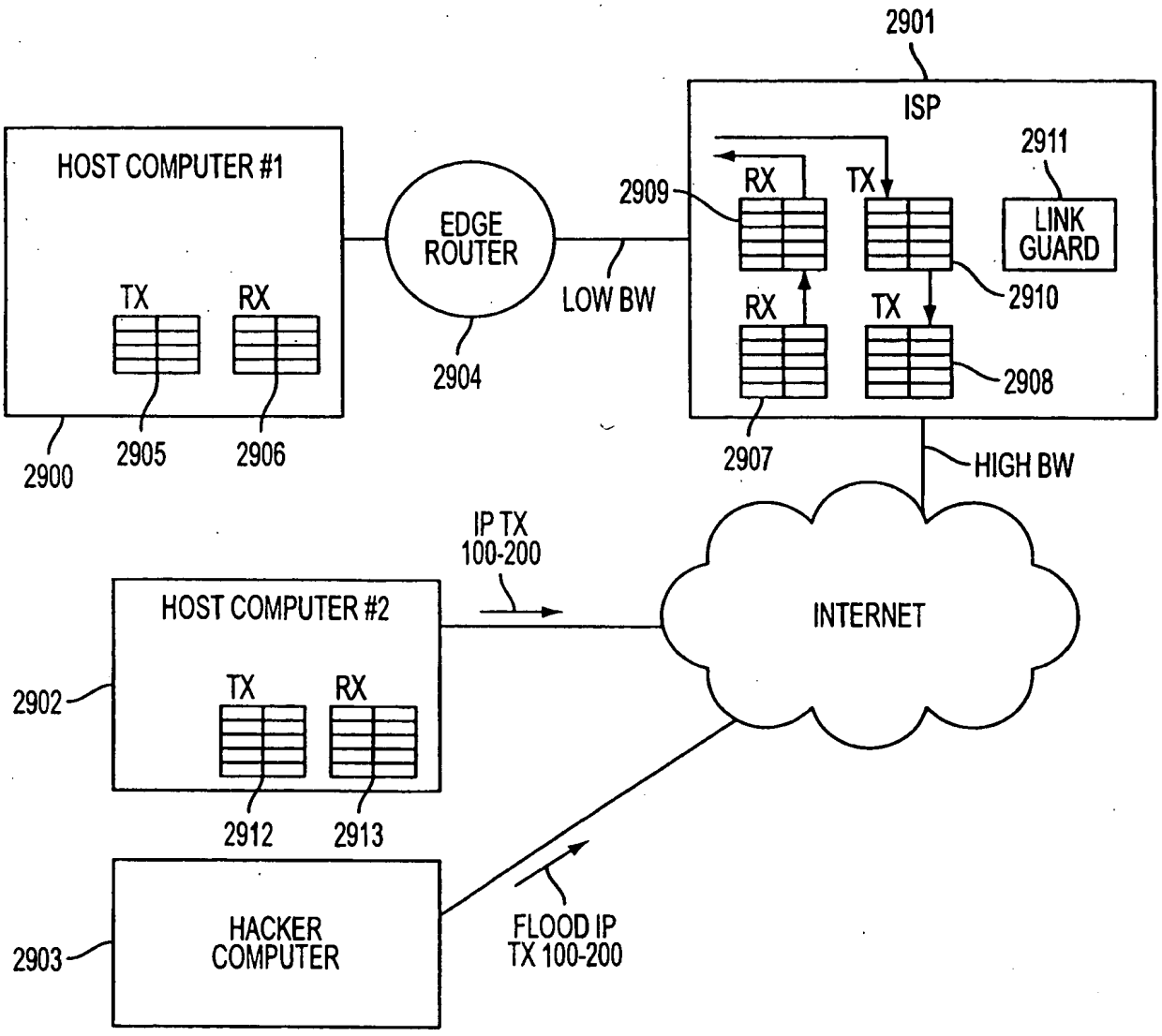

2901
ISP
2911
LINK GUARD
HOST COMPUTER #1
EDGE ROUTER
2909
RX
TX
2910
LOW BW
RX
TX
2908
2904
2907
HIGH BW
TX
RX
2900
2905
2906
IP TX 100-200
INTERNET
HOST COMPUTER #2
2902
TX
RX
2912
2913
HACKER COMPUTER
2903
FLOOD IP TX 100-200

FIG. 29

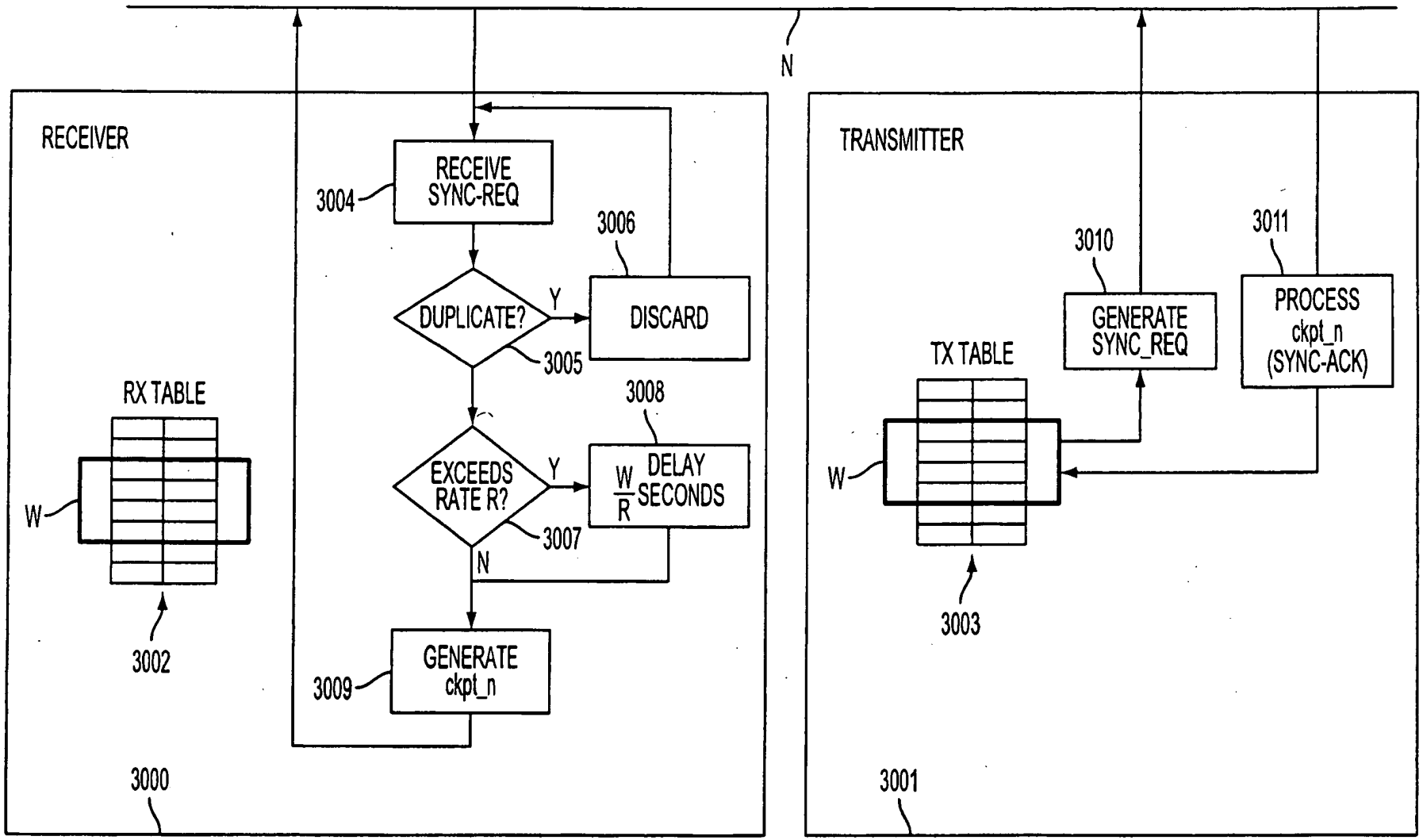


FIG. 30

Petitioner Apple Inc. - Exhibit 1026, p. 121

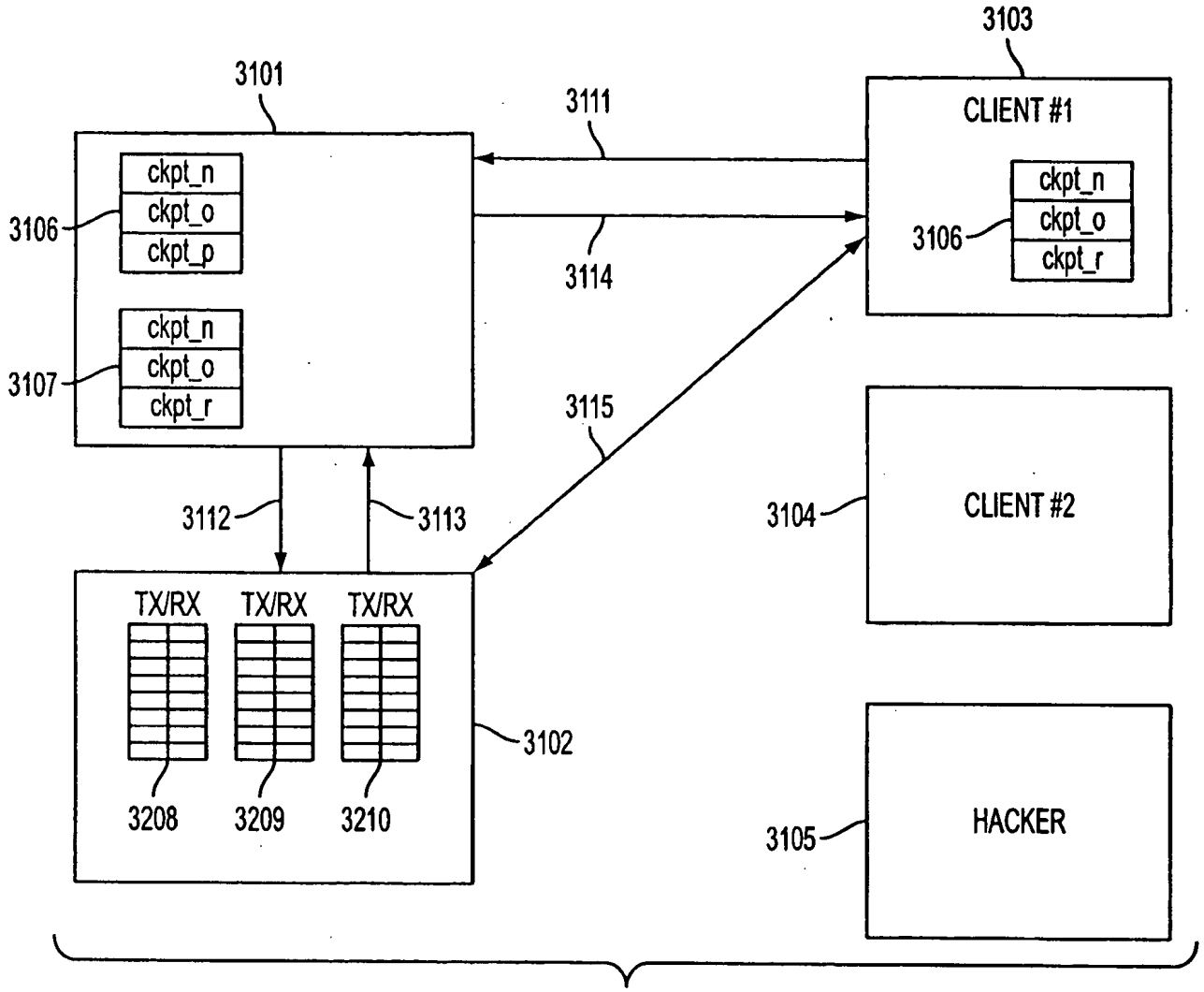

3101
3103
3111
CLIENT #1
ckpt_n
ckpt_o
ckpt_p
3106
ckpt_n
ckpt_o
ckpt_r
3106
3114
ckpt_n
ckpt_o
ckpt_r
3107
3115
3112
3113
3104
CLIENT #2
TX/RX
TX/RX
TX/RX
3102
3208
3209
3210
3105
HACKER

FIG. 31

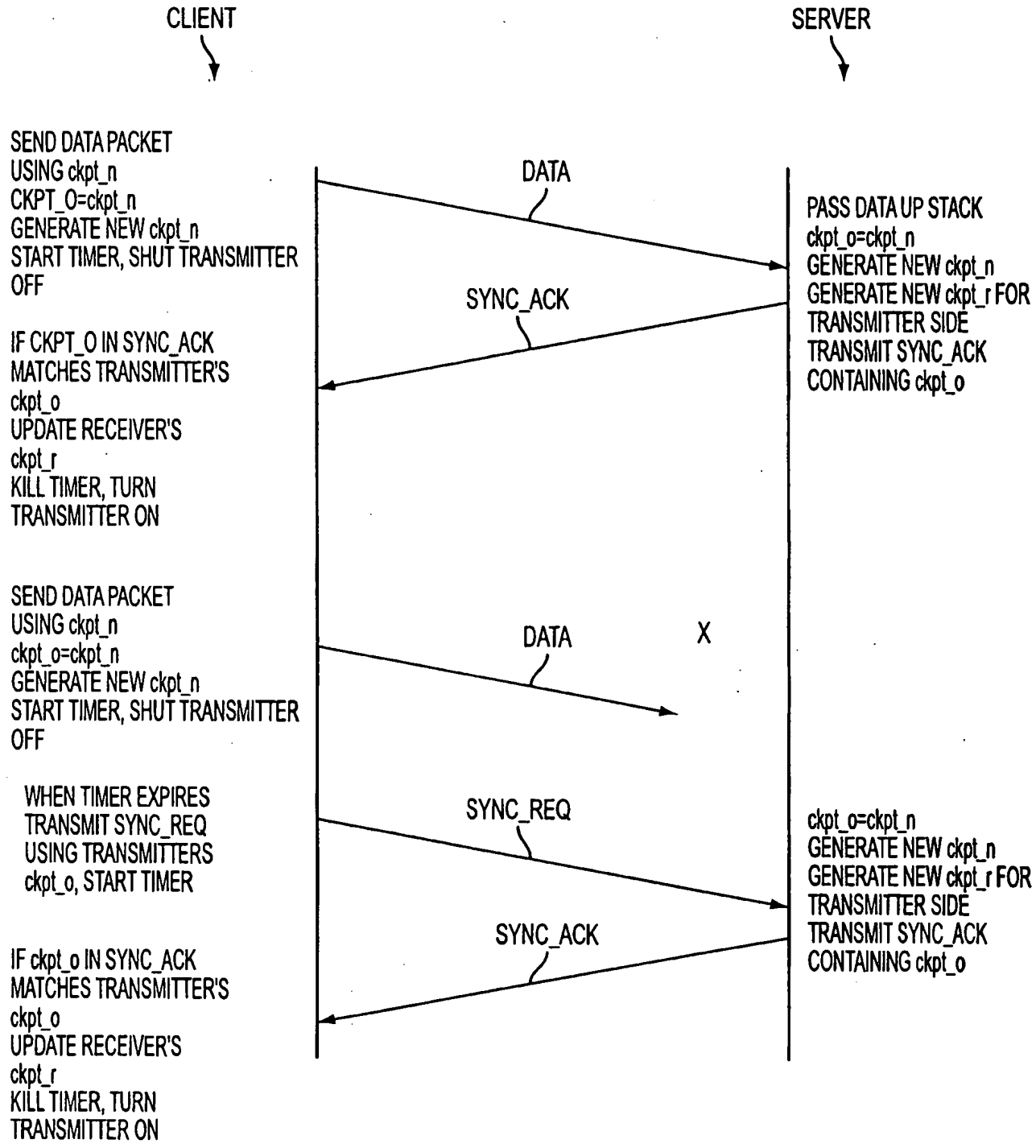

CLIENT
SERVER
SEND DATA PACKET
USING ckpt_n
CKPT_O=ckpt_n
GENERATE NEW ckpt_n
START TIMER, SHUT TRANSMITTER OFF
DATA
PASS DATA UP STACK
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
GENERATE NEW ckpt_r FOR TRANSMITTER SIDE
TRANSMIT SYNC_ACK CONTAINING ckpt_o
SYNC_ACK
IF CKPT_O IN SYNC_ACK MATCHES TRANSMITTER'S ckpt_o
UPDATE RECEIVER'S ckpt_r
KILL TIMER, TURN TRANSMITTER ON
SEND DATA PACKET
USING ckpt_n
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
START TIMER, SHUT TRANSMITTER OFF
DATA
X
WHEN TIMER EXPIRES
TRANSMIT SYNC_REQ
USING TRANSMITTERS
ckpt_o, START TIMER
SYNC_REQ
ckpt_o=ckpt_n
GENERATE NEW ckpt_n
GENERATE NEW ckpt_r FOR TRANSMITTER SIDE
TRANSMIT SYNC_ACK CONTAINING ckpt_o
SYNC_ACK
IF ckpt_o IN SYNC_ACK MATCHES TRANSMITTER'S ckpt_o
UPDATE RECEIVER'S ckpt_r
KILL TIMER, TURN TRANSMITTER ON

FIG. 32

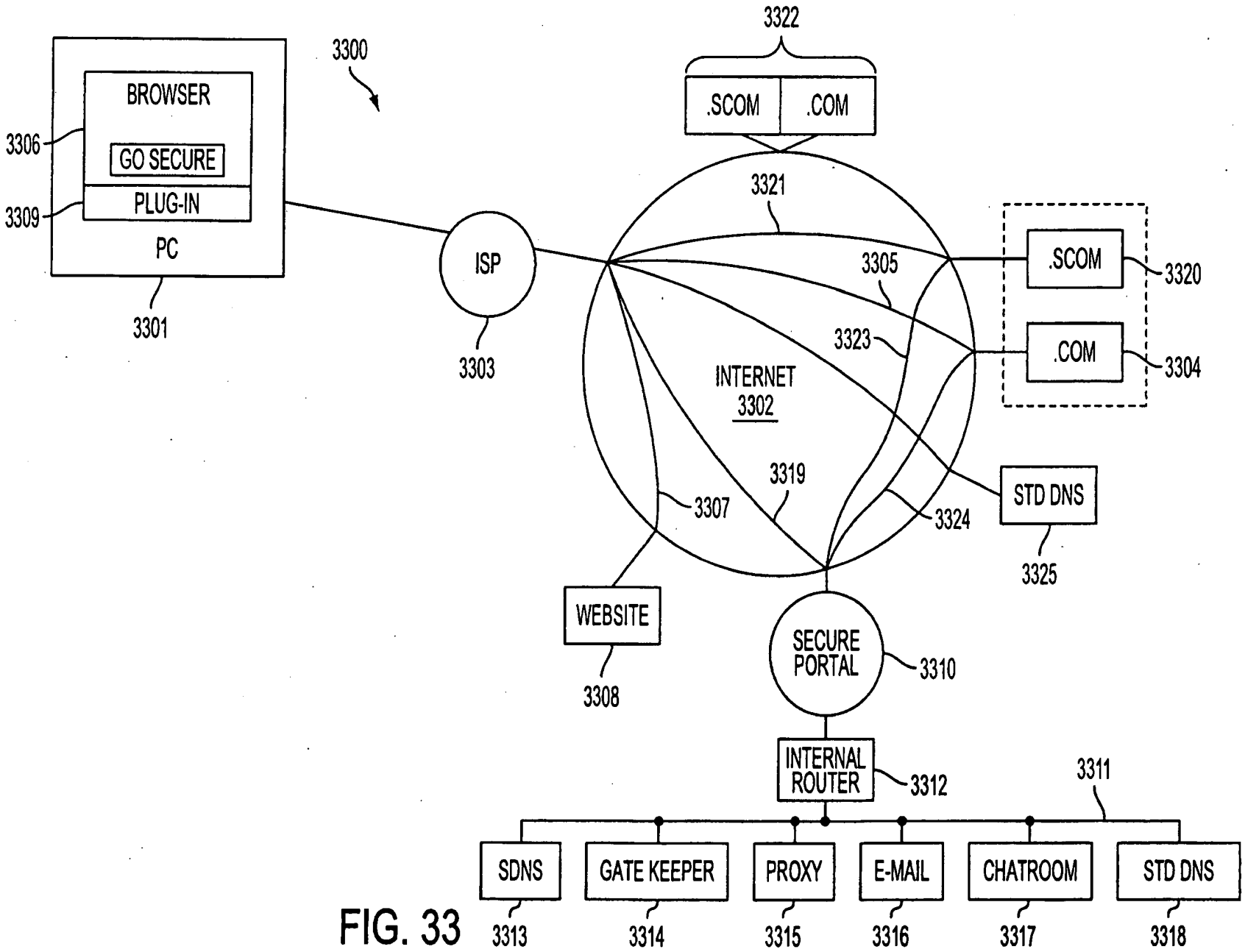


FIG. 33

Petitioner Apple Inc. - Exhibit 1026, p. 124

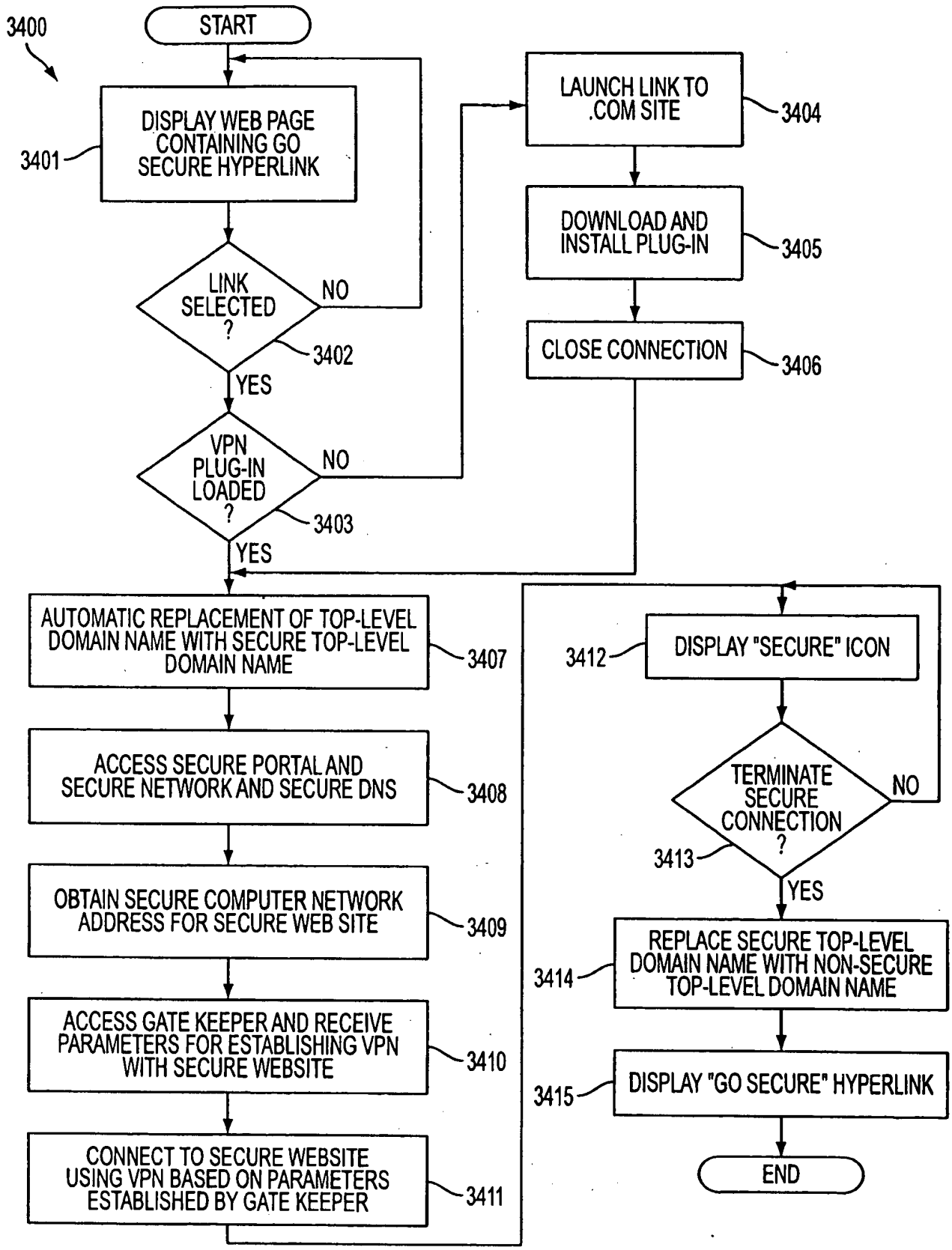

3400
START
DISPLAY WEB PAGE CONTAINING GO SECURE HYPERLINK
3401
LINK SELECTED ?
NO
3402
YES
VPN PLUG-IN LOADED ?
NO
3403
YES
LAUNCH LINK TO .COM SITE
3404
DOWNLOAD AND INSTALL PLUG-IN
3405
CLOSE CONNECTION
3406
AUTOMATIC REPLACEMENT OF TOP-LEVEL DOMAIN NAME WITH SECURE TOP-LEVEL DOMAIN NAME
3407
ACCESS SECURE PORTAL AND SECURE NETWORK AND SECURE DNS
3408
OBTAIN SECURE COMPUTER NETWORK ADDRESS FOR SECURE WEB SITE
3409
ACCESS GATE KEEPER AND RECEIVE PARAMETERS FOR ESTABLISHING VPN WITH SECURE WEBSITE
3410
CONNECT TO SECURE WEBSITE USING VPN BASED ON PARAMETERS ESTABLISHED BY GATE KEEPER
3411
3412
DISPLAY "SECURE" ICON
TERMINATE SECURE CONNECTION ?
NO
3413
YES
REPLACE SECURE TOP-LEVEL DOMAIN NAME WITH NON-SECURE TOP-LEVEL DOMAIN NAME
3414
DISPLAY "GO SECURE" HYPERLINK
3415
END

FIG. 34

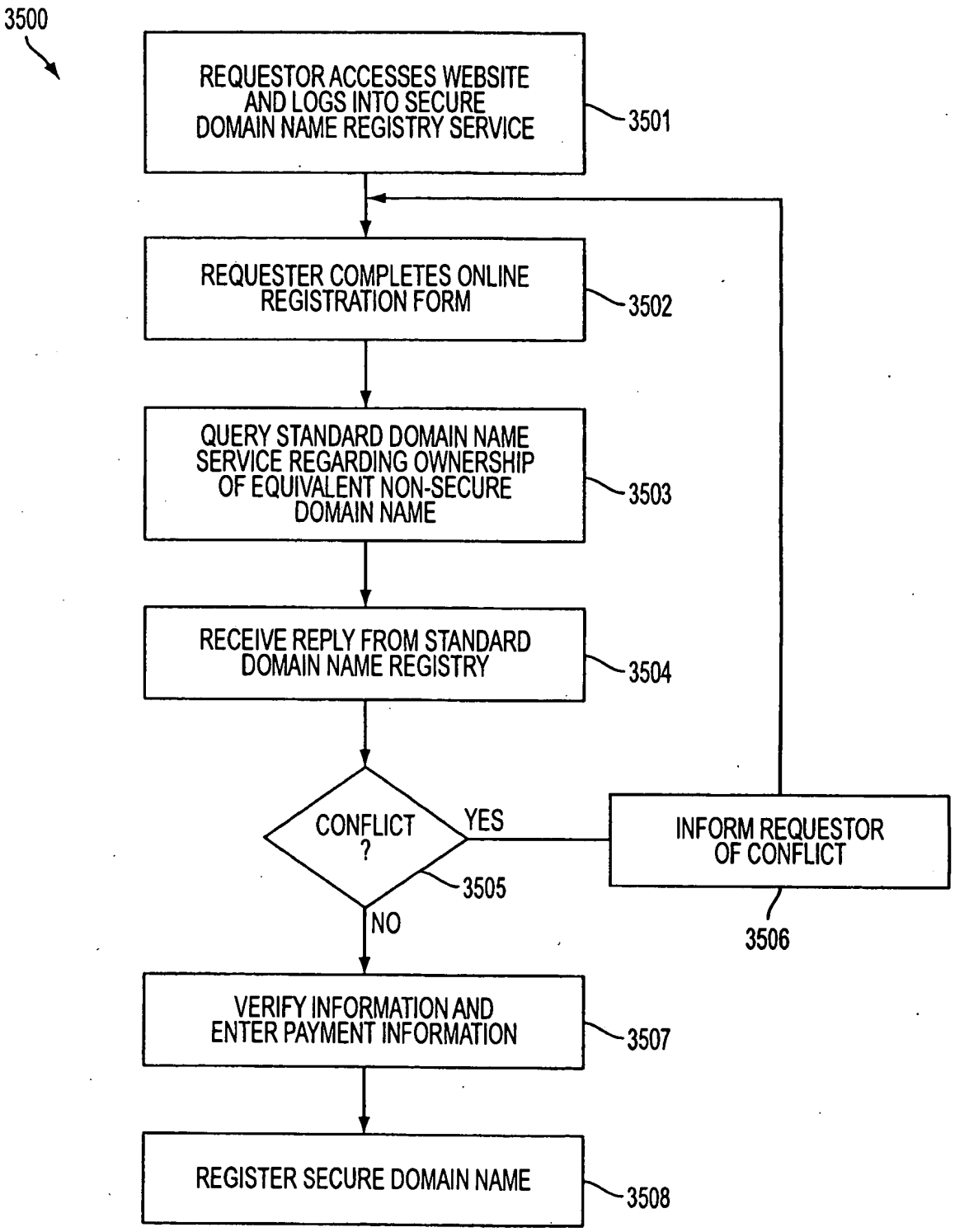

3500
REQUESTOR ACCESSES WEBSITE AND LOGS INTO SECURE DOMAIN NAME REGISTRY SERVICE
3501
REQUESTER COMPLETES ONLINE REGISTRATION FORM
3502
QUERY STANDARD DOMAIN NAME SERVICE REGARDING OWNERSHIP OF EQUIVALENT NON-SECURE DOMAIN NAME
3503
RECEIVE REPLY FROM STANDARD DOMAIN NAME REGISTRY
3504
CONFLICT ?
YES
NO
3505
INFORM REQUESTOR OF CONFLICT
3506
VERIFY INFORMATION AND ENTER PAYMENT INFORMATION
3507
REGISTER SECURE DOMAIN NAME
3508

FIG. 35

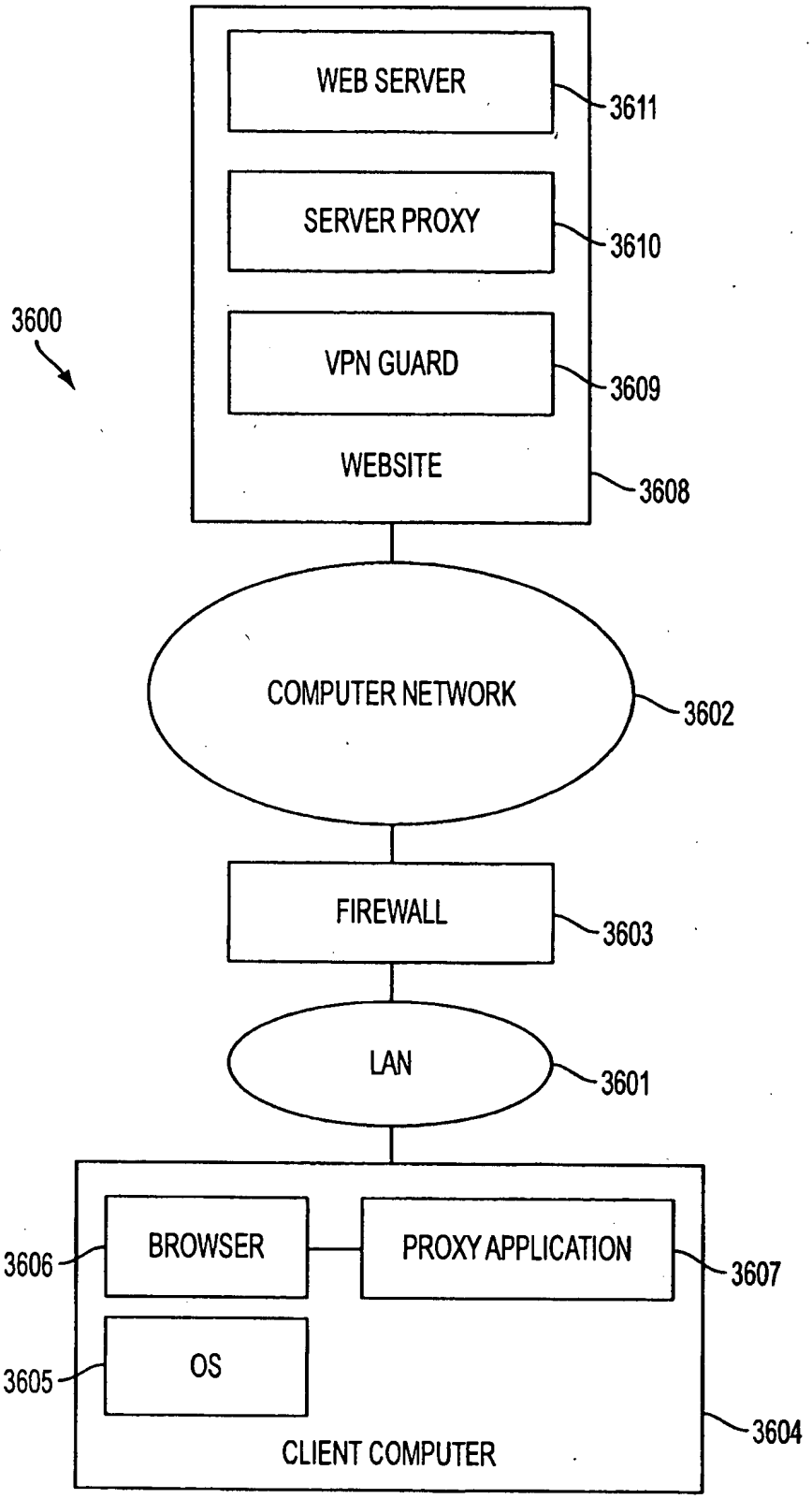

3600
WEB SERVER
3611
SERVER PROXY
3610
VPN GUARD
3609
WEBSITE
3608
COMPUTER NETWORK
3602
FIREWALL
3603
LAN
3601
BROWSER
PROXY APPLICATION
3607
3606
OS
3605
CLIENT COMPUTER
3604

FIG. 36

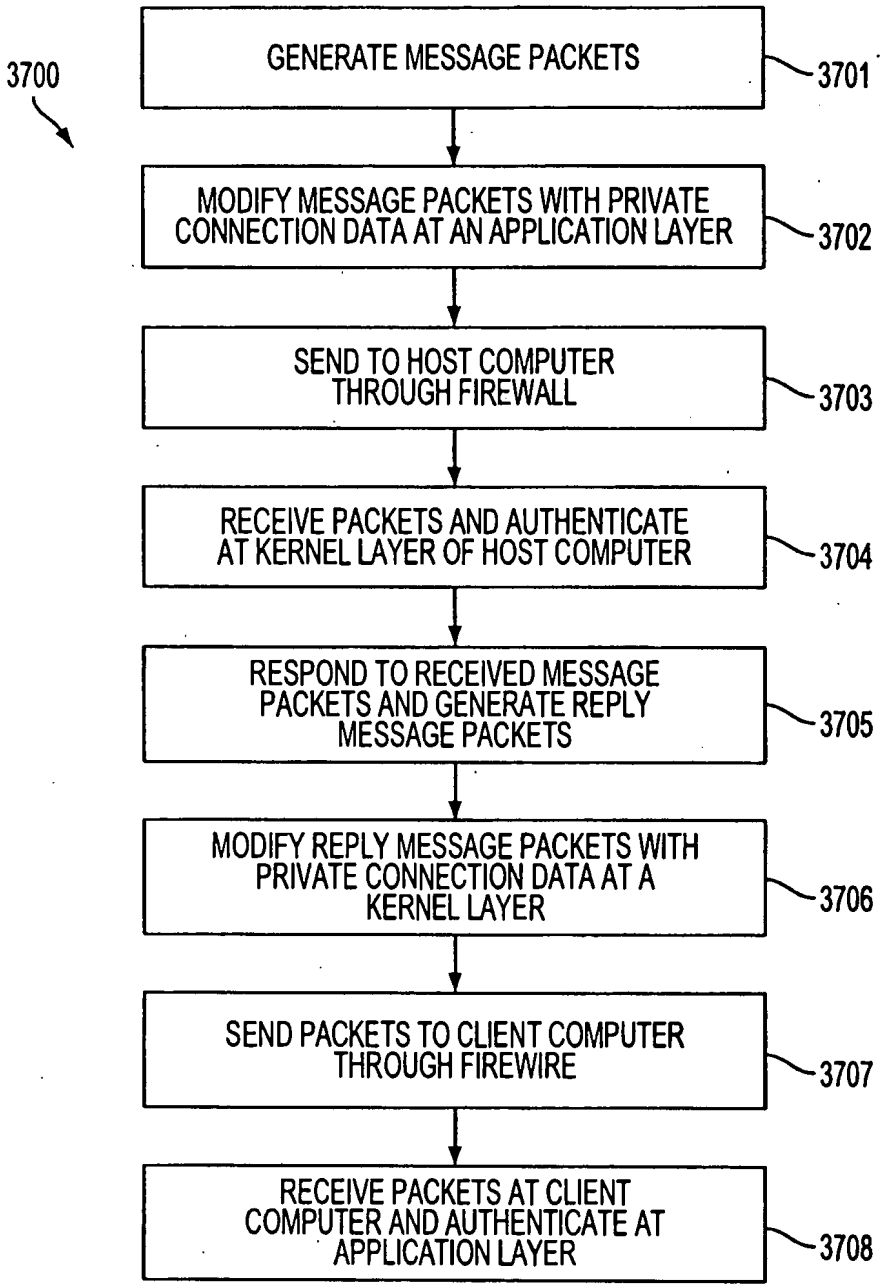

3700
GENERATE MESSAGE PACKETS
3701
MODIFY MESSAGE PACKETS WITH PRIVATE CONNECTION DATA AT AN APPLICATION LAYER
3702
SEND TO HOST COMPUTER THROUGH FIREWALL
3703
RECEIVE PACKETS AND AUTHENTICATE AT KERNEL LAYER OF HOST COMPUTER
3704
RESPOND TO RECEIVED MESSAGE PACKETS AND GENERATE REPLY MESSAGE PACKETS
3705
MODIFY REPLY MESSAGE PACKETS WITH PRIVATE CONNECTION DATA AT A KERNEL LAYER
3706
SEND PACKETS TO CLIENT COMPUTER THROUGH FIREWIRE
3707
RECEIVE PACKETS AT CLIENT COMPUTER AND AUTHENTICATE AT APPLICATION LAYER
3708

FIG. 37

PTO/SB/14 (08-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Victor		Larson	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Fairfax	State/Province	VA	Country of Residence i	US

Citizenship under 37 CFR 1.41(b) i US

Mailing Address of Applicant:

Address 1	12026 Lisa Marie Court		
Address 2			
City	Fairfax	State/Province	VA
Postal Code	22033	Country i	US

Applicant 2

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Robert	Durham	Short	III

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Leesburg	State/Province	VA	Country of Residence i	US

Citizenship under 37 CFR 1.41(b) i US

Mailing Address of Applicant:

Address 1	38710 Goose Creek Lane		
Address 2			
City	Leesburg	State/Province	VA
Postal Code	20175	Country i	US

Applicant 3

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Edmund	Colby	Munger	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Crownsville	State/Province	MD	Country of Residence i	US

PTO/SB/14 (06-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	

Citizenship under 37 CFR 1.41(b) i	US				
Mailing Address of Applicant:					
Address 1	1101 Opaca Court				
Address 2					
City	Crownsville	**State/Province**	MD		
Postal Code	21032	**Country**i	US		

Applicant 4

Applicant Authority (•) Inventor ( ) Legal Representative under 35 U.S.C. 117 ( ) Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Michael		Williamson	

Residence Information (Select One) (•) US Residency ( ) Non US Residency ( ) Active US Military Service

City	South Riding	**State/Province**	VA	**Country of Residence** i	US
Citizenship under 37 CFR 1.41(b) i	US				
Mailing Address of Applicant:					
Address 1	26203 Ocala Circle				
Address 2					
City	South Riding	**State/Province**	VA		
Postal Code	20152	**Country**i	US		

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. [Add]

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	22907		
Email Address		[Add Email]	[Remove Email]

Application Information:

Title of the Invention	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK		
Attorney Docket Number		**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)		**Suggested Figure for Publication (if any)**	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not been and will not be the subject of an application filed in another country, or under a multilateral agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ US Representative (37 CFR 11.9)
Customer Number	22907		

Domestic Priority Information:

This section allows for the applicant to claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c). Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
	Continuation of	10702486	2003-11-07	7188180	2007-03-06

Prior Application Status	Pending			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	
10702486	Division of	09558209	2000-04-26	

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
09558209	Continuation in part of	09504783	2000-02-15	6502135	2002-12-31

Prior Application Status	Pending			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	
09504783	Continuation in part of	09429643	1999-10-29	

Prior Application Status	Expired			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	
09429643	non provisional of	60106261	1998-10-30	

Additional Domestic Priority Data may be generated within this form by selecting the **Add** button.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK	

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			(•) Yes ( ) No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1

If the Assignee is an Organization check here. [X]

Organization Name	Science Applications International Corporation

Mailing Address Information:

Address 1	10260 Campus Point Drive		
Address 2			
City	San Diego	**State/Province**	CA
Country [i] US		Postal Code	92121
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button.

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Steve Chang/			Date (YYYY-MM-DD)	2007-02-27
First Name	Steve	Last Name	Chang	Registration Number	42402

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Method for Establishing Secure Communication Link Between Computers of Virtual Private Network
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Steve S. Chang/Tarsha Howard
Attorney Docket Number:	

Filed as Large Entity

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	300	300
Utility Search Fee	1111	1	500	500
Utility Examination Fee	1311	1	200	200
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	1000

PTO/SB/21 (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	3

Application Number	11/679,416
Filing Date	February 27, 2007
First Named Inventor	Victor Larson et al.
Art Unit	2153
Examiner Name	-
Attorney Docket Number	077580-0015 (VRNK-1CP2DVCN)

ENCLOSURES (*Check all that apply*)

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☑ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☑ Other Enclosure(s) (please Identify below):
  Statement under 37 CFR 3.73(b)

Remarks

There are no fees believed to be due with the filing of this paper. However, the commissioner is hereby authorized to charge any fees that may be required to our deposit account No. 50-1133.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDermott, Will & Emery LLP. (Customer No. 23,630)		
Signature	/Atabak R. Royaee/		
Printed name	Atabak R. Royaee		
Date	June 29, 2007	Reg. No.	59,037

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	/Atabak R. Royaee/		
Typed or printed name	Atabak R. Royaee	Date	59,037

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: 077580-0015

PTO/SB/82 (01-06)
Approved for use through 12/31/2006. OMB 0651-0035
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REVOCATION OF POWER OF ATTORNEY WITH NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	11/679,416
Filing Date	February 27, 2007
First Named Inventor	Victor LARSON et al.
Art Unit	2153
Examiner Name	
Attorney Docket Number	077580-0015 (VBNK-1CP2DVCN)

I hereby revoke all previous powers of attorney given in the above-identified application:

☐ A Power of Attorney is submitted herewith.

OR

☑ I hereby appoint the practitioners associated with the Customer Number: 23,630

☑ Please change the correspondence address for the above-identified application to:

☑ The address associated with Customer Number: 23,630

OR

☐ Firm *or* Individual Name					
Address					
City		State		ZIP	
Country					
Telephone		Email			

I am the:

☐ Applicant/Inventor.

☑ Assignee of record of the entire interest. See 37 CFR 3.71
Statement under 37CFR 3.73(b) is enclosed. (Form PTO/SB/96)

SIGNATURE of Applicant or Assignee of Record

Signature			
Name	Roger T. Carson		
Date	6/19/12	Telephone	831.938.1200

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.36. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending on the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: 077580-0015

PTO/SB/96 (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: VirnetX, Inc.

Application No./Patent No.: 11/679,416 Filed/Issue Date: February 27, 2007

Entitled: Method For Establishing Secure Communication Link Between Computers Of Virtual Private Network

VirnetX, Inc. , a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☑ the assignee of the entire right, title, and interest; or

2. ☐ an assignee of less than the entire right, title and interest
The extent (by percentage) of its ownership interest is _____ %

in the patent application/patent identified above by virtue of either:

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at _____, Frame _____, or a true copy of the original is attached.

OR

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Larson et al. (Inventors) To: Science Applications International Corporation
The document was recorded in the United States Patent and Trademark Office at
Reel 019463, Frame 0762, or for which a copy thereof is attached.

2. From: Science Applications International Corporation To: VirnetX, Inc.
The document was recorded in the United States Patent and Trademark Office at
Reel 019464, Frame 0133, or for which a copy thereof is attached.

3. From: N/A To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet.

☐ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Signature — Date: 6/19/07

Printed or Typed Name: Kenneth Larson — Telephone number: 831.458.8200

Title: President

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	1927672
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	22907
Filer:	Atabak R Royaee
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	29-JUN-2007
Filing Date:	
Time Stamp:	16:51:58
Application Type:	Utility

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	Transmittal.pdf	47482	no	1
Warnings:					

Information:					
2	Power of Attorney	SB82and73bStatement.pdf	425778	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	473260	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
11/679,416	02/27/2007	2157	1000	077580-0015 (VBNK-1CP2DVC	1	1

CONFIRMATION NO. 3528

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA02109-1775

FILING RECEIPT

Date Mailed: 09/21/2007

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Filing Receipt Corrections. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Victor Larson, Fairfax, VA;
Robert Dunham Short III, Leesburg, VA;
Edmund Colby Munger, Crownsville, MD;
Michael Williamson, South Riding, VA;

Assignment For Published Patent Application

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, San Diego, CA

Power of Attorney: The patent practitioners associated with Customer Number 23630

Domestic Priority data as claimed by applicant

This application is a CON of 10/702,486 11/07/2003 PAT 7,188,180
which is a DIV of 09/558,209 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6,502,135
which is a CIP of 09/429,643 10/29/1999 PAT 7,010,604
which claims benefit of 60/106,261 10/30/1998

Foreign Applications

If Required, Foreign Filing License Granted: 09/20/2007

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US11/679,416**

Projected Publication Date: 01/03/2008

Non-Publication Request: No

Early Publication Request: No

Title

METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Preliminary Class

709

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to

revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/679,416	02/27/2007	Victor Larson	077580-0015 (VBNK-1CP2DVC

CONFIRMATION NO. 3528

OC000000025951695

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775

Date Mailed: 09/21/2007

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/29/2007.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199
OFFICE COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/679,416	02/27/2007	Victor Larson	

CONFIRMATION NO. 3528

OC000000025951644

22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

Date Mailed: 09/21/2007

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/29/2007.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199
OFFICE COPY

McDermott
Will&Emery

RECEIVED
CENTRAL FAX CENTER
OCT 04 2007

Boston Brussels Chicago Düsseldorf London Los Angeles Miami Munich
New York Orange County Rome San Diego Silicon Valley Washington, D.C.
Strategic alliance with MWE China Law Offices (Shanghai)

FACSIMILE

Date: October 4, 2007 **Time Sent:**

To:	Company:	Facsimile No:	Telephone No:
Commissioner for Patents	U.S. Patent and Trademark Office	1.571.273.8300	

From:	Toby H. Kusmer, P.C.	*Direct Phone:*	617.535.4065
E-Mail:	tkusmer@mwe.com	*Direct Fax:*	617.535.3800
Sent By:	Cynthia Joseph	*Direct Phone:*	617.535.4111
Client/Matter/Tkpr:	77580-015/5496	*Original to Follow by Mail:*	No
		Number of Pages, Including Cover:	2

Re: In re Application of: Victor Larson, et al.
Serial No.: 11/679,416
Filing Date: February 27, 2007
Title: Method For Establishing Secure Communication Link Between Computers Of Virtual Private Network
Docket No.: 77580-015 (VRNK-1CP2DVCN)

Message:

Please enter the attached Status Inquiry.

The information contained in this facsimile message is legally privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copy of this facsimile is strictly prohibited. If you have received this facsimile in error, please notify us immediately by telephone and return the original message to us at the below address by mail. Thank you.

IF YOU DO NOT RECEIVE ALL OF THE PAGES, PLEASE CALL AS SOON AS POSSIBLE.

Main Facsimile: 617.535.3800 Facsimile Operator: 617.535.4000

U.S. practice conducted through McDermott Will & Emery LLP.
28 State Street Boston, Massachusetts 02109-1775 Telephone: 617.535.4000

RECEIVED
CENTRAL FAX CENTER

OCT 0 4 2007

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Victor Larson, et al.
Serial No:	11/679,416
Filing Date:	February 27, 2007
Title:	Method For Establishing Secure Communication Link Between Computers Of Virtual Private Network
Group Art Unit:	2157
Confirmation No.:	3528
Docket No:	77580-015 (VRNK-1CP2DVCN)

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

STATUS INQUIRY

Applicants make a request as to the status of the above-identified application and for information as to when they might expect to receive an Office Action.

Respectfully submitted,

Toby H. Kusmer, P.C.
Registration Number 26,418
McDermott Will & Emery LLP
28 State Street
Boston, Massachusetts 02109-1775
Telephone: (617) 535-4065
Facsimile: (617) 535-3800
e-mail: tkusmer@mwe.com

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being facsimile transmitted, via Facsimile No. 571.273.8300, to the U.S. Patent and Trademark Office and is addressed to: Commissioner For Patents, P. O. Box 1450, Alexander, VA 22313-1450 on the date indicated below.

Date: October 4, 2007

Cynthia Joseph

BST99 1553736-1.077580.0015

JFW

OIPE
NOV 13 2007
PATENT & TRADEMARK OFFICE

Docket No.: 077580-0015 (VRNK-1CP2DVCN) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Larson et al.
Appl. No.	:	11/679,416
Filed	:	February 27, 2007
Title	:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
Grp./A.U.	:	2131
Examiner:	:	Not Yet Assigned

Customer No.: 23,630
Confirmation No.: 3528

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First-Class Mail under 37 CFR 1.8(a) in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on November 9, 2007.

Cynthia Joseph

INFORMATION DISCLOSURE STATEMENT

Mail Stop IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached form PTO-1449. It is respectfully requested that the documents be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is being filed before the receipt of a First Office Action on the merits for above-referenced application; therefore, no fees is believed to be due with the filing of this paper.

References B1-B6, B8, B11-B13, B16-B17, C1-C17, C20-C24, and C29-C30 were cited by or submitted to the U.S. Patent and Trademark Office in parent application Serial No. 10/702,486, filed November 7, 2003, now U.S. Patent No. 7,188,180, which is relied upon for an earlier filing date under 35 USC 120. In accordance with 37 CFR 1.98(d), copies of these references are not attached. Applicants will be pleased to provide copies of the reference if requested by the Examiner.

This Statement is not to be interpreted as a representation that the cited publications are material, that an exhaustive search has been conducted, or that no other relevant information exists. Nor shall the citation of any publication herein be construed *per se* as a representation that such publication is prior art. Moreover, the Applicant understands that the Examiner will make an independent evaluation of the cited publications.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Atabak R. Royaee
Registration No. 59,037

28 State Street
Boston, MA 02109
Phone: 617-535-4108
Facsimile: 617-535-3800
Date: November 9, 2007

Please recognize our Customer No. 23630 as our correspondence address.

OIPE IAP95 NOV 13 2007 PATENT & TRADEMARK OFFICE

INFORMATION DISCLOSURE CITATION IN AN APPLICATION

(PTO-1449)

ATTY. DOCKET NO.	SERIAL NO.
077580-0015	**11/679,416**
APPLICANT: **Larson et al.**	
FILING DATE: **Feb. 27, 2007**	GROUP: **2131**

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	US	4,933,846 A	6/12/1990	Humphrey et al.	
	A2	US	4,988,990 A	1/29/1991	Warrior	
	A3	US	5,276,735 A	1/4/1994	Boebert et al	
	A4	US	5,311,593 A	5/10/1994	Carmi	
	A5	US	5,329,521 A	7/12/1994	Walsh et al.	
	A6	US	5,341,426 A	8/23/1994	Barney et al.	
	A7	US	5,367,643 A	11/22/1994	Chang et al	
	A8	US	5,559,883 A	9/24/1996	Williams	
	A9	US	5,561,669 A	10/1/1996	Lenney et al	
	A10	US	5,588,060 A	12/24/1996	Aziz	
	A11	US	5,625,626 A	4/29/1997	Umekita	
	A12	US	5,654,695 A	8/5/1997	Olnowich et al	
	A13	US	5,682,480 A	10/28/1997	Nakagawa	
	A14	US	5,689,566 A	11/18/1997	Nguyen	
	A15	US	5,740,375 A	4/14/1998	Dunne et al.	
	A16	US	5,774,660 A	6/30/1998	Brendel et al	
	A17	US	5,787,172 A	7/28/1998	Arnold	
	A18	US	5,796,942 A	8/18/1998	Esbensen	
	A19	US	5,805,801 A	9/8/1998	Holloway et al.	
	A20	US	5,842,040 A	11/24/1998	Hughes et al.	
	A21	US	5,845,091 A	12/1/1998	Dunne et al.	
	A22	US	5,867,650 A	2/2/1998	Osterman	
	A23	US	5,870,610 A	2/9/1999	Beyda et al.	
	A24	US	5,878,231 A	5/2/1999	Baehr et al	
	A25	US	5,892,903 A	4/6/1999	Klaus	
	A26	US	5,898,830 A	4/27/1999	Wesinger, Jr. et al.	
	A27	US	5,905,859 A	5/18/1999	Holloway et al.	
	A28	US	5,918,019 A	6/29/1999	Valencia	
	A29	US	5,996,016 A	11/30/1999	Thalheimer et al.	
	A30	US	6,006,259 A	12/21/1999	Adelman et al.	
	A31	US	6,006,272 A	12/21/1999	Aravamudan et al	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)	ATTY. DOCKET NO. **077580-0015**	SERIAL NO. **11/679,416**
	APPLICANT **Larson et al.**	
	FILING DATE **Feb. 27, 2007**	GROUP **2131**

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A32	US 6,016,318 A	1/18/2000	Tomoike	
	A33	US 6,016,512	1/18/2000	Huitema	
	A34	US 6,041,342 A	3/21/2000	Yamaguchi	
	A35	US 6,052,788 A	4/18/2000	Wesinger, Jr. et al.	
	A36	US 6,055,574 A	4/25/2000	Smorodinsky et al.	
	A37	US 6,061,736 A	5/9/2000	Rochberger et al	
	A38	US 6,079,020 A	6/20/2000	Liu	
	A39	US 6,092,200 A	7/18/2000	Muniyappa et al.	
	A40	US 6,119,171 A	9/12/2000	Alkhatib	
	A41	US 6,119,234 A	9/12/2000	Aziz et al.	
	A42	US 6,147,976 A	11/14/2000	Shand et al.	
	A43	US 6,157,957 A	12/5/2000	Berthaud	
	A44	US 6,158,011 A	12/5/2000	Chen et al.	
	A45	US 6,168,409 B1	1/2/2001	Fare	
	A46	US 6,175,867 B1	1/16/2001	Taghadoss	
	A47	US 6,178,409 B1	1/23/2001	Weber et al.	
	A48	US 6,178,505 B1	1/23/2001	Schneider et al	
	A49	US 6,179,102 B1	1/30/2001	Weber, et al.	
	A50	US 6,222,842 B1	4/24/2001	Sasyan et al.	
	A51	US 6,226,751 B1	5/1/2001	Arrow et al	
	A52	US 6,233,618 B1	5/15/2001	Shannon	
	A53	US 6,243,360 B1	6/5/2001	Basilico	
	A54	US 6,243,749 B1	6/5/2001	Sitaraman et al.	
	A55	US 6,243,754 B1	6/5/2001	Guerin et al	
	A56	US 6,256,671 B1	7/3/2001	Strentzsch et al.	
	A57	US 6,263,445 B1	7/17/2001	Blumenau	
	A58	US 6,286,047 B1	9/4/2001	Ramanathan et al	
	A59	US 6,301,223 B1	10/9/2001	Hrastar et al	
	A60	US 6,308,274 B1	10/23/2001	Swift	
	A61	US 6,311,207 B1	10/30/2001	Mighdoll et al	
	A62	US 6,324,161 B1	11/27/2001	Kirch	
	A63	US 6,330,562 B1	12/11/2001	Boden et al.	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 151

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)	ATTY. DOCKET NO. **077580-0015**	SERIAL NO. **11/679,416**
	APPLICANT **Larson et al.**	
	FILING DATE **Feb. 27, 2007**	GROUP **2131**

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A64	US	6,332,158 B1	12/18/2001	Risley et al.	
	A65	US	6,353,614 B1	3/5/2002	Borella et al.	
	A66	US	6,430,155 B1	8/6/2002	Davie et al	
	A67	US	6,430,610 B1	8/6/2002	Carter	
	A68	US	6,487,598 Bi	11/26/2002	Valencia	
	A69	US	6,502,135 B1	12/31/2002	Munger et al	
	A70	US	6,505,232 B1	1/7/2003	Mighdoll et al	
	A71	US	6,510,154 B1	1/21/2003	Mayes et al	
	A72	US	6,549,516 B1	4/15/2003	Albert et al	
	A73	US	6,557,037 B1	4/29/2007	Provino	
	A74	US	6,571,296 B1	5/27/2002	Dillon	
	A75	US	6,571,338 B1	5/27/2003	Shaio et al.	
	A76	US	6,581,166 B1	7/17/2003	Hirst et al.	
	A77	US	6,618,761 B2	9/9/2003	Munger et al.	
	A78	US	6,671,702 B2	12/30/2003	Kruglikov et al	
	A79	US	6,687,551 B1	2/3/2004	Steindl	
	A80	US	6,714,970 B1	3/30/2004	Fiveash et al.	
	A81	US	6,717,949 B1	4/6/2004	Boden et al.	
	A82	US	6,760,766 B1	7/6/2004	Sahlqvist	
	A83	US	6,826,616 B2	11/30/2004	Larson et al.	
	A84	US	6,839,759 B2	1/4/2005	Larson et al.	
	A85	US	7,010,604 B1	3/7/2006	Munger et al.	
	A86	US	7,133,930 B2	11/7/2006	Munger et al.	
	A87	US	7,188,180 B2	3/6/2007	Larson et al.	
	A88	US	7,197,563 B2	3/27/2007	Sheymov et al.	
	A89	US	2002/0004898 Al	1/10/2002	Droge	
	A90	US	2005/0055306 A1	3/10/2005	Miller et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 152

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)	ATTY. DOCKET NO. 077580-0015	SERIAL NO. 11/679,416
	APPLICANT Larson et al.	
	FILING DATE Feb. 27, 2007	GROUP 2131

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number 4-Kind Codes (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	B1	EP 0 814 589	12/29/1997	Harwood et al.			
	B2	EP 0 838 930	4/29/1998	Alden et al.			
	B3	EP 0 858 189	8/12/1998	Maciel et al.			
	B4	DE 199 24 575	12/2/1999	Provino et al.			
	B5	GB 2 317 792	4/1/1998	Minear et al.			
	B6	GB 2 334 181 A	8/11/1999	Noblet			
	B7	EP 836306A1	4/15/1998	Sasyan et al.			
	B8	WO 9827783 A	6/25/1998	Tello et al.			
	B9	WO 00/17775	3/30/2000	Miller et al.			
	B10	WO 00/70458	11/23/2000	Sheymov			
	B11	WO 01 50688	7/12/2001	Kriens			
	B12	WO 98 55930	12/10/1998	Tang			
	B13	WO 98 59470	12/30/1998	Kanter et al.			
	B14	WO 98/27783	6/25/1998	Tello et al.			
	B16	WO 99 38081	7/29/1999	Paulsen et al.			
	B17	WO 99 48303	9/23/1999	Cox et al.			

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1	Alan 0. Frier et al., "The SSL Protocol Version 3.0", Nov. 18, 1996, printed from http://www.netscape.com/eng/ss13/ draft302.txt on Feb. 4, 2002, 56 pages.	
	C2	August Bequai, "Balancing Legal Concerns Over Crime and Security in Cyberspace", Computer & Security, vol. 17, No. 4, 1998, pp. 293–298.	
	C3	D. B. Chapman et al., "Building Internet Firewalls", Nov. 1995, pp. 278–375.	
	C4	D. Clark, "US Calls for Private Domain–Name System", Computer, IEEE Computer Society, Aug. 1, 1998, pp. 22–25.	
	C5	Davila J et al, "Implementation of Virtual Private Networks at the Transport Layer", Information Security, Second International Work-shop, ISW'99. Proceedings (Lecture Springer-Verlag Berlin, Germany, [Online] 1999, pp. 85-102, XP002399276, ISBN 3-540-66695-B, retrieved from the Internet: URL: http://www. springerlink.com/content/4uac0tb0hecoma89/fulltext.pdf> (Abstract).	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)	ATTY. DOCKET NO. **077580-0015**	SERIAL NO. **11/679,416**
	APPLICANT **Larson et al.**	
	FILING DATE **Feb. 27, 2007**	GROUP **2131**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C6	Dolev, Shlomi and Ostrovsky, Rafil, "Efficient Anonymous Multicast and Reception" (Extended Abstract), 16 pages.	
	C7	Donald E. Eastlake, 3rd, "Domain Name System Security Extensions", INTERNET DRAFT, Apr. 1998, pp. 1-51.	
	C8	F. Halsall, "Data Communications, Computer Networks and Open Systems", Chapter 4, Protocol Basics, 1996, pp. 198–203.	
	C9	Fasbender, Kesdogan, and Kubitz: "Variable and Scalable Security" Protection of Location Information in Mobile IP, IEEE publication, 1996, pp. 963-967.	
	C10	Glossary for the Linux FreeS/WAN project, printed from http://liberty.freeswan.org/freeswan_trees/freeswan-1.3/ doc/glossary.html on Feb. 21, 2002, 25 pages.	
	C11	J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan _trees/freeswan-1.3/doc/rationale.html on Feb. 21, 2002, 4 pages.	
	C12	James E. Bellaire, "New Statement of Rules—Naming Internet Domains", Internet Newsgroup, Jul. 30, 1995, 1 page.	
	C13	Jim Jones et al., "Distributed Denial of Service Attacks: Defenses", Global Integrity Corporation, 2000, pp. 1–14.	
	C14	Laurie Wells (LANCASTERBIBELMAIL MSN COM); "Subject: Security Icon" USENET Newsgroup, Oct. 19, 1998, XP002200606, 1 page.	
	C15	Linux FreeS/WAN Index File, printed from http://liberty.freewan.org/freeswan_trees/freeswan-1.3/doc/ on Feb. 21, 2002, 3 Pages.	
	C16	P. Srisuresh et al., "DNS extensions to Network address Translators (DNS_ALG)", Internet Draft, Jul. 1998, pp. 1–27.	
	C17	Reiter, Michael K. and Rubin, Aviel D. (AT&T Labs—Research), "Crowds: Anonymity for Web Transactions", pp. 1-23.	
	C18	RFC 2401 (dated Nov. 1998) Security Architecture for the Internet Protocol (RTP)	
	C19	RFC 2543-SIP (dated March 1999): Session Initiation Protocol (SIP or SIPS)	
	C20	Rich Winkel, "CAQ: Networking With Spooks: The NET & The Control Of Information", Internet Newsgroup, Jun. 21, 1997, 4 pages.	
	C21	Rubin, Aviel D., Geer, Daniel, and Ranum, Marcus J. (Wiley Computer Publishing), "Web Security Sourcebook", pp. 82-94.	
	C22	Search Report (dated Aug. 20, 2002), International Application No. PCT/US01/04340.	
	C23	Search Report (dated Aug. 23, 2002), International Application No. PCT/US01/13260.	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 154

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)	ATTY. DOCKET NO. **077580-0015**	SERIAL NO. **11/679,416**
	APPLICANT **Larson et al.**	
	FILING DATE **Feb. 27, 2007**	GROUP **2131**

U.S. PATENT DOCUMENTS

* EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C24	Search Report (dated Oct. 7, 2002), International Application No. PCT/US01/13261.	
	C25	Search Report, IPER (dataed Nov. 13, 2002), International Applicatoin No. PCT/US01/04340.	
	C26	Search Report, IPER (dated Feb. 06, 2002), International Application No. PCT/US01/13261.	
	C27	Search Report, IPER (dated Jan. 14, 2003), International Application No. PCT/US01/13260.	
	C28	Shankar, A.U. "A verified sliding window protocol with variable flow control". Proceedings of ACM SIGCOMM conferece on Communications architectures & protocols. pp. 84-91, ACM Press, NY,NY 1986.	
	C29	Shree Murthy et al., "Congestion–Oriented Shortest Multi-path Routing", Proceedings of IEEE INFOCOM, 1996, pp. 1028–1036.	
	C30	W. Stallings, "Cryptography And Network Security", 2nd, Edition, Chapter 13, IP Security, Jun. 8, 1998, pp. 399–440.	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 836 306 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
15.04.1998 Bulletin 1998/16

(51) Int. Cl.[6]: **H04L 29/06**, H04Q 11/04

(21) Application number: **96410106.7**

(22) Date of filing: **10.10.1996**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV SI

(71) Applicant:
Hewlett-Packard Company
Palo Alto, California 94304 (US)

(72) Inventors:
- **Sasyan, Serge**
  38170 Seyssinet (FR)
- **Roger, Denis**
  38760 Varces (FR)
- **Terrasse, Denis**
  38320 Eybens (FR)

(74) Representative:
Squibbs, Robert Francis
Intellectual Property Section,
Legal Department,
Hewlett-Packard France,
Etablissements de Grenoble
F-38053 Grenoble Cédex 9 (FR)

Remarks:
The application is published incomplete as filed (Article 93 (2) EPC). A claim No.7 is missing.

(54) System providing for multiple virtual circuits between two network entities

(57) Computers sending IP datagrams over an ATM network are generally capable of operating multiple simultaneous virtual circuits over the network. However, in doing so, they normally only set up one virtual circuit to each destination IP address so that in order to test the simultaneous operation of N virtual circuits by a computer under test, N target computers are needed. To enable a single computer (T) to provide the destination endpoints for multiple virtual circuits (SVC) from a computer (M) under test, both computers (M,T) are allocated a plurality of virtual IP addresses ($I_{M(j)}$,$I_{T(i)}$) and the target computer (T) is additionally provided with a module running address-changing processes (70,71) that avoids the IP layers (20) of both computers from rejecting IP datagrams (25A,25B) addressed with the virtual IP addresses. As a result, each computer (M,T) can be addressed with any of a plurality of IP addresses and each will result in the creation of a respective virtual circuit (SVC) between the computers (M,T).

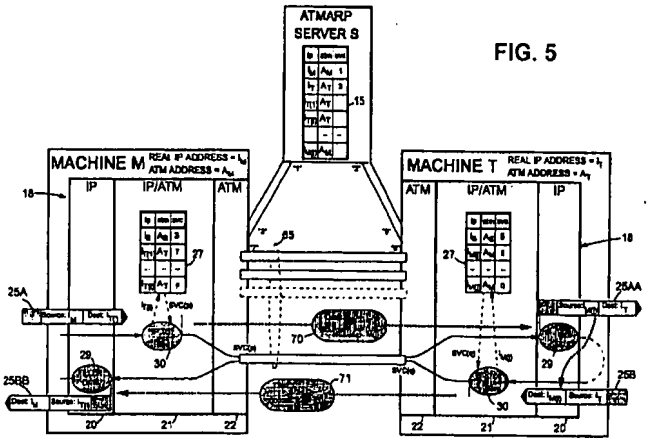


FIG. 5

EP 0 836 306 A1

Printed by Xerox (UK) Business Services
2.15.12/3.4

Description

Field of the Invention

The present invention relates to a system providing for multiple virtual circuits between two network entities for use in particular, but not exclusively, in the testing of network node apparatus providing IP messaging over an ATM network.

Background of the Invention

As is well-known, the Internet Protocol (IP) uses a scheme of IP addresses by which every connection of a node to the Internet has a unique IP address. IP addresses are high-level addresses in the sense that they are independent of the technology used for the underlying network to which a node is connected. Each node will also have a low-level, network-dependent address (often callled the MAC address) that is actually used for addressing at the network level and the IP protocol suite includes a address reolution protocol (ARP), logically positioned below the IP layer itself, that is responsible for translating between IP addresses contained in a message and the local MAC addresses.

An increasingly important technology for local area networks is ATM. ATM (Asynchronous Transfer Mode) is a multiplexing and switching technique for transferring data across a network using fixed sized cells that are synchronous in the sense that they appear strictly periodically on the physical medium. Each cell comprises a payload portion and a header, the latter including a label that associates the cell with an instance of communication between sending and receiving network end systems; this instance of communication may involve the transfer of many cells from the sending end system, possibly to multiple receiving end systems. ATM is asynchronous in the sense that cells belonging to the same instance of communication will not necessarily appear at periodic intervals.

In ATM, the labels appended to the cells are fixed-size context dependent labels, that is, they are only understandable in the light of context information already established at the interpreting network node, the label generally being replaced at one node by the label required for the next node. In other words, ATM is a virtual circuit technology requiring a set up phase for each instance of communication to establish the appropriate label knowledge at each node. Of course, to set up a desired communication, it is still necessary to identify uniquely the nodes forming the communication end points and this is achieved by using ATM addresses, generally of a significance limited to the particular ATM network concerned.

The process of sending IP messages (datagrams) over a ATM network, including the operation of the required ATM ARP system, is set out in RFC 1577 of the IETF Internet Engineering Task Force) dated January 1993. This RFC assumes an arrangement in which a sending node will only establish a single vircuit circuit to a given destination IP address (of course, this one vircuit circuit may carry multiple connections between respective pairings of high-level end points in the nodes).

Figure 1 of the accompanying drawings is a diagram illustrating the basic mechanism by which two machines M and T exchange IP datagrams over a switched virtual circuit (SVC) established across an ATM network. The machines M and T have respective IP addresses I_M and I_T and respective ATM addresses A_M and A_T; each machine knows its own addresses. An ATMARP server S knows the IP and ATM addresses of all active nodes on the network, including machines M and T; more particularly, server S maintains an ARP table 15 associating the IP address of each node with its ATM address. The server S maintains open a respective SVC (switched virtual circuit) to each active node and the identity of this SVC is held in the ARP table 15; thus, in the Figure 1 example, the server S is in communication with machine M over an SVC identified as SVC "1" at the server, and the server S is in communication with machine T over an SVC identified as SVC "2" at the server S. At machines M and T these virtual circuits are independently identified - thus at machine M its SVC to the server S is identified as SVC "3" whilst at machine T its SVC to the server S is identified as SVC "5".

The communications interface 18 in each of the machines M and T comprises three main layers, namely: an IP layer 20 responsible for forming IP datagrams (including source and destination IP addresses) for transmission ad for filtering incoming datagrams; an intermediate IP/ATM layer 21 for determining the SVC corresponding to the destination IP address of an outgoing datagram; and an ATM layer 22, including the low-level network interface hardware, for sending and receiving datagrams packaged in ATM cells over SVCs.

The IP/ATMlayer 21 maintains an ARP cache table 27 which like the table 15 of the server S contains associations between IP address, ATM address and SVC. Thus, table 27 of machine M contains an entry of the IP address I_S, ATM address A_S, and SVC identity "3" for the server S, and similarly, table 27 of machine T contains an entry of the IP address I_S, ATM address A_S, and SVC identity "5" for the server S. The cache table 27 only holds information relevant to current SVCs of the machine concerned so that during the initial establishment of a SVC to a new destination, the cache table must be updated with relevant information from the ATMARP server S; this general process will be described in more detail hereinafter with reference to Figure 2. For the present, it will be assumed that an SVC has already been established between machines M and T and that the cache tables contain the relevant information (in particular, cache table 27 of machine M contains an entry with the IP address I_T, ATM address A_T, and SVC identity "4" for machine T, and cache table

Petitioner Apple Inc. - Exhibit 1026, p. 157

27 of machine T contains an entry with the IP address I_M, ATM address A_M, and SVC identity "9" for machine M).

Considering now the case of a high-level application in machine M wanting to send a message to machine T, this application passes the message to the IP layer 20 together with the destination IP address I_T. IP layer 20 packages the message in one (or more) datagrams 25A with a destination IP address of I_T and source I_P address of I_M. Datagram 25A is then passed to the IP/ATM layer 21 which executes an IP-to-SVC lookup task 30 to determine from table 27 the SVC to be used for sending the datagram to its destination address I_T; in the present case, table 27 returns the SVC identity "4" and the layer 21 passes this identity together with the datagram 25A to the ATM layer 22 which then sends the datagram in ATM cells on SVC "4". The datagram is in due course received by machine T and passed up by layers 22 and 21 to the IP layer 20 where a filtering task 29 determines from the datagram destination address that the datagram is indeed intended for machine T; the contents of the datagram are then passed to the relevant high-level application. In the present example, this high-level application produces a reply message which it passes to the IP layer 20 together with the required return address, namely the source IP address in the received datagram 25A. IP layer 20 generates datagram 25B with the received return address as the destination address, the IP address I_T of machine T being included as the source address. The datagram 25B is passed to IP/ATM layer 21 where IP-to-SVC lookup task 30 determines from cache table 27 that the required destination can be reached over SVC "9". This information together with datagram 25B is then passed to ATM layer 22 which transmits the datagram in ATM cells over SVC "9" to machine M. When the datagram is received at machine M it is passed up to the IP layer 20 where it is filtered by task 29 and its contents then passed on to the relevant high-level application.

Figure 2 of the accompanying drawings illustrates in more detail the functioning of the IP/ATM layers 21 of machines M and T in respect of datagram transmission from machine M to machine T, it being appreciated that the roles of the two layers 21 are reversed for transmission in the opposite direction. More particularly, upon the IP-to-SVC lookup task 30 being requested to send a datagram to IP address I_T, it first carries out a check of the cache table 27 (step 31) to determine if there is an existing entry for I_T (and thus an SVC, assuming that entries are only maintained whilst an SVC exists). Step 32 checks the result of this lookup - if an SVC already exists (in this case, SVC "4"), then step 39 is executed in which the datagram is passed together with the identity of the relevant SVC to the ATM layer 22; however, if the lookup was unsuccessful, task 30 executes steps 33 to 38 to set up an SVC to destination I_T before executing step 39.

The first step 33 of the setup process involves the sending of an ARP request to the ATMARP server S over the relevant SVC requesting the ATM address corresponding to I_T. Server responds with ATM address A_T which is received by task 30 at step 34.

Task 30 now updates the cache table 27 with the IP address I_T and ATM address A_T (step 35). Next, task 30 requests (step 36) the ATM layer 22 to establish a new SVC to ATM address A_T and this initiates an SVC setup process 28 which may be executed in any appropriate manner and will not be described in detail herein. In due course, process 28 returns the identity of the SVC that has been set up to A_T (in this case, SVC "4"), this identity being received at step 37 of task 30. Finally, cache table 30 is updated at step 38 by adding the SVC identity ("4") to the entry already containing I_T and A_T.

In machine T, the setup of the new SVC to the machine from machine M is handled by the setup process 28 of machine T. The process 28 informs the IP/ATM layer that a new SVC has been setup and this triggers execution of an update task 40 to update the cache table 27 of machine T. More particularly, on the new SVC indication being received (step 41), a first update step 42 is carried out to add an entry to the table confining the identity of the new SVC (in the present example "9"), and the ATM address A_M of the node at the other end of the SVC; at this stage, the corresponding IP address is not known to machine T. In order to obtain this IP address, an inverse ARP request is now made to machine M (step 43). In due course a response is received (step 44) containing the IP address of machine M. The cache table 27 is then updated at step 45 with the IP address I_M of machine M and the IP/ATM layer is now ready to effect IP-to-SVC translations for datagrams intended for machine M.

The inverse ARP request sent by machine T to machine M is handled by an inverse ARP task 50 that examines the request (step 51) and on finding that it contains the ATM address A_M, responds with the IP address I_M of machine M (step 52).

To facilitate explanation of the preferred embodiment of the invention hereinafter, the messages across the boundary between the IP/ATM layer 21 and the ATM layer 22 have been labelled in Figure 2 as follows where superscript "T" indicates an outgoing message (that is, from the IP/ATM layer to the ATM layer) and the superscript "R" indicates incoming messages (that is, from the ATM layer to the IP/ATM layer):

- $X1^T$ - outgoing ARP request;
- $X2^R$ - incoming ARP response;
- $X3^T$ - outgoing SVC setup request;
- $X4^R$ - incoming SVC setup done indication;
- $X5^R$ - incoming new SVC indication;
- $X6^T$ - outgoing INARP request;
- $X6^R$ - incoming INARP request;
- $X7^T$ - outgoing INARP response;
- $X8^T$ - outgoing datagram;
- $X8^R$ - incoming datagram.

Petitioner Apple Inc. - Exhibit 1026, p. 158

It will be appreciated that machines connecting to an ATM network, such as machines M and T as well as the server S, are designed to handle a large number of virtual circuits simultanteously. If in testing such a machine (machine M in the following discussion) it is desired to fully stress the machine under test, then the design limit of concurrently operating virtual circuits must be simultaneously used. However, as already indicated, current practice is that only one virtual circuit is established to each distinct IP address. As a result, since generally each machine that might be used to test machine M has only one network connection and therefore only one IP address, if machine M is designed to operate up to N virtual circuits simultaneously, then it requires N machines to test machine M. Such an arrangement is illustrated in Figure 3 where the N machines are constituted by the server S and (N-1) other machines here represented as machines T1 to T(N-1). Such an arrangement is generally impractical as N may be as high as 1024 or more.

It is an object of the present invention to provide a mechanism that enables, inter alia, the foregoing test problem to be overcome.

Summary of the Invention

According to the present invention, there is provided a system in which a plurality of entities are connected to a network ad can exchange messages across virtual circuits set up over the network between said entities, each entity having a operative high-level address on the network, and each entity comprising:

-- high-level messaging means for handling message transmission and receipt on the basis of the aforesaid high-level addresses, the high-level messaging means comprising means for including in outgoing messages the operative high-level address of the entity as a source identifier and the operative high level address of the intended recipient entity as a destination identifier, and means for filtering incoming messages according to the destination identifier contained in the message:

-- virtual-circuit means for providing virtual circuits between the entity and other entities, there being a respective virtual circuit for each different destination identifier in use, and

-- intermediate means for passing an outgoing message from the high-level messaging means to that one of the virtual circuits provided by the virtual-circuit means which corresponds to the destination identifier of the message;

characterised in that each of a first and a second one of the entities has a plurality of virtual high-level addresses associated with it that are different from the operative high-level address of the entity, the virtual high-level addresses being usable by the messaging means of the first and second entities as destination identifiers in outgoing messages; **and in that** between the intermediate means of the first and second entities, there are provided address-changing means responsive to each of at least some of the messages sent between these entities with a said virtual high-level address as its destination identifier, to change that address to the operative high-level address of the corresponding entity and to change the operative high-level address provided as the source identifier of the message into one of the said virtual high-level addresses associated with the sending entity in dependence on the virtual high-level address initially provided as the destination identifier of the same message.

By virtue of this arrangement, it is possible to establish a plurality of virtual circuits between the first and second entities by using the different virtual high-level addresses of the entities as the destination identifiers in messages exchanged between the entities, the receiving high-level adressing means accepting such messages due to the address-changing means having changed the destination identifier to the operative high-level address of the receiving entity. By also changing the source identifier, it is possible to retain in the message information sufficient to associate any reply message with a particular one of the virtual circuits established with the sending entity (in particular, the reply message can be sent back over the same virtual circuit as the message to which it is a reply - however, if desired, it is also possible to use a separate virtual circuit for the reply messages).

Preferably, the address-changing means comprises first address-changing functionality for effecting the aforesaid changes for messages sent from the first entity to the second entity, and second address-changing functionality for effecting these changes for messages sent from the second entity to the first entity, both the first and second address-changing functionalities being provided in the second entity. This configuration is well suited for testing the ability of network node apparatus to concurrently operate a plurality of virtual circuits where the network node apparatus is operative to establish a virtual circuit for each different high-level destination address being handled; more particularly, the network node apparatus serves as the aforesaid first entity, and is caused to send messages to at least some of the vial high-level addresses associated with the second entity. By placing the address-changing means in the second entity, no modifications are needed to the network node apparatus in order for it to be able to establish a plularity of virtual circuits with the second entity.

Advantageously, the address-changing means effects a predetermined transformation on the virtual high-level address forming the initial destination identifier of a said message in order to form the virtual high-level address to be used for the source identifier of that message. For example, this transformation may simply

Petitioner Apple Inc. - Exhibit 1026, p. 159

involved changing the address by one (where the address is numeric in form).

The present invention is particularly applicable to systems in which the high-level addresses are IP addresses and the network is an ATM network.

Brief Description of the Drawings

A system embodying the invention will now be described, by way of non-limiting example, with reference to the accompanying diagrammatic drawings, in which:

- **Figure 1** is a diagram of a known system for sending IP datagrams over a ATM network between two machines M and T;
- **Figure 2** is a diagram illustrating the steps carried out by the Figure 1 system in establishing a virtual circuit between machines M and T;
- **Figure 3** is a diagram of a known test arrangement for testing the ability of a machine M to concurrently operate multiple virtual circuits;
- **Figure 4** is a diagram showing a test arrangement embodying the invention for testing the ability of a machine M to concurrently operate multiple virtual circuits;
- **Figure 5** is a diagram similar to Figure 1 but showing a system embodying the invention in which multiple virtual circuits are established between machines M and T;
- **Figure 6** is a diagram illustrating the processing effected by a module VNS disposed in machine T of the Figure 5 system when machine M initiates the opening of a new virtual circuit between machines M and T; and
- **Figure 7** is a diagram illustrating the processing effected by a module VNS disposed in machine T of the Figure 5 system when machine T initiates the opening of a new virtual circuit between machines M and T.

Best Mode of Carrying Out the Invention

The embodiment of the invention now to be described provides a system in which it is possible to establish a plurality of SVCs (switched virtual circuits) across an ATM network for the exchange of IP datagrams between two machines M and T whereby it is possible to test the ability of machine M to concurrently operate a plurality of virtual circuits without needing to provide a respective destination machine for each SVC operated by machine M. The overall test arrangement is illustrated in Figure 4 where machine M operates N SVCs over ATM network 10, one SVC being with ATMARP server S and (N-1) SVCs being with machine T. According to the preferred embodiment, the establishment of multiple concurrent SVCs between machine M and T is effected without modification to machine M.

Figure 5 shows a system embodying the present invention, this system being similar to that of Figure 1 but being operative to provide a plurality of concurrent SVCs 65 between machines M and T. In the Figure 5 system, the machines M and T and the server S are assumed to operate in the same way and have the same IP and ATM addresses as in Figure 1; in addition, in Figure 5 the same SVCs are established between the server S and the machines M and T as in Figure 1. The Figure 5 system includes, however, added functionality provided by processes 70 and 71 which in Figure 5 are shown independent of machines M and T but in practice would be provided either distributed between machines M and T or wholly in one of these machines; in a preferred embodiment, the processes 70 and 71 are provided in machine T.

In accordance with the present invention, each machine M and T is allocated a number of virtual IP addresses different from its operative (or "real") IP address (this latter address being the one which the IP layer knows about for inclusion as the source address in outgoing datagrams and upon which filtering is carried out by task 29). Thus, machine M is allocated virtual IP addresses $I_{M(1)}$, $I_{M(2)}$,.....$I_{M(j)}$...; similarly, machine T is allocated virtual IP addresses $I_{T(1)}$, $I_{T(2)}$,.....$I_{T(i)}$....

Each of these virtual IP addresses is entered into table 15 of ATMARP server S together with the ATM address of the corresponding one of the machines M,T; thus virtual IP address $I_{M(j)}$ is associated with ATM address A_M and virtual IP address $I_{T(i)}$ is associated with ATM address A_T.

Now, if the communications interface 18 of machine M is asked to send a message to IP address $I_{T(i)}$, IP layer 20 will construct a datagram 25A having a destination address of $I_{T(i)}$ and a source address of I_M. The IP-to-SVC task 30 of IP/ATM layer 21 then acts in the manner already described to fetch the ATM address corresponding to $I_{T(i)}$ from server S and set up an SVC (here identified by "p") towards machine T; the cache table 27 is updated appropriately. The datagram 25A is now sent by ATM layer over SVC(p) to machine T.

If no further action is taken, the datagram 25A, after receipt at machine T, will be rejected by the filter task 29 as the destination address $I_{T(i)}$ of the datagram differs from the operative IP address I_T known to task 29 of machine T. Accordingly, a process 70 is provided that recognises the destination address of datagram 25A as being a virtual IP address of machine T and substitutes the real IP address of machine T for the virtual address in the destination field of the datagram 25A. The datagram will now be allowed through by filter task 29 of machine T.

However, a further difficultly remains. If only the destination address is changed, the resultant datagram contains no indication that the datagram was not ordi-

Petitioner Apple Inc. - Exhibit 1026, p. 160

narily sent with the real IP address of machine T; any reply will therefore be sent on an SVC set up to take datagrams from machine M to the real IP address of machine M. This SVC would end up taking all the reply messages for messages sent from machine M to machine T over all the SVCs set up in respect of the virtual IP addresses allocated to machine T. This is clearly undesirable. To avoid this, the source address of datagram 25A is also changed by process 70. More particularly, the source address is changed from the real IP address of machine M to one of the virtual IP addresses $I_{M(j)}$ of this machine, the virtual address chosen being dependent on the original virtual IP address forming the destination address of the datagram. As a result, all datagrams 25A having the same virtual destination address end up after operation of process 70 as datagrams 25AA with the same virtual source address, whereas datagrams 25A having different initial virtual destination addresses end up as datagrams 25AA with different source addresses. The process of changing the source address preferably involves a predetermined transformation of the virtual destination address - for example, to obtain the required virtual source address, the virtual destination address can simply be incremented by one (there would thus exist, for example, a set of even virtual IP addresses for machine M and a corresponding set of odd virtual IP addresses for machine T, each even virtual IP address of machine M being associated with the immediately adjacent, lower-valued, odd virtual IP address of machine T).

The address-changing process 70 must be carried out on datagram 25A after operation of the IP-to-SVC task 30 in machine M and prior to the filter task 29 in machine T. In addition, whilst the two address-hanging operations of process 70 need not be carried out at the same time or at the same location (though it is, of course, convenient to do so), the changing of the source address must be done whilst the initial virtual destination address is still available.

The contents of datagram 25AA are passed by IP layer 20 of machine T to a high-level application which, in the present example, produces a reply that it passes to layer 20 for sending back to IP address $I_{M(j)}$, that is, to the source address contained in datagram 25AA. Layer 20 produces a datagram 25B with source address I_T and destination address $I_{M(j)}$. Next, IP-to-SVC task 30 of layer 21 looks up the destination address in the cache table 27 to find out the SVC to be used for the reply. If, as will normally be the case, the same SVC is to be used for the reply as carried the original datagram 25A with destination address $I_{T(i)}$, then the SVC setup process will have been arranged to enter the address $I_{M(j)}$ in cache table 27 against that SVC (in present case, identified to machine T by "q"); a lookup on $I_{M(j)}$ will thus return "q" as the required SVC. However, if it is desired to use a different SVC for datagrams 25B passing from T to M as used for datagrams 25A passing from M to T, then the first lookup on $I_{M(j)}$ by task 30 will not identify an SVC and task 30 must then initiate set up of a new SVC.

Assuming that the same SVC is to be used for the datagrams 25B with destination address $I_{M(j)}$ as for the datagrams 25A with destination address $I_{T(i)}$, then alter task 30 has identified SVC(q) as the appropriate SVC, the datagram 25B is passed to the ATM layer 22 for sending out over SVC(q). In due course, machine M receives this datagram and passes it up to IP layer 20; however, before the datagram reaches this layer, it must undergo address-change processing similar to that carried out on datagram 25A. More particularly, the virtual destination address $I_{M(j)}$ must be changed to the real IP address I_M of machine M, and the real source address I_T of machine T must be changed to the virtual IP address $I_{T(i)}$ of machine T associated with the virtual destination address $I_{M(j)}$. This address-change processing is carried out by process 71.

With regard to the source address change, where the corresponding change was effected for datagram 25A by incrementing by one the virtual destination address $I_{T(i)}$ of that datagram, then for datagram 25B, the source address is changed to the destination address $I_{M(j)}$ decremented by one.

In a similar manner to process 70, process 71 must be carried out on datagram 25B after operation of the IP-to-SVC task 30 in machine T and prior to the filter task 29 in machine M. In addition, whilst the two address-changing operations of process 71 need not be carried out at the same time or at the same location, the changing of the source address must be done whilst the initial virtual destination address is still available.

Following operation of process 71, datagram 25BB with source address $I_{T(i)}$ and destination address I_M is allowed through by filter task 29 and the contents of the datagram are passed to the relevant high-level application.

Having described the general mechanism by which virtual IP addresses can be used for exchanging datagrams 25A and 25B across a SVC between machines M and T, the issue will now be addressed as to how the cache table 27 in machine T is updated on SVC setup to associate the new SVC (that is, SVC(q) at machine T) with the virtual IP address $I_{M(j)}$ of machine M (this is required where the same SVC is to be used for the reply datagram 25B as for the original datagram 25A). It will be appreciated that when the task 40 (see Figure 2) is executed, the INARP request sent to machine M will only return the real IP address I_M of machine M, there being no other information available to the update task 40 by which any other result could be obtained from the INARP task 50; clearly, something additonal needs to be done for update task 40 to be able to associate the virtual IP address $I_{M(j)}$ with the newly created SVC(q) in table 27. In fact, there are a number of ways in which the update task could be informed that the IP address to be associated with SVC(q) is $I_{M(j)}$. For example, the update task 40 could be arranged to send a request back over the newly-created SVC(q) asking machine M to identify

Petitioner Apple Inc. - Exhibit 1026, p. 161

the destination IP address $I_{T(i)}$ it associates with that SVC; from this information, the update task could determine the associated virtual IP address $I_{M(j)}$ of machine M (assuming there is a predetermined relation between the two as is the case in the described embodiment) and then update table 27 accordingly. An alternative approach that avoids sending a special request to machine M is to wait for machine M to supply the destination IP address $I_{T(i)}$ in the first IP datagram 25A sent over the new SVC(q), the update task then deriving the required address $I_{M(j)}$ as described above.

A variant of this latter approach is to leave the update task 40 unchanged but provide an additional process that:

(a) delays the INARP request until the destination address $I_{T(i)}$ of the first datagram from machine M to machine T can be captured;
(b) uses the captured address $I_{T(i)}$ as the source address of the INARP request that is now sent on to machine M.

The INARP response from machine M will therefore have a destination address $I_{T(i)}$ and a source address (that forms the substance of the INARP response) of I_M. By ensuring that this response datagram is subject to the processing effected by process 70, the source data in the INARP response will be changed to $I_{M(j)}$ by the time the response reaches the update task 40. Thus, the required updating of the table 27 of machine T can be achieved without modification to the existing tasks of machines M and T but simply by the addition of a further process for effecting steps (a) and (b) described above. This approach is the preferred one for updating table 27 and is the one used in the module described below with reference to Figures 6 and 7.

The above-described system involving the allocation of multiple virtual IP addresses to machines M and T and the provision of the address-changing processes 70 and 71, permits multiple SVCs to be concurrently operated between the machines M and T thereby enabling implementation of the test arrangement depicted in Figure 4. Of course, when testing the machine M, it is desirable that no changes are made to this machine; accordingly, it is preferred for such a test arrangement to implement the address-changing processes 70 and 71 in machine T.

The implementation of the address-changing processes 70 and 71, and of the INARP request modification process, can conveniently by done by inserting a module (hereinafter called the VNS module) between the IP/ATM layer 21 and the ATM layer 22 of machine T; in fact, an instance of this module is created for each SVC, this being relatively easy to implement when using a STREAMS type I/O implementation as provided in most UNIX systems (conveniently one stream is provided for each SVC and the VNS module is pushed onto each stream when the stream is created).

The messages passing across the boundary between layers 21 and 22 have already been described above with reference to Figure 2 and the processing effected by the VNS module on each of these messages will next be described. First, the situation of Figure 5 will be considered where it is machine M that initiates the setting up of a new SVC to machine T. The first message received by the VNS module will be the SVC setup indication message $X5^R$ and this is passed through the VNS module without modification (see Figure 6). Next, the INARP request $X6^T$ is received and is subject to the modification process 82 described above, namely it is delayed until the first IP datagram 25A is received and the address $I_{T(i)}$ extracted and used for the source address of the INARP request. The INARP response $X7^R$ is then received and subject to the address-changing process 70.IP datagrams $X8^R$ from machine M to machine T are also subject to the address-changing process 70. IP datagrams $X8^T$ from machine T to machine M are subject to address-changing process 71.

Figure 7 depicts the processing effected by the VNS module in the situation where it is the machine T rather than the machine M that initiates SVC setup. The messages passing through the VNS module in this case are those shown crossing the boundary between layers 21 and 22 in Figure 2 for machine M. The first four messages $X1^T$, $X3^T$, $X2^R$, and $X4^R$ are passed through without modification. The INARP request received from machine M is subject to the modification process 82, being delayed until the destination address of the first IP datagram from machine T to machine M can be captured and used as the source address of the INARP request. The INARP response $X7^T$ is subjected to process 71 as are IP datagrams $X8^T$ from machine T to machine M. IP datagrams $X8^R$ from machine M to machine T are subjected to process 70.

It will be appreciated that many variants are possible to the above-described embodiment of the invention. It will also be appreciated that the invention is not limited to switched virtual circuits but can equally be applied to permanent virtual circuits. Furthermore, the setting up of multiple virtual circuits between two machines can be used not only for implementing the test arrangement described above with reference to Figure 4 but also for other purposes.

Although the present invention has been described in the context of high-level addresses constituted by IP addresses and virtual circuits set up across an ATM network, the invention can be applied to other types high-level addresses and other types of virtual-circuit network. For example, the high-level addresses could be MAC addresses in the case of a network in the form of a emulated LAN (ELAN) over an ATM network.

Claims

1. A system in which a plurality of entities are con-

Petitioner Apple Inc. - Exhibit 1026, p. 162

nected to a network and can exchange messages across virtual circuits set up over the network between said entities, each entity having an operative high-level address on the network, and each said entity comprising:

-- high-level messaging means for handling message transmission and receipt on the basis of said high-level addresses, said high-level messaging means comprising means for including in outgoing ones of said messages the operative high-level address of the entity as a source identifier and the operative high level address of the intended recipient entity as a destination identifier, and means for filtering incoming ones of said messages according to the destination identifier contained in the message:
-- virtual-circuit means for providing virtual circuits between the entity and other said entities, there being a respective virtual circuit for each different destination identifier in use, and
-- intermediate means for passing an outgoing message from said high-level messaging means to that one of the virtual circuits provided by the virtual-circuit means which corresponds to the destination identifier of the message;

characterised in that each of a first and a second said entity has a plurality of virtual high-level addresses associated with it that are different from said operative high-level address of the entity, said virtual high-level addresses being usable by the messaging means of said first and second entities as destination identifiers in outgoing messages; **and in that** between said intermediate means of said first and second entities, there are provided address-changing means responsive to each of at least some of said messages sent between these entities with a said virtual high-level address as its destination identifier to change that address to the said operative high-level address of the corresponding entity, and to change the operative high-level address provided as the source identifier of the message into one of the said virtual high-level addresses associated with the sending entity in dependence on the virtual high-level address initially provided as the destination identifier of the same message.

2. A system according to claim 1, wherein said address-changing means effects a predetermined transformation on the virtual high-level address forming the initial destination identifier of a said message to which the address-hanging means is responsive in order to form the virtual high-level address to be used for the source identifier of that message.

3. A system according to claim 2, wherein said address-changing means is responsive to messages sent in both directions between said first and second entities with virtual high-level addresses as destination identifiers, the said transformation effected in respect of such messages sent in one said direction being the reverse of the transformation effected in respect of other such messages sent in the opposite said direction.

4. A system according to claim 1, wherein said address-changing means comprises first address-changing functionality for effecting said changes for messages sent from said first entity to said second entity, and second address-changing functionality for effecting said changes for messages sent from said second entity to said first entity, both said first and second address-changing functionalities being provided in said second entity.

5. A system according to claim 1, wherein said address-changing means comprises first address-changing functionality for effecting said changes for messages sent from said first entity to said second entity, and second address-changing functionality for effecting said changes for messages sent from said second entity to said first entity, the two said address-changing functionalities being provided in respective ones of said first and second entities.

6. A system according to claim 1, wherein:

-- each said entity has a low-level address on the network;
-- said intermediate means of each entity further comprises:

-- first association means for providing an association between the destination identifier of a outgoing message and the low-level address of the corresponding said entity,
-- second association means for providing an association between the destination identifier of an outgoing message and a said virtual circuit,

said intermediate means using its second association means to identify from the destination identifier of a said outgoing message which virtual circuit is to be passed the message where such virtual circuit exists, and otherwise first passing a request to the said virtual circuit means of the same entity to establish a virtual circuit to the entity having the low-level address identified by said first association means as

Petitioner Apple Inc. - Exhibit 1026, p. 163

associated with the destination identifier of the outgoing message; and

-- the said virtual-circuit means of each entity includes setup means responsive to a said request from the intermediate means of the same entity to establish a virtual circuit to the said entity having the low-level address provided in said request, said setup means causing the intermediate means to update its second association means to associate the newly-established virtual circuit with the said destination identifier relevant to said request;

the first association means of each of said first and second entities serving to provide an association between the virtual high-level addresses of the other of said first and second entities and the low-level address of that other entity.

8. A system according to claim 7, further comprising a network server containing associations between high-level addresses and low-level addresses, said first association means of each said entity comprising means for interrogating said network server for a required association.

9. A system according to claim 7, wherein said second association means comprises cache means for temporarily holding said associations between said destination identifiers and currently corresponding virtual circuits.

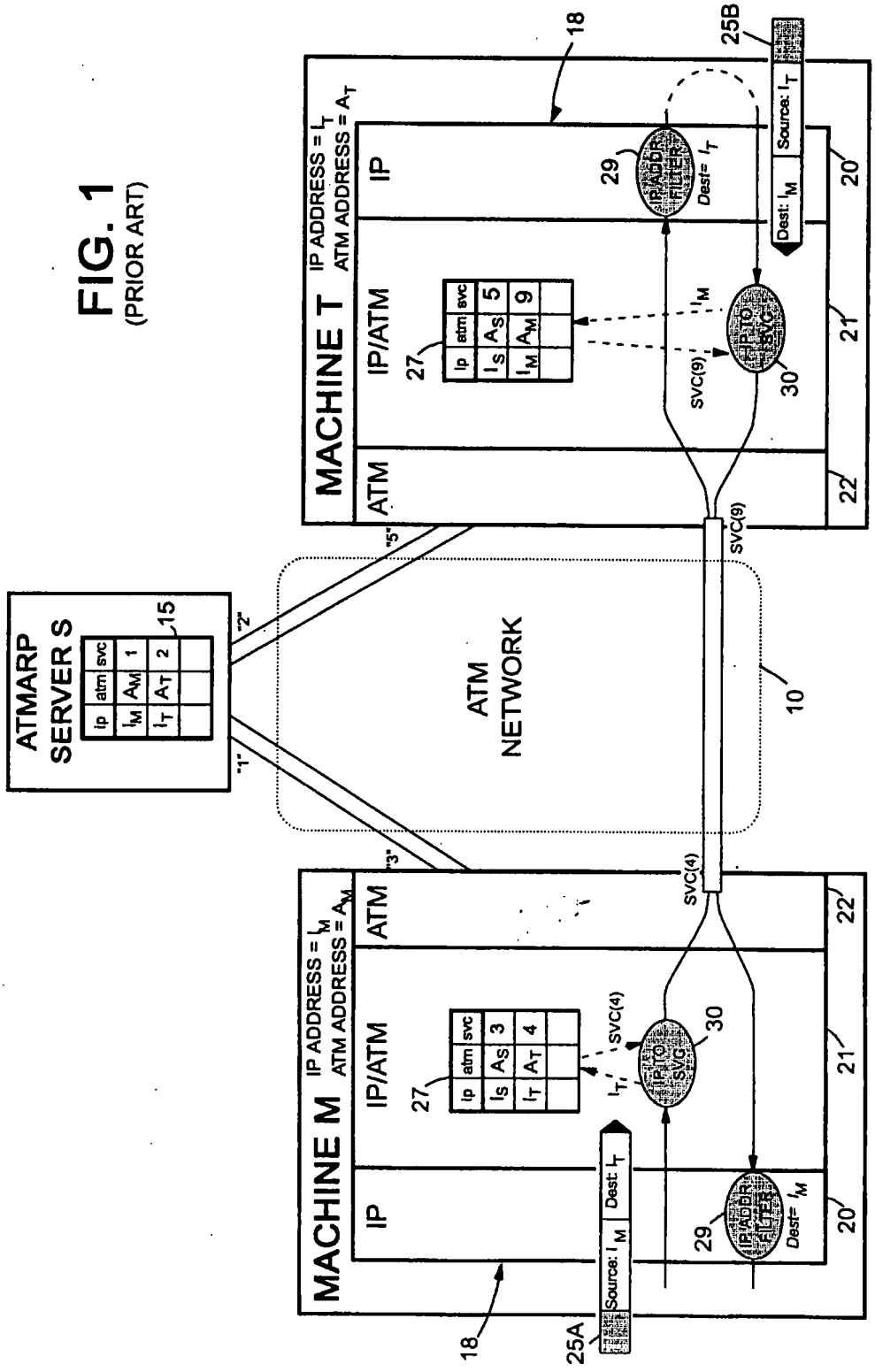
10. A system according to any one of claims 1 to 9, wherein said high-level addresses are IP addresses and said network is a ATM network.

11. A system according to any one of claims 1 to 9, wherein said high-level addresses are MAC addresses and said network is a emulated LAN over an ATM network.

12. A method of testing the ability of network node apparatus to operate a plurality of virtual circuits at the same time, said network node apparatus being arranged to establish a virtual circuit for each different high-level destination address being handled, said method involving setting up a system according to claim 4 with said network node apparatus as said first entity, and causing the network node apparatus to send messages to at least some of said virtual high-level addresses associated with said second entity.

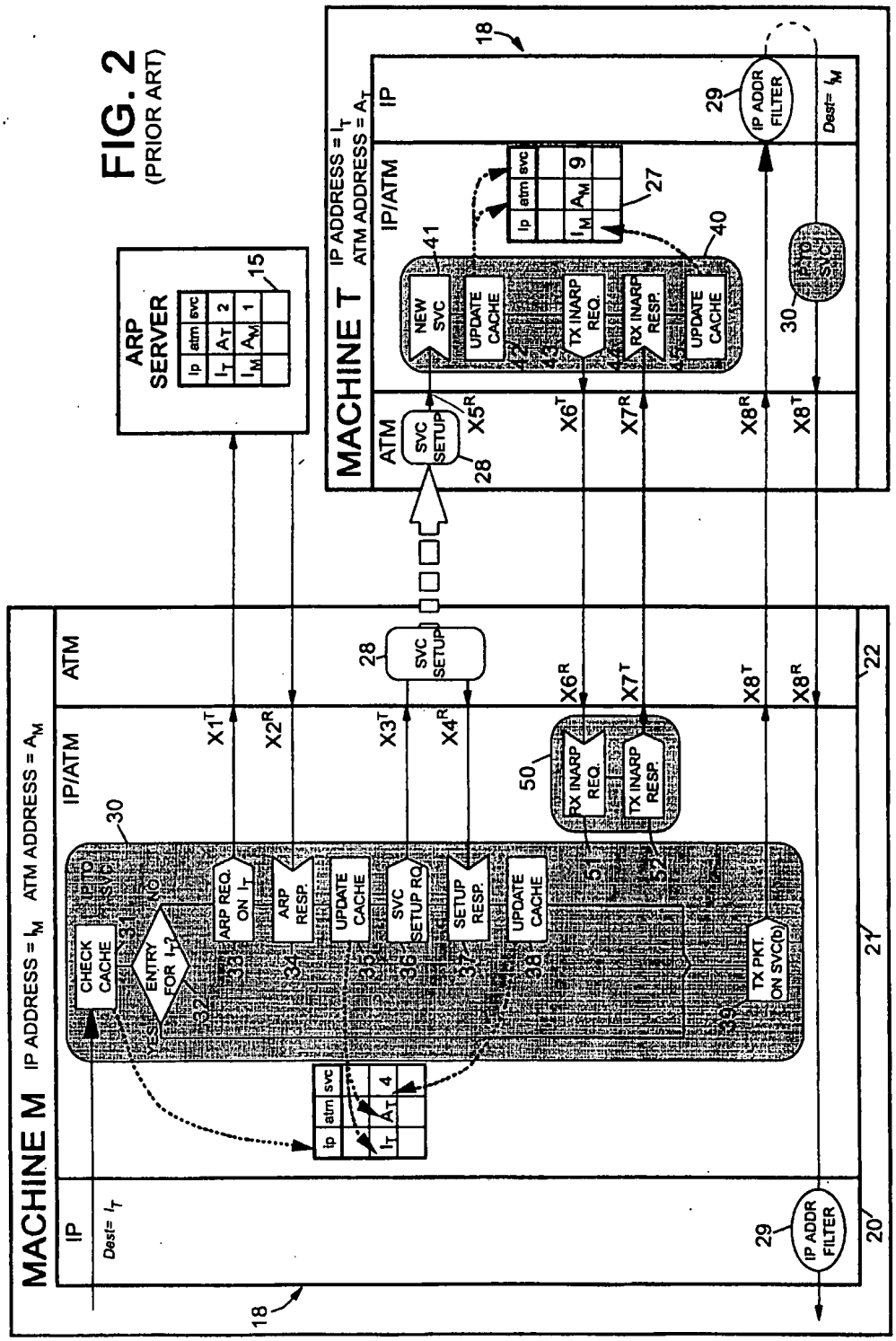
Petitioner Apple Inc. - Exhibit 1026, p. 164

FIG. 1
(PRIOR ART)



Petitioner Apple Inc. - Exhibit 1026, p. 165

FIG. 2
(PRIOR ART)



Petitioner Apple Inc. - Exhibit 1026, p. 166

FIG. 3
(PRIOR ART)

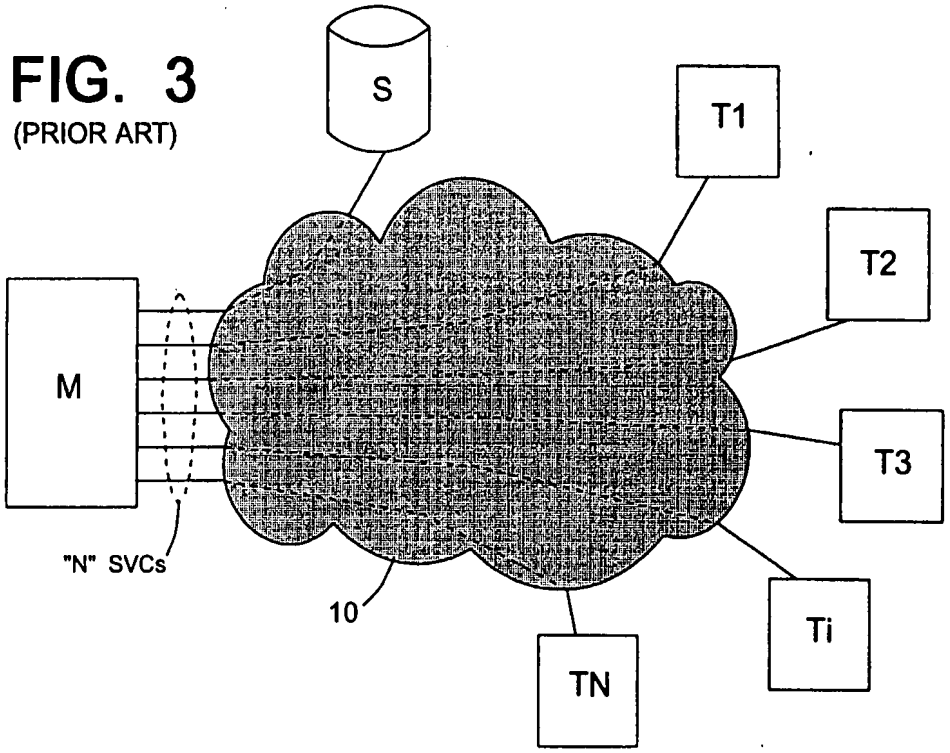
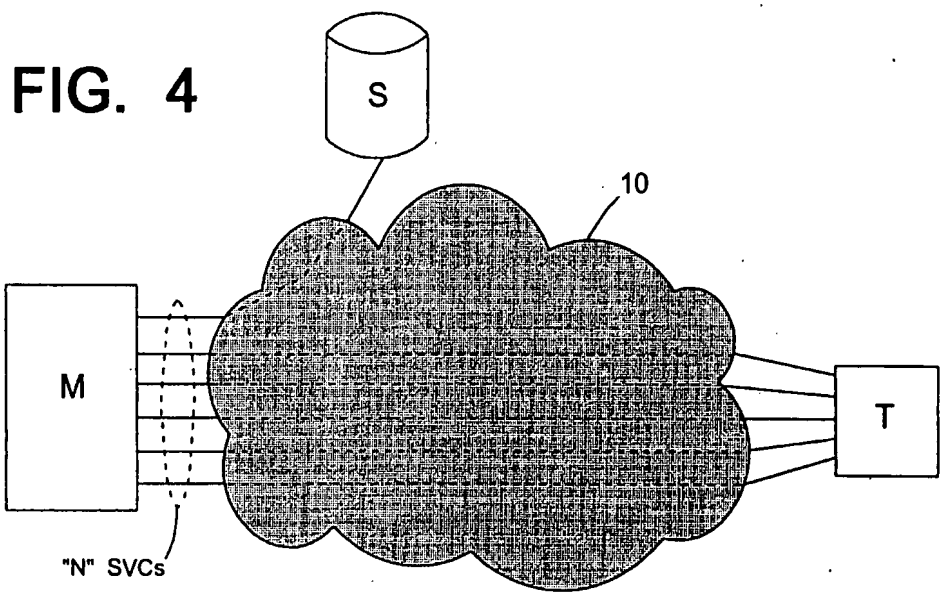
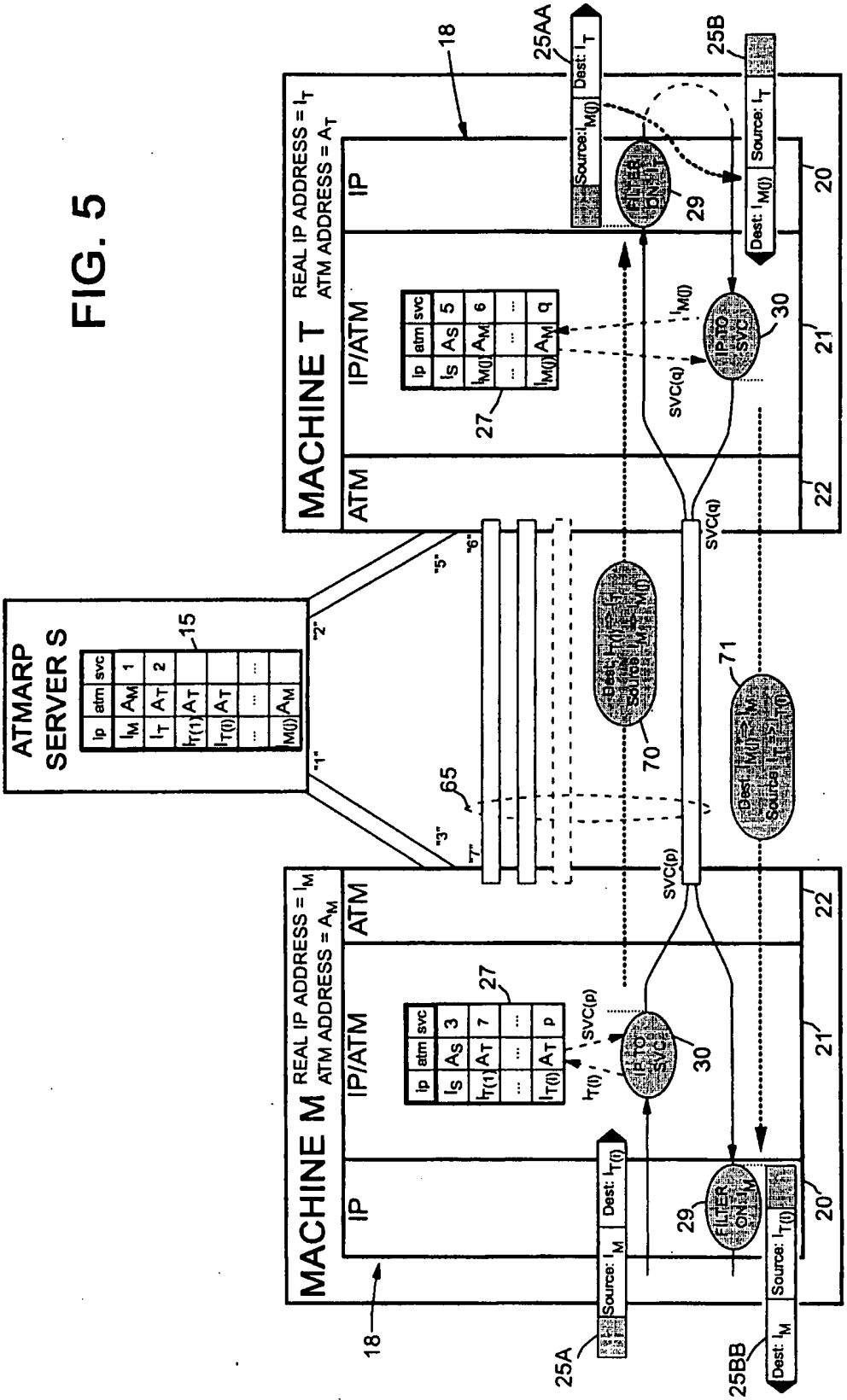


FIG. 4



Petitioner Apple Inc. - Exhibit 1026, p. 167

FIG. 5



Petitioner Apple Inc. - Exhibit 1026, p. 168

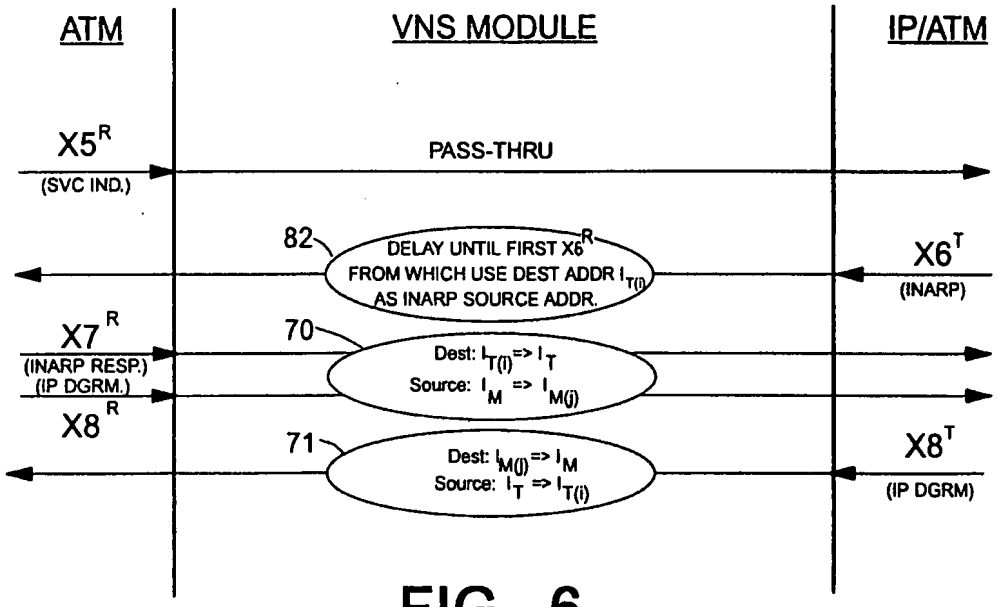


FIG. 6

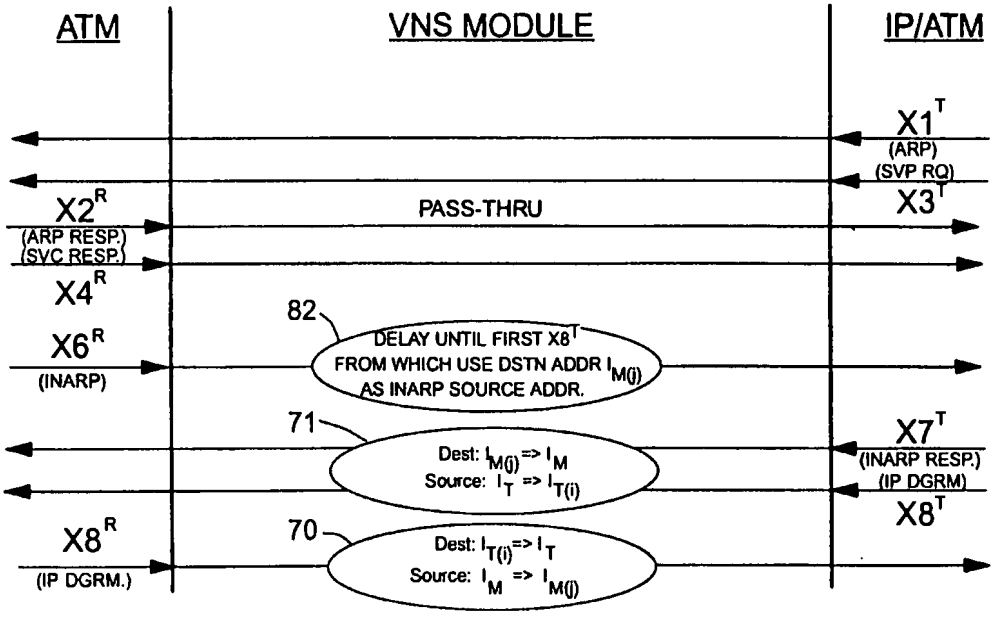


FIG. 7

Petitioner Apple Inc. - Exhibit 1026, p. 169

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 96 41 0106

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	COMPUTER COMMUNICATIONS REVIEW, vol. 25, no. 4, 1 October 1995, pages 49-58, XP000541650 PARULKAR G ET AL: "AITPM: A STRATEGY FOR INTEGRATING IP WITH ATM" * paragraph 2.1 * ---	1,10	H04L29/06 H04Q11/04
A	PROCEEDINGS OF THE ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIE, SANTA FE, NOV. 20 - 22, 1994, no. SYMP. 35, 20 November 1994, GOLDWASSER S (EDITOR), pages 424-434, XP000531950 LUND C ET AL: "IP OVER CONNECTION-ORIENTED NETWORKS AND DISTRIBUTIONAL PAGING" * paragraph 1 - paragraph 1.1 * ---	1,10	
A	DATA COMMUNICATIONS, vol. 24, no. 17, 1 December 1995, page 103/104, 106, 108, 110 XP000547618 MARSHALL G: "CLASSICAL IP OVER ARM:A STATUS REPORT" paragraph "Simple virtues"" ---	1,10,11	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L H04Q
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 35, no. 4A, 1 September 1992, pages 28-31, XP000314666 "COORDINATED ADDRESS RESOLUTION PROTOCOL PROCESSING" * the whole document * ---	6,8,9	
A	EP 0 523 386 A (FUJITSU) * page 4, line 20 - page 5, line 14; figure 3 * -----	12	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	13 March 1997	Staessen, B

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Petitioner Apple Inc. - Exhibit 1026, p. 170

B9

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 17/00 — A2

(11) International Publication Number: **WO 00/17775**

(43) International Publication Date: 30 March 2000 (30.03.00)

(21) International Application Number: PCT/US99/21934

(22) International Filing Date: 22 September 1999 (22.09.99)

(30) Priority Data:

60/101,431	22 September 1998 (22.09.98)	US
09/399,753	21 September 1999 (21.09.99)	US

(71) Applicant *(for all designated States except US)*: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION [US/US]; 10260 Campus Point Drive, San Diego, CA 92121 (US).

(72) Inventors; and

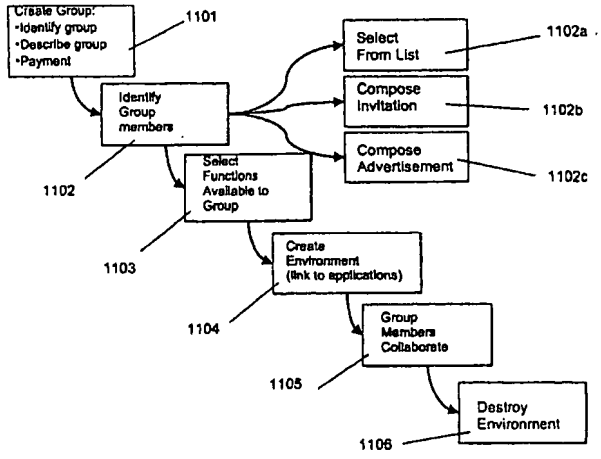
(75) Inventors/Applicants *(for US only)*: MILLER, Craig [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). MANGIS, Jeffrey, K. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). LESTER, Harold, D. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). NICHOLAS, John, M. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). WALLO, Andrew [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). KRESS, Thomas, P. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). CHEAL, Linda, J. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). WEATHERBEE, James, E., Jr. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). DAVIES, Linda, M. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US).

(74) Agents: WRIGHT, Bradley et al.; Banner & Witcoff, Ltd., Eleventh floor, 1001 G Street, N.W., Washington, DC 20001-4597 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: USER-DEFINED DYNAMIC COLLABORATIVE ENVIRONMENTS



(57) Abstract

A collaborative system and method allows members of a group to collaborate on a project such as a bid or proposal. According to a first embodiment, a complex instrument trading engine (CITE) facilitates negotiation between two or more parties. A set of tools and techniques are provided in order to facilitate negotiation and execution of complex instruments such as contracts between corporations and governments. According to a second embodiment, referred to as a dynamic collaborative environment, a user can define a group and a virtual private network environment including user-selected tools that facilitate communication, research, analysis, and electronic transactions within the group. The environment can be destroyed easily when it is no longer needed. Multiple environments can co-exist on the same physical network of computers.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

USER-DEFINED DYNAMIC COLLABORATIVE ENVIRONMENTS

This application is related in subject matter to and claims priority from provisional U.S. application serial number 60/101,431, filed on September 22, 1998. The contents of that application are bodily incorporated herein.

BACKGROUND OF THE INVENTION

1. Technical Field

This invention relates generally to computer systems and networks. More particularly, the invention relates to systems and methods for providing user-defined collaborative environments for transacting business or electronic commerce.

2. Related Information

Following hurricane Andrew, many insurance companies sought to limit their risk by withdrawing coverage from coastal areas. While this made good sense for the specific companies, it was not acceptable from a societal perspective. The cities, towns, homes and businesses built near the coasts could not afford to go without insurance, nor could the financial institutions that loaned money on these properties afford the risk. The problem facing the insurance companies was not the absolute magnitude of the risk, but the concentration of the risks in one area, leading to the possibility of very large losses resulting from a single event.

One law firm had conceived the idea of providing a mechanism for insurance companies to exchange risk. Companies with a high exposure in one area (e.g. Florida windstorms) could reduce their risk by ceding part of this to another company with non-coincident risk (e.g. California earthquakes) and assume part of the second company's risk in return. A company (CATEX) was formed to conduct such trading, but the trading rules had yet to be defined and the trading infrastructure had not yet been developed. CATEX postulated that the key barrier to insurance risk trading was determining the relative risk of different perils in different regions. One approach suggested by CATEX was to try to estimate these relative risks (termed relativities) for a broad set of perils and regions, to provide an initial basis for trading.

It was recognized, for various reasons, that this could not be done feasibly because: general estimates of risk, rather than the risk for specific locations, buildings, ships, etc. would be inadequate for commerce; there were many risks to evaluate given all of the permutations of location, perils, and structure; and companies would not be willing to trade risk based strictly on a third-party's analysis

Petitioner Apple Inc. - Exhibit 1026, p. 173

An analysis of the problem, however, indicated that estimating the relativities was not essential to facilitate trading, or, in a broader sense, that trading was the only way to address the problem of insuring concentrated risk. The key difficulty was determining how to create greater efficiency in the reinsurance market, whether by introducing new instruments (like swaps), bringing new capital to the market, connecting more buyers to more traders, or reducing the cost of placing reinsurance. It was determined that the above concept could be implemented in an electronic trading system that could play an important role in promoting these factors, and could, in fact, transform the reinsurance market, which is not very automated. A system that allowed trading was developed and implemented. A more detailed description of this system, as enhanced in accordance with various inventive principles herein (referred to as "first-generation" complex instrument trading technology), are provided below. More generally, as electronic commerce (and business-to-business commerce, in particular) has grown, various companies have developed software tools and services to facilitate transactions on the Internet and over private networks. E-Bay, for example, hosts a well-known web site that operates a transaction model (a so-called "concurrent auction") that permits buyers to submit bids on items offered by individuals. Lotus Notes provides a network-oriented system that allows users within a company to collaborate on projects. Oracle Corporation hosts various transaction engines for clients that pay to host such services on a web site. DIGEX Corporation similarly hosts web-based application programs including various transaction engines. Other companies sell so-called "shrink wrap" software that allows individuals to set up web sites that provide catalog ordering facilities and the like.

Some Internet service providers, such as America Online, host "chat rooms" that permit members to hold private discussions with other members who enter various rooms associated with predetermined topics. A company known as blueonline.com hosts a web site that facilitates collaboration on construction projects. Various virtual private networks have been created to facilitate communication among computer users across the Internet and other networks, but these networks provided very limited functionality (e.g., e-mail services); are not user-defined (they must be created and installed by system administrators); and they cannot be easily destroyed when they are no longer needed.

Petitioner Apple Inc. - Exhibit 1026, p. 174

The aforementioned products and services are generally not well suited to facilitating complex electronic transactions. As one example, most conventional services are predefined (not user-defined) and are centrally administered. Thus, for example, a group of companies desiring to collaborate on a project must fit their collaboration into one of the environment models provided by an existing service provider (or, alternatively, build a custom system at great expense).

Suppose, for example, that a group of high school students needs to collaborate on a research paper that requires soliciting volunteers for a survey on drug use, conducting the survey, brainstorming on the survey results, posing follow-up questions to survey participants anonymously, publishing a report summarizing the results, and advertising the report for sale to newspapers and radio stations. This project requires elements of communication among persons inside a defined group (those writing the paper) and outside the group (e.g., survey participants); conducting research (conducting the survey, compiling the results, comparing the results with other surveys published by news sources; and brainstorming on the meaning of the results); and conducting a commercial transaction (e.g., publishing the survey in electronic form and making it available at a price to those who might be interested in the results). No existing software product or service is available to meet the specific needs of this research team. Creating a user-defined environment including tools and communication facilities to perform such a task would be prohibitively expensive. Even if such a tailor-made environment could be created, it would be difficult to disassemble the environment (computers, networks, and software) after the project was completed.

In short, there is a need to provide a user-defined collaborative environment that is tailored to the needs of particular groups that conduct communication, research, electronic transactions, and deal-making.

SUMMARY OF THE INVENTION

A first embodiment of the invention, referred to as a complex instrument trading engine (CITE), facilitates negotiation between two or more parties. In this embodiment, a set of negotiation tools and techniques such as anonymous email, secure communication, document retention, and bid and proposal listing services are provided in order to facilitate the negotiation and execution of complex instruments such as contracts between corporations, governments, and individuals.

Petitioner Apple Inc. - Exhibit 1026, p. 175

A second embodiment of the invention, referred to as a dynamic collaborative environment (DCE), allows members of a group to define a dynamic virtual private network (DVPN) environment including user-selected tools that facilitate communication, research, analysis, and electronic transactions both within the group and outside the group. The environment can be destroyed easily when it is no longer needed. Multiple environments can co-exist on the same physical network of computers.

Although the two embodiments are described separately for ease of comprehension, it should be understood that the two embodiments share many features and, in fact, the second embodiment could include some or all of the features of the first embodiment in a generalized collaborative system. Consequently, references to a specific embodiment in the following description should not be deemed to limit the scope of features or tools included in each embodiment. Moreover, references to specific applications, such as the reinsurance industry, should not be deemed to limit the application of the invention to any particular field.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1A shows a four-step model of deal making including meeting, analysis, negotiation, and closing the deal.

FIG. 1B shows contract formation among a group of parties to a contract.

FIG. 2 shows a listing display system showing all offers for contracts and responses thereto.

FIG. 3 shows details of a listing that has been selected by a user.

FIG. 4 shows one possible implementation of a reply card definition screen.

FIG. 5 shows one possible implementation of a document management screen.

FIG. 6 shows one possible implementation of a screen indicating persons having access to a shared folder.

FIG. 7 shows a list of consummated deals in the system.

FIG. 8A shows detailed information regarding a completed trade.

FIG. 8B shows a deal summary including structured and unstructured information concerning the deal.

FIG. 9 shows a "flip widget" in a first state.

FIG. 10 shows a "flip widget" in a second state.

Petitioner Apple Inc. - Exhibit 1026, p. 176

FIG. 9A shows a more detailed example of a "flip widget" in a first state.

FIG. 10A shows a more detailed example of a "flip widget" in a second state.

FIG. 11 shows method steps that can be carried out to define, create, and destroy an environment according to a second embodiment of the invention.

FIG. 12 shows one possible system architecture in which various principles of the invention can be implemented.

FIGS. 13A through 13C show one possible user interface for creating a group and identifying group members.

FIG. 14A shows one possible user interface for selecting group members from one or more lists.

FIG. 14B shows one possible user interface for selecting group members by composing invitations.

FIG. 14C shows one possible user interface for selecting group members by composing an advertisement.

FIG. 15 shows a banner advertisement 1501 displayed on a web site, wherein the banner advertisement solicits participation in a group.

FIG. 16 shows one possible user interface for selecting communication tools to be made available to group members.

FIG. 17 shows one possible user interface for selecting research tools to be made available to group members.

FIG. 18 shows one possible user interface for selecting transaction engines to be made available to group members.

FIG. 19 shows one possible user interface for selecting participation engines to be made available to group members.

FIG. 20A shows an authentication screen for group members to gain access to a newly created environment.

FIG. 20B shows a web page generated for a specific user-defined environment, including tools available to group members having access to the environment.

FIG. 21 shows one possible method of generating environments in accordance with various aspects of the present invention.

FIG. 22 shows one possible data storage arrangement for storing and manipulating brain writing cards.

Petitioner Apple Inc. - Exhibit 1026, p. 177

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

A. COMPLEX INSTRUMENT TRADING ENGINE EMBODIMENT

A first embodiment of the present invention provides a second-generation version of a complex instrument trading system. The second-generation system includes specialized tools that were not included in the first version of the prior art CATEX insurance trading system described above. These tools represent a substantial improvement over the first generation and incorporate new concepts of communications in a trading environment, and other capabilities that did not exist in the first generation technology. In addition, it is believed that many of these tools are also applicable to software systems other than the Complex Instrument Trading Engine or Negotiating System (CITE) described herein. Thus, the inventive principles are not limited to trading systems for complex instruments, nor even to trading systems in general.

Primarily, the tools described herein ameliorate certain difficulties associated with trading of complex instruments. Complex instruments are instruments where there is more than one dimension for negotiation. As compared to such instruments as securities, complex instrument transactions take longer to research and consummate and require more extensive documentation. For example, stock trading employs a simple instrument (a share) and negotiation focuses on one dimension (price) while insurance contracts have many dimensions (term, price, coverage, definitions of perils, etc.). The stock market is relatively simple to automate -- as soon as bid and asked prices match, the deal is concluded in an instant according to the rules of the exchange. Automation of complex trading is much more difficult, since the parties must negotiate and reach agreement on multiple dimensions and document that agreement using an instrument specific to the precise agreement. Automation of complex instrument trading is more difficult in every way than trading simple instruments.

The trading model behind the Complex Instrument Trading Engine or Negotiating System is built around a simple, four-step model of deal making. Referring to FIG. 1A, the steps are as follows:

1. Meeting: Potential buyers connect with potential sellers with reciprocal interests. This connection does not mean that a deal will necessarily be concluded but simply that the two parties have some basis for continuing discussion. In simple

Petitioner Apple Inc. - Exhibit 1026, p. 178

instrument trading, it is typically only necessary to advertise quantity and price offered or sought. Offers for complex instruments must include substantially more detail and (frequently) extensive attachments or exhibits.

2. Research/Analysis: Each company considers its own position and/or offer and the counter party's position. Using information and analytic tools from various sources, including internal resources and resources provided by or through the trading system, each party does research and refines its position. The multiple dimensions of complex instruments increases the analytical complexity and limits the value of a simple market price. As indicated by the arrows in FIG. 1, this step is usually performed iteratively with the negotiation.

3. Negotiation: Parties to the negotiation speak directly and exchange whatever information is necessary to advance the deal. As indicated by the arrows in FIG. 1A, this step is usually performed iteratively with the research step.

4. Close: the companies negotiate and sign an instrument that documents the deal. This can be a complete and detailed contract, or it may be a simple memorandum. In simple instrument trading, the actual trade agreement is often standardized by the exchange. In complex instrument trading, the agreement must be more specific to the deal, though it is possible to use such tools and fill-in-the blank forms.

Within a system using these complex instrument tools, trading parties can place offers to buy, sell, or trade in a public area, and examine such offers ("listings") posted by others. Using advanced communications tools the parties can conduct initial discussions to determine if a placement is possible. Using tools described herein, the initial contact can be done anonymously.

If a deal seems possible, the system preferably provides access to the extensive information necessary to assess the possible deal. This can include static information (e.g. reports or data) maintained within the system, links to information providers outside the system, online analytical tools, and links to providers of analytical services.

For complex instruments, the process of negotiating a deal is contemplated to be an iterative one, with successive stages of analysis and discussion. The need for extensive communication is one of the critical distinctions between trading of simple instruments (e.g. retail sale) and complex instruments. Complex instrument

Petitioner Apple Inc. - Exhibit 1026, p. 179

trading requires dialog and more -- exchange of documents (often voluminous), consultation with counsel and intermediaries, conferencing, and working together on the final agreement. For electronic commerce to have an impact in complex instrument trading, it must support and facilitate this communication, and not force traders to fall back on methods and technology outside the electronic trading environment.

The final step is closing the deal. The companies can negotiate a contract online. Tools provide sample, fill-in the blank contracts and memoranda of understanding as a starting point. Negotiators can begin with these, or they can use one of their own. Collaborative software makes it possible to display text simultaneously on each negotiator's screen and to work on the language together. When the contract is final, the system allows for secure, online signature, though companies not comfortable with electronic signature for very large deals may print a hard copy and sign it conventionally.

By creating electronic exchanges for complex instrument trading, the CITE tools can have a fundamental and positive impact on many areas of commerce:

1. An electronic exchange makes it possible to put an offer in front of more people more quickly than could be informed through direct contact, even allowing for active intermediaries or brokers.

2. Traders can advertise and conclude deals without the need for an intermediary when they have adequate support or internal resources.

3. Through better communications, wider exposure for offers, and the first steps towards standard contract language, electronic trading of complex instruments can substantially reduces transaction costs.

4. With lower transaction costs, it is possible to conclude deals that were not possible with higher overhead.

5. Through the immediate posting of the results of trades, pricing is moved towards a market basis, reducing research and analysis costs enormously. This speeds placement.

6. Smaller exposure means lower risk, and market pricing is an adequate surrogate for analytically derived pricing in some circumstances. Together these factors make it possible for traders to participate in markets or market segments in which they would not normally do business.

Petitioner Apple Inc. - Exhibit 1026, p. 180

7. By making it possible for all companies, large and small, to talk directly to each other, electronic trading of complex instruments can lead to the democratization of the marketplace increasing competition.

Overall, electronic trading of complex instruments has the potential to improve the efficiency of markets enormously, and to establish markets in areas of commerce that are currently done through intermediaries or on a one-on-one basis. The trading tools described herein are designed to facilitate electronic trading of complex instruments. The first-generation complex instrument trading tools broke new ground in the extension of electronic commerce into new and more complicated markets. The table below summarizes the areas of new and improved technology, organized into the four steps of the general complex instrument trading model.

Phase	First Generation Complex Instrument Trading Technology (PRIOR ART)	Advanced Complex Instrument Trading Technology
Meet	• Operates on private network only • Post a listing to board by filling out a form • Display listing summary in a table • Search listings by key word • Post response to listing on board • Establish communications with lister by following up on contact information in listings using unconnected communications tools	• Operates on private network or over the Internet • Post listing to a board by filling out a form • Listings and responses can have attachments and documents • Display listing summary in a table, with sorting by title, date, market type, buy/sell, or listing number. • Search listings by keyword • Register keywords with an electronic "agent" that monitors listings and sends notice of relevant new listings by Email • Post response to listing on board • Send private response (anonymously or with name attached). • Response can be through a "reply card" designed by the trader posting a listing, to structure responses • Direct connection between listings and communications tool

Petitioner Apple Inc. - Exhibit 1026, p. 181

Analysis	• Internet access to research resources, on line and third-party analysis	• Internet access to research resources, on line and third-party analysis • Research resources searchable using the same search engine and display as used for listings. • Online dialogs / user groups
Negotiation	• Requires private network • Directory of contact information for all traders • Connection between directory and Email client. • Directory not linked to other components of the system • Anonymous mail application providing for communications between two individuals • Anonymous mail delivered to mail client • No attachments for anonymous mail • No system for central repository of documents	• Works on Internet or private network • Directory of contact information for all traders. • Direct connection between directory and Email client • Direct connection between directory and online conferencing software • Directory linked to listings and document management tool • Anonymous mail application providing for communications between individuals or groups of people working together • Anonymous mail does not require separate Email client software • Anonymous mail supports attachments • Internet-based system for distributions and sharing of documents. • Password and secure has protection for documents.
Closure	• Requires private network • Online signature of uploaded document	• Internet or private network • Online signature of uploaded document • Registration / closure of deal through a fill-in form • Provision for digital signature and archiving of all documents associated with a deal

Referring to FIG. 1B, one aspect of the system within the framework of the

Petitioner Apple Inc. - Exhibit 1026, p. 182

negotiation/analysis loop shown in FIG. 1, is the ability to define one or more contracts, for example, in the parlance of the reinsurance trade, "slip sheets." Various members of a group of authorities modify the contract causing it gradually to take a final form that is either rejected as untenable or accepted as a finalized deal. The system exposes various aspects of the contract and attendant documents to the appropriate participants in the transaction, also providing each with a level of authority to add, delete, or modify documents as well as the evolving contract or contracts (assuming there may be various contract templates being discussed). These filters (filter 1 through filter 4, for example), as shown in FIG. 1B, determine the authority of the party (Party 1-Party 4) to modify or see the data object, whether it is a document or a slip sheet. The system combines this system of filters with signature technology for closing the deal; that is, implementing signatures so that an enforceable contract is generated.

A deal is like any other data object and once it is defined and entered, it cannot be modified. Elements of the deal can be "signed" such as documents attached to a contract (for example, Contract 1 has documents D1 and D2 attached to (combined with) it. Together these elements, the contract and the attachments, define the deal. Also, the entire deal 245 can be signed using a signature device ("widget") S8. Other documents may relate to a deal but not be attached. These can be viewed using a document manager described further below.

Listing System

Referring to FIG. 2, a listing screen displays all offers for contracts, for example offer 314, as well as responses to them, for example, response 313. The parameters of the offers and responses to them are shown in columns, the heading of each of which may be selected to sort the listings by that heading, for example heading 315 if clicked would sort by the unique index number for the listing. Notice that the responses (for example, response 313) are shown indented to indicate a series of elements of a dialogue-thread. As indicated, the responses have a "daughter" relationship to the parent listings. That is, listing 314 is a parent and reply 313 is a daughter. The daughters remain in their hierarchical position beneath the parent despite sorting by the column headings. This makes the tabular sort scheme compatible with a threaded display, which is useful to show dialogues.

Referring now also to FIG. 3, when a user invokes a display of the details of

Petitioner Apple Inc. - Exhibit 1026, p. 183

a listing by clicking on an index hyperlink 312 to show the details of the listing, a user interface element displays the lister's defined parameters of the listing. As shown, various parameters are displayed, many of which are hyperlinked. For example, attachments 304 may be selected to display the corresponding attachments. A detailed description 301 may be provided as well as specific instructions for responding 302. A reply button 303 permits the user to reply. Activating the reply button 303 will either invoke a standard public reply screen which creates a new listing similar to the parent listing or a special reply defined by a reply card which is further described below.

A reply to a listing can take the form of a public reply that invokes a screen substantially the same as FIG. 3 but with blank spots for entry of reply information. A more useful kind of response element is a reply card that can be defined by the lister. This is because in negotiations on complex transactions such as reinsurance contracts and, for example, pollution emission allowances, the parties with whom a lister would be willing to trade are limited in terms of certain criteria. These criteria will vary from one type of transaction to another.

In an active trading system, the number of listings can quickly grow to a large number and quickly exceed the number which can conveniently be displayed in a single table. Several capabilities are built into the system to address this problem. First, by default, listings are presented in order from newest to oldest. Second, the sort capabilities previously described allow users to modify the standard order. Third, the total market may be divided into subcategories. In the area of insurance catastrophe risk, these could include categories for different lines of insurance (e.g. marine, aviation, commercial buildings). Fourth, users may enter search criteria to identify a subset of listings of particular interest.

Searching listings: A user may enter a keyword such as "hurricane" to identify all listings that contain that word in the title, description, and (optionally) attachments. To improve the reliability of the search, users are provided access to a standard lexicon when composing a listing. In the first embodiment, this capability is invoked by pressing the right mouse button while the cursor is any field of the listing. A list of common terms is displayed. The user can select the term of interest, which is then placed into the text of the listing at the insertion point marked by the cursor. For example, a listing for insurance risk would typically include a

Petitioner Apple Inc. - Exhibit 1026, p. 184

field for geographic scope (i.e. the location of the properties to be insured). When in this field, the lexicon displayed would include terms such as "California" and "Coastal Florida". Choosing a term from the lexicon insures uniformity of terminology across listings and between the search engine and the listings. "California" will be used rather than a mix of "Ca", "CA", "Calif", etc. The search is further improved by symantic indexing. Essentially, this means that synonymous terms are grouped, so that searches for one will find the other. A person who searches for "California" will get listings for "Los Angeles" that do not include the word "California".

The search engine can include an agent capability. This agent capability offers the user the option of saving a search, after the user reviews the results and deems them acceptable. This search is retained in a library of searches along with the email address of the owner of the agent. The search is retained in the library until is it either deleted by the user when it is no longer needed or automatically deleted in a cleanup of searches older than a certain date. Whenever a new listing is placed on the system, all of the saved searches are executed. If the new listing meets any of the search criteria, a message is sent to the owner of that criterion via email or instant messaging.

A model was developed to allow a lister to define a set of criteria and request a set of information from any respondents in the form of an anonymous reply "card." The card defines a set of requested information which may be packaged as a document object and placed in the document manager system and connected with each listing. A user would download the reply card and fill the card out and send it back to the posting party.

A document object, called a reply card, is made available to a respondent through the document manager. The respondent is permitted to retain his anonymity as is the lister. Each may communicate with the other through an Amail system described in more detail below. The respondent supplies the requested information and sends the data to the lister. A system in the listing manager allows a lister to define a reply card having any particular fields and instructions required of a respondent. Some of the information required may be obtained automatically from a set of default data stored on the respondent's computer.

Referring to FIG. 4, a reply card definition screen is invoked to define the

Petitioner Apple Inc. - Exhibit 1026, p. 185

parameters of a new listing. The new listing is defined using a user-interface element looking much like FIG. 3. While the details are not critical, the definition of reply card involves, in essence, the definition of a user-interface control such as a dialog with radio buttons, text boxes, etc. These are definable for server-side implementation through HTML and are well known so the details are not discussed here. The lister defines a set of controls that allow the entry by a replying party of the information that the lister requires. The reply card is stored as any other information object and may be organized and accessed through the document manager described below. FIG. 4 shows a simple example of a format of a reply card.

A reply card is created by a user when posting a new listing. The lister specifies the information that must be included in a response, and the type of information object to display for the data element (e.g. a text box, check box, radio button). The system then creates an HTML page to collect the requested information. When a respondent clicks "Reply Card" on the listing screen, the page is displayed. All of the responses are automatically entered into a database created automatically when the reply card is composed. As each respondent fills out a reply card, a new record is added to the database of the system and the lister is permitted to view it through an appropriate filter as discussed above.

Signature System

As business is increasingly done in an electronic environment, electronic signature and approval is becoming more critical. The typical electronic signature model has focused on two aspects:

1. Electronic validation of the user -- specifically determining that the person viewing a document on line is the authorized signatory; and
2. Validating the document being signed by a means that either prevents modification of a document or will reveal whether changes have been made.

Methods for validation of identity range from simple personal identification numbers or passwords, to electronic signature pads, and more advanced methods of biogenic validation such as fingerprint or retinal patterns. Methods for document validation range from simple archiving of one or more copies in a read-only model or inaccessible location to methods based on mathematical algorithms that create a characteristic number or alphanumeric string for a document. These strings are

Petitioner Apple Inc. - Exhibit 1026, p. 186

termed "electronic signatures." Changes to the document change the electronic signatures. Because the signatures are much shorter than the documents, very many documents have precisely the same signature, but the algorithms to calculate the signature are very difficult to invert, so that it is effectively impossible to deduce a meaningful change to a document that will preserve a specific signature.

These two aspects of electronic signature are highly developed, but there has been little analysis or development of the general process by which documents can be signed.

The invention allows for secure and reliable routing of documents, for which signatures are required, to a specified list of signatories. Unlike prior art systems, such as ordering or accounts payable systems which have highly structured signature procedures tailored to a specific process, the present invention provides a flexible method and system that allows a signature-type of authority/requirement to be attached any kind of information object. The method is sufficiently abstract, flexible, and general that it can be applied in many contexts aside from the CITE embodiment described in the present specification.

One signature method/device employs the following steps:

1. Registration of signatories – This process provides a register of identifiers indicating entities with signatory authority and correlates these identifiers with the information objects for which the signatory authority is applicable. The same register may also be used to identify other types of authority in the system in which the signature device is implemented. For example, document read authority, modification authority, exclusive access to documents, etc. may also be provided in the same register. Signature registration may be provided automatically in certain systems where registration of, for example, read/write authority is provided since any entity with signatory authority would in almost all instances, also be provided with some other kind of authority, most notably, read authority. Thus, where the signatory system is embedded in certain kinds of systems, it may be that no particular additional method or device is required to implement signatory registration since an existing register may already exist or be required for other purposes.

Registration information includes the general categories of information listed below. Definitions of specific fields within these categories are a function of the specific implementation of the signature system or the parent system. The following

Petitioner Apple Inc. - Exhibit 1026, p. 187

are exemplary:

1. Identity – unique identifier of the entity, the organization(s) with which the entity is affiliated, other relevant information.

2. Contact information – information indicating how the entity can be reached, how documents and mail messages can be routed to the entity.

3. Security Information – a password for each class of signature as described further below.

2. Classes of signatures – The device/method provides a variety of classes of signature, each associated with a unique level of approval or level of commitment. For example, a class of signature-authority can be defined that represents individuals, for example, with authority to sign contracts only below a set amount, or for expenses relating only to one department of an organization, or within certain time constraints, etc. The signatory system maintains this taxonomy of possible signature types in a database with a unique identifier for each level of authority defined. The system allows the creation and deletion of classes. Each class is preferably permitted to be named and a descriptive definition attached to each class.

3. Defining a Set of Signatures – Using an appropriate user interface element, the user of the system selects an information object (for example, a document, file, or collection of such objects) requiring signature(s). The entity originating the signature process then identifies the entity or entities required to sign the object. The specification of the signers can proceed either by the selection of individuals from a list supported by the above defined entity register. Alternatively, in an environment where individuals are strongly bound to organizations, for example, it can proceed by selecting the list of organizations that will sign and, within each organization, the person who will sign. The list is built by a series of selections. After each selection from the list, the user indicates his/her desire to add the selected individual to a list of required signatories. The user interfaces provides for entries in which all the selected signatories are required or only one of the selected signatories are required.

For example, if more than one entity is selected from the list prior to the selection (e.g., clicking an "Add" button), the system may require a signature from any of the people selected, but not all of them. To require signature from every member of the group, the initiator may select one person, then "add", select the second, then "add", and so on. Thus, adding a group with one "add" command would

Petitioner Apple Inc. - Exhibit 1026, p. 188

provide an "any signature will suffice" list and adding members individually would require a signature from that individual or entity. Note that this technique may also be used to define combinations of required and "any of" groups.

For each signer or group of signers selected in a single "add" command, the initiator of the signing sequence must specify the class of signature associated with the person for the document being signed. This may be selected from a list of signature classes (see item 2). If the specific implementation of the signature process only supports one class of signature, the selection of class may be omitted.

4. Random or Serial Order of Signature – After or concurrent with the creation of a signature list, the initiator specifies whether signatures must be in order or if a specific order is not required. For purposes of defining the order of signature, individuals who are selected as a group are considered as occupying a single place in the sequence.

5. Document Authentication – Upon initiating a signature sequence, the information object is authenticated by means of a secure hash algorithm. The specific hashing algorithm is a matter of design choice or may made dependent on a user's choice. There are several possible hash algorithms available in the public domain. The electronic signature produced by the secure hash algorithm is archived with the information object in a secure repository. If the information object is, for example, a record in a database, the contents of the record are copied to a file in delimited format for archival purposes. If the object is a table, the table is exported prior to archive.

6. Document Routing – Upon initiation of a signature sequence, the initiator specifies how the signatories are to be informed. The options are:

- No notification from the signature system
- Email message
- Email message with attachment of the information object.
- Posting on a signature web site

The system accepts and implements the chosen method, which may be connected to the signature or a single choice applied to all signatories. Alternatively, the method of notification may be stored with the signature class definitions. In a signature process with no required order, e-mail notice may be sent simultaneously to all of the

Petitioner Apple Inc. - Exhibit 1026, p. 189

designated individuals at the time of initiation. If the process is serial, only the first person may be notified. The electronic signature of the information object may be included in an e-mail message.

7. Accessing the signature system – The signature system can be implemented for access via a web browser or database client-server software across the Internet, an intranet, a LAN, or a WAN. Access to the system will typically require a password, but this may not be necessary on a secure network. Upon access to the system a user will have the option to display a list of all of the information objects which he or she has signed or is being asked to sign. For each object, the display can include the following information:

- Object name
- Description of object (text, mime, size, date)
- List of scheduled signatories
- Date each person signed
- Class of signature for each person
- Electronic signature produced by the secure hash algorithm

If the object is available (viewable) on line, the display may also include a link to display or download the object.

8. Validation of the Object at Time of Signature – If the user downloads or views the object, the system will execute the secure hash algorithm to calculate the electronic signature. This will be displayed so that the potential signer can compare it to the signature calculated at the time the process was initiated. If the user has previously downloaded the object or received it as an attachment to an Email, the user may access the secure hash code through the signature system and apply it to the version on the user's disk.

9. Signing a Document – After the user has determined that an information object is authentic and that the contents merit signature, he or she can affix a signature by authenticating his or her identity. Various means of authentication may be used. The means of authentication may be at the discretion of the manager of the signature system. Such means may include personal identification numbers, passwords, authentication based on computer address or information stored on the signer's computer, third party validation using a public key or other security infrastructure,

Petitioner Apple Inc. - Exhibit 1026, p. 190

or biogenic (fingerprint-recognition, retina scan) methods.

After a document is signed, the date of signature is recorded in a database so that the display to other potential signers is updated. If the signature process is serial, the next person in the sequence is notified. E-mail notice can be sent to all signers when the last signature is collected.

10. Follow-up – At the time a signature process is initiated, the initiator can select a time (in hours, days, or a time or date-certain) for automated follow-up. If a document is not signed within the specified period after notice, a follow-up e-mail can be sent as a reminder. Additional reminders may be sent at the same interval if the object has not been signed. The reminders can be sent automatically by the system according to user-input specifications.

11. Cancellation – The initiator of a signature sequence can modify the sequence at any time, except that a signer can not be deleted from the list once they have signed an object.

12. Transfer of authority – The individual initiating a sequence can transfer the right to modify the list signature list to another individual in the system with appropriate validation of identity.

Document Manager

Successfully conducting commerce over an electronic network requires the exchange not only of messages, but of substantial blocks of information in the form of documents and data. Beyond simply transferring files from hand to hand, it is often necessary for multiple parties to work on a document simultaneously or serially, to track changes, and to maintain a record of versions. Two general architectures have emerged for document management, which can be termed a "mail model" and a "repository model." Under the mail model, documents are attached to messages and circulated person to person. Under the repository model, documents are placed in a central location. There are advantages and disadvantages to each. At a summary level:

	Mail Model	Repository Model

Petitioner Apple Inc. - Exhibit 1026, p. 191

Advantages	Precise routing on a document specific basis. Push in the recipient is informed of a new document. Coupling between document flow and a messaging. Dating is automatic.	Compact storage -- only one version of a file need to be stored. Natural group of files on the basis of subject or access group. Supports good configuration management and version control.
Disadvantages	Creates multiple versions of a document, confounding configuration management and version control. Does not easily couple to online collaboration. Many mail servers limit size of attachment. Relatively high effort to prepare messages.	Not push in the sense that users are automatically informed of new documents. Security model is more complicated than for email. Prior arrangement is necessary to access a repository.

A browser-based document management model and tool combines the best features of repository model and the mail model, for document dissemination and sharing across the Internet or an intranet.

General Architecture – The general architecture of the system combines two basic components: (1) a database of directories and documents and (2) a directory of users. The directory of documents lists documents (of any type) contained in the system, and folders that can contain documents or other folders. The directory of users contains a list of individuals and organizations that can access the system, with passwords and/or other information necessary to validate identity and to establish authority.

Representation of document – The term "document" is used here in the broadest sense of any file that can be stored magnetically or electronically. Preferably, each file is given a unique name consisting of a string of no more than 256 characters. Preferably, the character set is limited to those members of the ASCII character set

Petitioner Apple Inc. - Exhibit 1026, p. 192

which are displayable or printable. Thus, such codes as "escape" which have no visible representation, would be excluded. This is the file name that is displayed for purposes of identifying the document to the users. There is also an actual file name (which is not shown to users) to identify where copies of the file are stored in the central repository. Certain other information is kept in addition to the name of the file. This includes the following:

1. Data of creation
2. Date entered into repository
3. Person who entered the document into the repository
4. Description
5. Size of the document
6. Document type if known
7. Date of last update
8. Access password (optional) stored in encrypted form
9. File folder(s) where the document appears
10. Actual file name

In addition to the above information, data indicating whether the file is checked-out and to what entity, and the identities of entities that have checked the document out and returned it in the past are also stored. The term "checking out" is described further below. These functions related to file change control and configuration management, which are discussed later.

User database – A database contains information on all individuals who can currently access the system or who previously had access up to an administratively determined retention period. This database includes standard contact information including physical and electronic addresses. Security data such as passwords and/or encryption keys is also maintained. In a combined system such as the presently described system, the same database or registry of users can be employed for the document manager as for the signature system.

High level directories – The entire document management system can be divided into a number of high level directories that the user can display, one at a time. These include, at a minimum, a "Private" directory of files and folders visible only to the user, and a "Public" directory of files and folders visible to all users. Additional high-level directories can be created by the system administrator as needed. These

Petitioner Apple Inc. - Exhibit 1026, p. 193

could correspond to projects, business units, or any other logical basis. At any point in the use of the document management system, a user can see and select from the high level directories to which the user has access. The name of the currently open directory can be always displayed on the screen.

Displaying the contents of a high-level directory – When a user selects a high-level directory, the repository displays a series of file folders against the left margin of the active window. File folders whose contents are displayed are shown as open folders. File folders who contents are not displayed are shown as closed folders. A folder is opened or closed by clicking a single time. When a folder is opened, the contents are shown with an indent to indicate the parent/child relationship between the folder and its contents. Each folder can contain files, shown by an icon representing a printed page and other folders, represented by an image of a closed folder.

Information about a folder – Information about each folder is displayed on the same line, to the right of the folder icon. This information is as follows, from left to right:

1. Name of the folder
2. Number of files in the folder, or the word "empty"
3. Accessibility of the folder

Accessibility refers to user access rights to a folder which may private relative to the entity that created it, restricted (limited to a subset of people who can access the high level directory), or shared (available to everyone with access to the high-level directory). The level of access to a directory is indicated by the words "private", "restricted" or "shared."

If the directory is restricted, clicking on the word restricted displays a list of the entities that have access to the folder. This list is a series of hyperlinks. Clicking on the name of a person pulls up detailed contact information (discussed below). The objective is to facilitate communications between people with a shared interest in a file.

Information about a file – Information about a file is displayed to the right of the file icon. From left to right, the first item displayed is the name. This is followed by the word "details." Clicking on "details," causes the document management system to display complete information about the file (see Item 2, above), the person who placed the document in the file, (see Item 3, above), and the person who most recently modified the file.

Petitioner Apple Inc. - Exhibit 1026, p. 194

Information about people/entities, and the link to communications – Information about people/entities with access to the system is displayable at several points in the document manager system:

1. by accessing the directory of users
2. when creating a new folder with "restricted" access
3. when displaying detailed information about a file (see #7)
4. when displaying information about a restricted directory (see #6)

Whenever such information is displayed, contact information from the database is rendered along with the name. Depending on the implementation, this can include complete contact info (multiple addresses, telephone and fax numbers, and email addresses), or some of the contact information may be restricted, in which case it is not displayed.

Creating a new top level folder – A new folder is created within a high-level directory, for example by clicking a button labeled "new folder." This can bring up a dialog in which the user assigns a name to the new folder and selects the type of access (private, shared, or restricted) rights to be assigned. If the document is restricted, the user specifies the entities (organizations and/or people) that can access the folder. If the creator of the folder specifies that an organization has access to a folder, all individuals associated with that organization may be granted access. Folders to which a user does not have access may remain hidden or not displayed. Alternatively, these folders can be shown with some indication that they are not accessible, for example, by ghosting.

Functions related to a folder – Once a folder is defined, a user can execute the following options.

1. Create a subfolder, using the same process described in 9
2. Add a document to the folder, using the process described in 11
3. Delete the folder, if it is empty
4. Modify access to the folder using the same tools used to specify access initially

The functions can be invoked by, for example, clicking on the appropriate label to the right of the name of the folder icon.

Adding a file – Users add a document using a dialog box that prompts for the following information:

Petitioner Apple Inc. - Exhibit 1026, p. 195

1. Location of file - may be entered by user, or selected through a standard file browse dialog
2. Name to be used for the file in the repository
3. Version number or name (optional)
4. Password or encryption key (optional)
5. Description (optional)
6. Access rules (read only or read-write)

After entering the above information, the user either aborts or initiates upload. The information listed above is recorded along with the name of the person entering the document, and date and time.

File options – The following functions may be provided, preferably for every file in the system:

1. Delete (with confirmation)
2. Archive. The file is removed from main repository, but a copy is retained outside the repository. It may be restored though manual intervention.
3. View or download: a copy of the file is brought to the user's computer. This file can be modified there for the individual user's use. A modified version can be uploaded as a new file or different version of a current one, but a file in the repository can only be replaced if the user has it checked out.
4. Check out / check in (see below)
5. Forward (see below)
6. Change Password. The old password must be entered followed by a new password and confirmation.
7. Move: copy or more a document from one folder to another.

The functions may be invoked, for example by clicking on a label corresponding to the function, which can be displayed to the right of the name of the file. Not all options are shown to all users. If an entity does not have write-access to a file, the entity may not delete it, archive it, check it in or out, or change the password.

Check in / Check Out – All entities with write access to a file may check it out. By checking the file out, the entity reserves the exclusive write to save changes to a file. A person may not replace a file that is checked out. To check out a file, the user selects this option from the list of functions associated with the file. The user can

Petitioner Apple Inc. - Exhibit 1026, p. 196

then enter an expected return date and a reason that the file is checked out or the changes to be made. This information is available to all others who can view the file. Each check in or check out is recorded in a permanent log. After a file is checked out, the "check out" button or link is changed to read "check in."

Each individual can check in only the files that he or she has checked out. This is done by clicking "check in." The user may then upload a new version of the file by specifying the location of the file on disk, or indicate that the version of the file currently in the repository is to be retained. After a file is checked in, the check button is changed back to "check out" and the file can be checked out by another user.

Forwarding – A file can be forwarded to any other user of the system. When the forward function is invoked, a list of users is displayed. The sender selects one or more users. Upon confirmation, a copy of the document is placed in folder labeled "in box" in each recipients private directory.

Referring to FIG. 5, a main screen for the document manager creates (using server-side scripting) a user-interface display with some of the features of a Windows Explorer® -type display. File and folder icons are shown along with an array features arranged next to each. The similarities with Windows Explorer® fairly well end there, however. Each of the properties shown next to each file/folder entry invokes a feature.

A parameter object W "Details" invokes a detailed display of the corresponding document object. The details can include contact information about the creator of poster of the document or other data as desired. This data can be hyperlinked and a return button can be provided to return the display back to the screen shown in FIG. 5. Clicking the "details" button to the right of any document brings up the display which can include the name, contact information, and other details about the person who loaded the document into the system, similar information about a person who has the document checked out, and, optionally, a description of the document and information on its change history.

A parameter object X "Forward" simply sends the document to a selected user. A selection screen can be invoked to allow selection of the recipient of the document from the user registry. Of course, since most correspondence can be handled on the server side, the user is, in reality, simply notified of the transfer and

Petitioner Apple Inc. - Exhibit 1026, p. 197

the recipient's action to view the document simply invokes a server side feature to display the document. The document is not actually transferred bodily to the recipient since the recipient, as a registrant logged in the user registry, can access it through the server by requesting to do so.

A parameter object U "Check-in" checks in a document that has been checked out. Other users may view the document, but not modify it when it is checked out. This button is not accessible to users that have not checked the document out and may be displayed ghosted or not displayed at all. A similar button can be displayed if a document that is not checked out may be checked out by the user authorized to see the document manager displayed shown in FIG. 5.

A parameter object T "Download" actually transfers a copy of the document to the client computer. Another object S "Delete" allows the document to be deleted. A new document can be added by clicking "New Document" Q. These are fairly conventional notions, except for their placement on the screen and the fact that each is filtered depending on the user's rights.

Note that when a folder is created, access to the folder can be restricted to the creator, shared with everyone (in which case the folder is created in the public directory), or shared with a select group of other users. The other users can be selected by company or organization (providing access to all individuals in the organization) or by individual within an organization. These are all selectable through a linked selection control where if one selects a company in one selection control, it shows employees in the linked selection control.

A parameter object P "Shared" displays a hyperlinked page that shows all users with access rights to the document. This page allows a user that places a document in the document manager or a user that has pertinent modify rights, to alter the parties that have access to the document. Also, it allows a user with read-only rights to see the list of users that can access that document. The names of the sharing parties are hyperlinked to invoke the user's email client to allow fast sending of email (which again may be performed server-side without actual transfer) or conventionally or selectively. If a folder is shared, the word "Shared" appears to the right of the folder. Clicking on "Shared" brings up the list of person who can access the folder, as shown in FIG. 6. Each name is a hyperlink to detailed contact information.

FIG. 7 shows a list of all deals that were completed through the system. The

Petitioner Apple Inc. - Exhibit 1026, p. 198

trade number (left column of the grid) is a hyper link to detailed information.

FIG. 8A shows detailed information about a completed trade. It shows the party to the trade, the price or rate, and a description of what was traded. The particular nomenclature is specific to a market. For insurance, for example, price is termed rate, and the summary of a deal is the slip sheet. A complete contract can be attached. Included documents can be downloaded to view on line. The intended signatories to a deal are shown (there can be more than two).

If a signatory has actually signed the document electronically, the date and time are shown. No date and time are shown for parties that have not yet signed. The amount of information displayed on the screen is dependent on the identity of the person viewing the screen. The viewer can be blocked from viewing any information about a deal, or certain fields, such as the contract details or the name of signatories.

Note that the detail screen of FIG. 8A would also show attached exhibits. The FIG. 8A display is the basic device for signing deals. A similar device would be used for signing documents.

Referring to FIG. 8B, all of the information necessary to document a deal is pulled together through the screen below. The deal summary includes highly structured information on parties, dates, terms, etc., as well as unstructured information in the form of attachments. The bottom part of the page allows the person registering the deal to designate the intended signatories. When the signers affix their electronic signature, they are doing so to all of the documents in the deal, including the attachments. These are archived and protected from tampering using secure hash technology. In this way it is possible to create a reliable, on line electronic signature to a complex deal, without risk of repudiation.

Note that any number of exhibits can be added to the UI device of FIG. 8B since the list scrolls from the bottom each time a second exhibit is added. The user interface has self-explanatory elements for defining information about the deal.

Anonymous Mail

For purposes of the following description, a "subscriber" is a person or entity that subscribes to an anonymous mail system to be described below. Certain types of negotiations and communications require anonymous initial contact, followed by some period of anonymous discourse, leading to eventual disclosure of the parties'

Petitioner Apple Inc. - Exhibit 1026, p. 199

identities. In the course of a typical sale or business deal, the initiating party begins either by contacting one or more targeted potential trading partners or advertising to a community of potential partners. While the identity of the initial offeror is usually clear in any direct contact, it need not be so in advertising. In certain cases it could be problematic for the initiating party to reveal his or her identity:

A party to a deal can have difficulty controlling the method of contact once the party's identity is known. If a company is known to be in the market for office space, for example, the party may be subjected to badgering by real estate firms outside the established bidding process. Executives of the company may be contacted directly in an effort to influence the decision.

Disclosure of intent may adversely affect the market. If a large company begins to acquire land in an area, the price can rise very quickly. Simple exploration of an option can make the option more costly or even impossible.

Disclosure of intent may adversely impact the reputation or standing of a company. An insurance company that determines that it is over exposed to a certain peril (e.g. hurricane losses in the Southeastern U.S.) would reveal that situation to their competitors and investors by a large public solicitation.

While anonymity can be crucial for the initiator of a deal, it can be equally important for the respondent for the same reasons. The need for controlled anonymity has been addressed by several methods that were initially developed for paper communications and have been extended to analogues in telephonic and computer communications.

- Numbered mail boxes, including government and private
- Communications through a mediator
- Anonymous voice mail drops
- The use of pseudonyms in computer e-mail and dialogs.

These methods have several serious shortcomings:

- The method may only allow anonymity from one side.
- There is no inherent mechanism to validate the credentials and intent on an anonymous party
- Use of a pseudonym may invalidate its future use by associating the name with a specific party

Petitioner Apple Inc. - Exhibit 1026, p. 200

- Manually mediated communications are slow
- The creation and deletion of pseudonyms may not be completely within the control of the party, imposing an overhead cost (in cash or labor) and/or delay in creating a new name
- In most systems, a person with multiple pseudonymous mailboxes or e-mail addresses will receive communications in several different places (mailboxes or accounts), thus requiring multiple logons/passwords.
- Routing of messages received anonymously requires manual forwarding to all relevant parties by the individual with access to the anonymous mail box or email account.
- There is no mechanism to reveal actual identities in a secure and mutually acceptable way.

The present invention addresses these deficiencies by providing two-way anonymous communications, a central point of collection for messages sent to multiple pseudonymous addresses, connection of multiple parties to a single anonymous account, and a mechanism to reveal identities to all parties to a deal simultaneously, by mutual consent. In summary, the anonymous mail system is a server side system that allows clients to create anonymous handles on the fly. It also allows them to share anonymous handles among multiple recipients so that the group of recipients appears as a single recipient to the sender using the anonymous handle. It is like a transparent mailing group. When mail is sent to an anonymous handle, it is sent to all members of the group.

Multiple Systems – In contrast to the first-generation anonymous mail system, the present system allows for multiple anonymous mail (Amail) systems. Each Amail system operates in association with a conventional e-mail server, and uses the e-mail server for communications with non-subscribers, subscribers to Amail systems other than the local one, and for forwarding messages to the subscribers Email client software.

Registration – Subscribers to an anonymous mail system (Amail) each complete a registration that provides:

- Contact information (name, address, telephone number, fax, etc.)
- Information to determine whether they the party is qualified to

Petitioner Apple Inc. - Exhibit 1026, p. 201

participate in the communications exchange. For example, if the system were to be used between and among real-estate agents, registrants to the system might be required to supply a real estate license number.

- Association with an organization (if appropriate)
- Additional information on the individual or organization that may be of use to others in the Amail system to determine the suitability of the party as a partner in negotiations.

The additional information can include such factors as credit ratings, assets, or the region in which the company does business. The specific information required depends on the application. Insurance, real estate, energy marketing, etc. would all have different data of interest.

Validation – Depending on the business model and role of the organization operating the Amail exchange, the organization can either accept the information provided by the subscriber, or verify the information and provide verification as part of the service. Upon acceptance of a subscription applications and validation of the background information if necessary, the use is assigned an Amail user ID and password.

In the first version of the Amail system, logon was automatic from the general application (CATEX); there was no separate user ID and password. In alternative versions, the Amail system can provide its own user ID and password, with the ability to bypass logon when it accessed from other applications with acceptable user validation. All of the actual contact information and validation information are maintained in a database. Validation information was not provided in the first version of CATEX.

Assignment of an Email address – Each subscriber must provide an Internet accessible Email address or be assigned an e-mail address in the Amail system. The first version of the Amail required that the user have an Email address on the system. The new version works directly with e-mail systems other than the Amail.

Logon – Subscribers access the Amail system by connecting an Amail web page provided either over the Internet or on an Intranet. The subscriber enters a user name and password. The first version of Amail was not browser-based and worked only over a LAN or WAN, not over the Internet or an intranet.

Petitioner Apple Inc. - Exhibit 1026, p. 202

Available functions – After logon, the subscriber can access the following functions:

- Manage aliases
- Compose an anonymous message
- Read Amail messages. In the original CATEX system, the user could not access messages from within the Amail application.
- Log off

Managing Aliases – Aliases are directly under user control. After logon, a user can:

- Add a new aliases
- Delete an existing alias
- Create a free-form note associated with a new alias, or edit the note for an existing alias that will be accessible to recipients from the alias.
- Identify other subscribers to whom messages to alias should be forwarded
- Identify other subscribers with permission to generate messages from the alias

These last two features make it possible for a group of subscribers to share an alias, allowing them share communications and work together more effectively. The user will:

Compose an anonymous message – After logon, a user can create and send an anonymous message. After the option is selected, the system will display a message creation screen with the following features:

1. A list of aliases currently owned by the user (i.e. created by the user and not deleted), for the user to select the alias from which the message will originate.
2. A subject box for the mail.
3. A list of the e-mail and alias addresses to which messages can be sent for the user to select one or more. The original version could only send to one alias. The user can also supply an Internet e-mail address off system.
4. A list of the e-mail and alias addresses to which copies of the messages can be sent for the user to select one or more. The user may also supply an Internet e-mail address off system. The original version did not include a "CC" feature.
5. A space where the message can be typed, allowing for users to paste text copies form another system using the Windows-based clipboard utility.

Petitioner Apple Inc. - Exhibit 1026, p. 203

6. A check box to select whether the sender is willing to reveal his identify to the recipient on mutual consent.

7. A check box to select whether the copies of the message should be sent to other subscribers who share the Alias. The original version allowed only one subscriber to access an alias.

Delivery of Messages – After an Amail message has been composed (see step 7), it is delivered as follows.

1. The body of the email message is modified by adding a header including routing information and an indication of whether the sender is willing to reveal identities if there is reciprocal concurrence. The message would appear as shown below. The items in italics are new since the original (prior art) version. The first generation of the anonymous mail system did not allow for communications between multiple Amail systems and, hence, did not list the Amail system name in the list of respondents. The first generation system also did not allow for multiple recipients.

Petitioner Apple Inc. - Exhibit 1026, p. 204

> *This message was sent anonymously from alias: Amail system name: alias*
> The message was sent to:
> Amail system name: *alias*
> Amail system name: alias (cc)
> Amail system name: alias
> The sender is willing to reveal identities.
> [Original body of the message]

2. If the message is sent to a specific, non-anonymous e-mail address, Amail composes and transmits a standard Email message. The sender is listed as "amail.admin.alias@xxxxx" where "xxxxx" is the address of the standard mail server supporting the mail system. Off-system access was not a feature of the first version.

3. If a message is sent to an alias on the local or any other related Amail system, and the owner of the alias has an off system email address, a message is sent as in step 1, above. In addition, however, the message is stored in an Amail message database for access through the Amail system interface. The original version did not have an Amail message database.

4. If a message has been sent to an alias for which there is no associated conventional mail account, the message is stored in the Amail message database. The Amail message database contains a repository for all messages, listing the subscriber(s) associated with the alias to which the message was addressed. The database contains the message (including sender, addressees, and ccs), date and time of transmission, and the alias of the subscriber to which the message was sent. The original version did not have an Amail message database.

5. If the option was checked to send copies to other that share the alias (see above), copies of the message are placed in the message database for the subscribers associated with each of the aliases.

Receipt of Messages – Messages sent from the Amail system can be received in a standard e-mail client by Amail subscribers and non-subscribers.

Amail subscribers can also receive messages through an Amail reader interface. All messages received are placed in the Amail message database (see above). Since an alias can be associated with more than one subscriber, the Amail message database can list more than one subscriber as an "owner" of the message even if it was sent to only one alias. When a user logs on and selects the option to

Petitioner Apple Inc. - Exhibit 1026, p. 205

read Amail messages (see above) the messages are rendered as an HTML page through a browser. Messages to all of the aliases associated with the user are displayed. Each message has a hotlink to respond to send a message back to the sending alias. Each message also has a link to display the background and validation information and note associated with the alias (see above). The original version did not provide an Amail viewer nor did it provide for display of validation information.

Responding from off System from Amail – Individuals from off system can respond to Amail messages using the standard reply feature of their mail server. Messages will be returned to the reply address (see above). Messages received by the conventional e-mail server supporting the Amail system will forward the message to the Amail message repository for the alias listed in the return address. Responding from a standard Email client was not provided in the original version.

Flip Widget

Increasingly, computer applications are delivered through browsers over the Internet or an intranet. There are many design considerations in building a system for browser delivery in contrast to delivery as conventional client server application. Two related considerations are the graphic richness of a browser screen and the time lag to render a new screen. Partly because good web pages contain complex graphics and partly because the Internet can be a relatively slow network, it is important to design a web application to make few unnecessary wholesale screen changes. It is more economical from the perspective of data transmission and, hence, from response time, to create a "flat" rather than "deep" hierarchy of screens, and change only the part of a screen that is minimally necessary.

For example, it is better in a data query to provide a single screen that allows a user to specify a state and city within the state than to provide a first screen for the state, followed by a second screen for the city. As the function of screens becomes more complex, however, it becomes an increasingly difficult challenge to fit all of the options onto the screen (particularly when a user selects a lower screen resolution) and while maintaining a clean appearance. The invention described here provides a tool that allows the Internet application developer to display an effectively unlimited number of options in a very small space using a very familiar and intuitive display feature.

Appearance – The "Flip Widget" tool renders a graphical object representing two

Petitioner Apple Inc. - Exhibit 1026, p. 206

rows of file folders, overlapping. The labels on the front row are visible, the labels on the second row are obscured by the front row of tabs, but the edges of the apparent back tabs are visible. The number of the apparent tabs displayed in each row is a function of the screen resolution and the length of the longest label entered by the user.

The Flip Tab – In one embodiment, the rightmost tab on the front row is labeled "FLIP". When a user actuates this tab, the response is as described below.

Database of labels and links – In creating the display, the application programmer enters a set of paired values. Each pair consists of (1) text of the label to be displayed and a tab, and (2) the name of an HTML link, either within or external to the page to be rendered when the tab is selected.

Action – Upon rendering a page containing the flip widget, the two-row tab display shows the first "n" options from the list of labels and links. The value of "n" represents the maximum number that can be displayed while allowing room for the flip tab. Upon clicking any of these tabs, the corresponding link is executed. Upon clicking the flip tab, the two-row tab display is changed to reflect the next "n" options from the list of labels and links, retaining the flip tab on the right. If there are fewer than n options remaining, the flip widget will either display the last n options, or whatever number remain supplement by as many options are needed from the start of the list. Clicking the flip tab when the list has been completed starts the cycle over again with the first option.

Referring to FIGS. 9 and 10, a flip widget in a first state is shown in FIG. 9. In the first state, any of the tabs A through E can be selected and the corresponding set of controls displayed. For example, in FIG. 9, tab B has been selected and the controls 430-432 are displayed. If the flip tab 410 is selected, a next row of tabs is brought forward so that the display appears as in FIG. 10 with tabs F through J showing. In FIG. 10, tab G has been selected and the corresponding controls 435-437 are displayed.

FIGs. 9A and 10A show a more detailed example of how a flip widget can be used to organize functions available to a user. For example, suppose that one application is a commodity futures trading system that permits a user to execute trades, review prices, and obtain other information relating to various metals such as gold, silver, and platinum. As shown in FIG. 9A, for example, controls or functions

Petitioner Apple Inc. - Exhibit 1026, p. 207

430, 431, and 432 (e.g., execute a trade, review current prices, and the like) are associated with a "gold" category and can be invoked easily when that category is at the forefront of the flip widget as shown. Clicking one of the other tabs (e.g., silver tab 400) would bring the functions associated with that category to the forefront while allowing the user to readily select other categories visible behind the front. Clicking "other markets" tab 410 would change the selection of front-row tabs to a different set of categories, as shown in FIG. 10A. The "other markets" tab 410 could be continually clicked to rotate through a plurality of groupings of markets, each having a set of functions or controls associated therewith.

A flip widget can be implemented in conjunction with the first or second embodiments of the present invention in order to permit many different functions to be displayed in a small screen space. The flip widget is a device to organize many different functions in a logical way, and can be used as a tool for building an interface to multiple applications. As one example, in a DCE (described in more detail below), there may exist n functions (e.g. bulletin boards, chat rooms, e-mail, a-mail, transaction engines, and the like) the specific availability of which can be defined by a user who creates the collaborative environment. This collection can change over time. Accordingly, the interface cannot be "hard coded" for a particular user.

One way to represent an indefinite (and potentially large) number of functions in a small space is with tabs resembling a file folder, with a graphic element representing hidden cards, implying that the user can reach the functionality on the cards by paging (i.e. flipping) to them. The flip widget makes it possible to provide a link to a list of applications maintained in a database rather than requiring that they be hard coded. Programming logic for storing folder labels in a database, linking those labels with associated functions and activating them using browser-type buttons, and for performing the display features described above, are conventional and no further elaboration is necessary. Although the "flip widget" provides one method of structuring a user interface to structure a user's view of application functions, other methods can of course be used.

B. DYNAMIC COLLABORATIVE ENVIRONMENT EMBODIMENT

In a second embodiment of the invention, a dynamic, user-defined collaborative environment can be created in accordance with a set of tools and method steps. As explained previously, this system differs significantly from

Petitioner Apple Inc. - Exhibit 1026, p. 208

conventional networked environments in that: (1) the environment (including access and features) is user-defined, rather than centrally defined by a system administrator; (2) each environment can be easily destroyed after completion of its intended purpose; (3) users can specify a group of participants entitled to use the environment and can define services available to those participants, including offering participation to unknown potential users; (4) the networked environment (including access features and facilities) can cross corporate and other physical boundaries; and (5) the environment offers a broad selection of tools that are oriented to communication, research, analysis, interaction, and deal-making among potential group members. Moreover, in a preferred embodiment, the environment is implemented using web browser technology, which allows functions to be provided with a minimum of programming and facilities communication over the Internet.

FIG. 11 shows various method steps that can be carried out to define, create, and destroy an environment according to a second embodiment of the invention. The term "environment" as used herein refers to a group of individuals (or computers, corporations, or similar entities) and a set of functions available for use by that group when they are operating within the environment. It is of course possible for one individual to have access to more than one environment, and for the same functions to be available to different groups of people in different environments.

The process of creating a collaborative environment involves the migration of tools and information resources available in the library of the environment generator into a specific collaborative environment. The collaborative environment can include / link to any application available to the environment generator. It can also include applications specific to the environment provided that theses are accessible through Internet protocols.

Underlying the environment is a directory of users, information about users, and their authorities. The core structure for the environment user database should conform to a directory standard – typically DAP (Directory Access Protocol) or LDAP (the lightweight directory access protocol). The environment generator has access to its own directory of users and to the user directories of the environments it has generated. The directory of an environment can be populated initially by selecting users from the environment generator's directories. These are added to the directory of the environment in one of two ways depending on the

Petitioner Apple Inc. - Exhibit 1026, p. 209

specific implementation. Directory records can be copies from the environment generators user database to a separate database for the environment or a flag can be added to the user data record in the environment generators users database to indicate that the user has access to the environment. The second, simple model is useful when all users in an environment have equal authority. A separate user database (directory) is necessary for an environment when the environment has its own security / authority model.

Additional members can be added through a set of standard application / subscription routines. These then become known to the environment generator (as well as the specific environment) providing the foundation for greater speed and efficiency in creating subsequent environment.

Beginning in step 1101, a new group is created by identifying it (i.e., giving it a name, such as "West High School Research Project," and describing it (e.g., providing a description of its purpose). The process of creating a group and defining functions to be associated with the group can be performed by a user having access to the system without the need for system administrator or other similar special privileges (e.g., file protection privileges, adding/deleting application program privileges, etc.). In this respect, environments are, according to preferred embodiments, completely user-defined according to an easy-to-use set of browser-driven user input screens. The principles described herein are thus quite different from conventional systems in which a central system administrator in a local area network can define "groups" of e-mail participants, and can install application programs such as spreadsheets, word processing packages, and the like on each computer connected to the network. Moreover, according to various preferred embodiments, the facilities provided to group members can be provided through a web-based interface, thus avoiding the need to install software packages on a user's computer.

It is also contemplated that various methods of obtaining payment for creating or joining groups can be provided. For example, when a new environment or group is created, the person or entity creating the group can be charged a fixed fee with payment made by credit card or other means. Alternatively, a service fee can be imposed based on the number of members that join, the specific functions made available to the group, or a combination of these. Moreover, fees could be charged

Petitioner Apple Inc. - Exhibit 1026, p. 210

to members that join the group. The amount of the fee could also be based on the length of time that the environment exists or is used.

Although not specifically shown in FIG. 11, step 1101 can include the step of creating a new entry in a database table (e.g., a relational or object-oriented database) to store information concerning the new group and the environment in which the group will operate. Database entries related to the group, including some or all of the information described below, can be created as the environment is defined. It is assumed that one or more computers are linked over a network as described in more detail below in order to permit the environment to be created, used, and destroyed, and that a database exists on one or more of these computers to store information concerning the environment.

In step 1102, the group members are identified. According to various embodiments, the group members can be identified in three different ways (or combinations thereof), as indicated by sub-steps 1102a, 1102b, and 1102c in FIG. 11. It is contemplated that group members can span physical networks and computer systems, such as the Internet. Consequently, group members can include employees of different corporations, government agencies, and the like. In contrast to conventional virtual private networks, both the group members and the functions made available to those group members are entirely user-selected, thus permitting a broad range of persons to easily create, use, and destroy virtual private networks and associated functionality.

First, in step 1102a, group members can be identified by selecting them from a list of known users that are to be included in the group. For example, within a corporation or similar entity, a list of internal e-mail addresses can be provided, or an electronic version of a phone list or other employee list can be provided. If the hosting computer system is associated with a school, then a list of students having accounts on the computer (or those in other schools that are known or connected to the host) can be provided. From outside a corporate entity, users can be selected based on their e-mail addresses (e.g., by specifying e-mail addresses that are accessible over the Internet or a private or virtually private network). In this step, the environment creator specifies or compels group members to belong to the group.

Second, in step 1102b, group members can be invited to join the group by composing an invitation that accomplishes that purpose. For example, a group

Petitioner Apple Inc. - Exhibit 1026, p. 211

creator may choose to send an invitation via e-mail to all members of the corporation, or all members of a particular department within the corporation, all students in a school or region, or members of a previously defined group (e.g., the accounting department, or all students in a particular teacher's class). The invitation would typically identify the purpose of the group and provide a button, hyperlink, or other facility that allows those receiving the invitation to accept or decline participation in the group. As those invited to join the group accept participation, their responses can be stored in a database to add to those members already in the group. Invitations could have an expiration date or time after which they would no longer be accepted. As invitees join the group, the group creator can be automatically notified via e-mail of their participation.

Third, in step 1102c, group members can be solicited by way of an advertisement that is sent via e-mail, banner advertisement on a web site, or the like. Persons that see the advertisement can click on it to join the group. It is also possible for advertisements to have a time limit, such that after a predetermined time period no more responses will be accepted. The primary difference between advertising participation in a group and inviting participation in a group is that invitations are sent to known entities or groups, while advertisements are displayed to potentially unknown persons or groups.

It will be appreciated that group members can be selected using combinations of steps 1102a, 1102b, and 1102c. For example, some group members can be directly selected from a list, while others are solicited by way of invitation to specifically identified invitees, and yet others are solicited by way of an advertisement made available to unknown entities.

In step 1103, the functions to be made available to the group are selected. For example, the group can be provided with access to an auction transaction engine; a survey tool; research tools; newswires or news reports; publication tools; blackboard facilities; videoconferencing facilities; and bid-and-proposal packages. Further details of these facilities and tools are provided herein. The group creator selects from among these functions, preferably by way of an easy-to-use web browser interface, and these choices are stored in a database and associated with the group members. Additionally, the group creator can specify links to other web-based or network-based applications that are not included in the list by specifying a web site

Petitioner Apple Inc. - Exhibit 1026, p. 212

address, executable file location, or the like. The group creator can also define shared data libraries that will be accessible to group members.

In step 1104, the environment is created (which can include the step of generating a web page corresponding to the group and providing user interface selection facilities such as buttons, pull-down menus or the like) to permit group members to activate the functions selected for the group. In some embodiments, access to the group may require authentication, such as a user identifier and password that acts as a gateway to a web page on which the environment is provided. Other techniques for ensuring that only group members access the group functions and shared information can also be provided. A web page can be hosted on a central computer at an address that is then broadcast to all members of the group, allowing them to easily find the environment.

In step 1105, group members collaborate and communicate with one another using the facilities and resources (e.g., shared data) available to group members. In the example provided above, for example, a group of high school students collaborating on a school research project could advertise for survey participants; conduct an on-line survey; compile the results; communicate the results among the group members; brainstorm about the results using various brainstorming tools; conduct a videoconference including group members at various physical locations; compile a report summarizing the results and exchange drafts of the report; and publish the report on a web site, where it could optionally be offered for sale through the use of an on-line catalog transaction engine. The group could even contact a book publisher and negotiate a contract to publish the report in book form using bid and proposal tools as described herein.

In step 1106, after the environment is no longer needed, it can be destroyed by the person or entity that created the group. Again, in contrast to conventional systems, the destruction of the environment is preferably controlled entirely by the user that created the environment, not a system administrator or other person that has special system privileges. Destruction of the environment would typically entail deleting group entries from the database so that they are no longer accessible.

FIG. 12 shows one possible system architecture for implementing the steps described above. As shown in FIG. 12, an Internet Protocol-accessible web server 1201 is coupled through a firewall 1202 to the Internet 1203. The web server includes

Petitioner Apple Inc. - Exhibit 1026, p. 213

an environment generator 1201a which can comprise a computer program that generates user-defined environments as described above. Further details of this computer program are provided herein with reference to FIG. 21.

Web server 1201 can include an associated system administrator terminal 1204, one or more CD-ROM archives 1205 for retaining permanent copies of files; disk drives 1206 for storing files; a database server 1207 for storing relational or object-oriented databases, including databases that define a plurality of user-controlled environments; a mail server 1208; and one or more application servers 1209 that can host application programs that implement the tools in each environment. Web server 1201 can also be coupled to an intranet 1210 using IP-compatible interfaces. Intranet 1210 can in turn be coupled to other application servers 1211 and one or more user computers 1212 from which users can create, participate in, and destroy environments as described herein, preferably using standard web browsers and IP interfaces. Web server 1201 can also be coupled to other user computers 1217 through the Internet 1203; to additional application servers 1215 through another firewall 1216; and to another IP-accessible web server 1213 through a firewall 1214.

It will be appreciated that the system architecture shown in FIG. 12 is only one possible approach for providing a physically networked system in which user-defined network environments can be created and destroyed in accordance with the principles of the present invention. It is contemplated that application programs that provide tools used in a particular user-defined environment can be located on web server 1201, on user computers 1217, on application servers 1215, on application servers 1209, on application servers 1211, or on any other computer that provides communication facilities for communicating with web server 1201. It will also be appreciated that web pages that provide access to each user-defined environment need not physically reside on web server 1201, but could instead be hosted on any of various computers shown in FIG. 12, or elsewhere.

Reference will now be made to exemplary steps and user interfaces that can be used to carry out various principles of the invention, including steps of creating a group, selecting group members, and defining functions to be made available to group members in the environment.

FIGS. 13A through 13C show one possible user interface for creating a group

Petitioner Apple Inc. - Exhibit 1026, p. 214

and identifying group members. In FIG. 13A, a user gains access to an environment creation tool by way of an authentication process. This may be a simple username and password device as shown in FIG. 13A, or it could be some other mechanism intended to verify that the user has access to the environment creation tool. In the case of a corporation, school, or other entity that already provides a log-in procedure to access the entity's network, such log-in procedure could serve to authenticate the user for the purpose of creating a new environment. It should be appreciated that user authentication is not essential to carrying out the inventive principles. Moreover, although it is contemplated that for ease of use (and to minimize programming) web browsers and web pages be used to receive user-defined information to create each environment, other approaches are of course possible.

In FIG. 13B, the user is prompted to create a new group by supplying a group name (e.g., "Joe's Homework") and a brief description of the group. This information is preferably stored in a database file and associated with group members and functions available to those group members.

In FIG. 13C, the user is prompted to identify group members. As described previously, group members are preferably identified in one of three ways (or combinations of these): (1) selection from a list of known group members; (2) inviting known candidates to join the group; or (3) advertising for new members. When the user clicks one of the options in FIG. 13C, he or she is prompted to supply additional information as shown in FIGS. 14A through 14C.

Beginning with FIG. 14A, for example, group members can be individually specified by entering an e-mail address (e.g., an internal or external e-mail address) in a text form data entry region and/or by selecting from a previously known list. This screen permits the user to compel attendance in the group by specifying names and/or e-mail addresses to which group messages will be sent. All those added to the group in this manner will be provided with access to the environment corresponding to the group. Aliases and pre-defined groups could also be specified as the basis for membership (e.g., all those in the accounting department of a corporation, or all students in a high school).

Each member of a group might have a group email account, or they may use an off-system email account. Off-system email addresses can be maintained in a database of users. Mail sent to the group email address is preferably forwarded off-

Petitioner Apple Inc. - Exhibit 1026, p. 215

system, protecting the actual email address of the person unless that person wishes to give out that address. New members can be added until the group is completed. Although not explicitly shown in FIG. 14A, it is contemplated that new members can be added to a previously defined group after the environment has already been created.

When group members are selected or specified, the user creating the environment can also create a password for each user in the group in order to enable those in the group to access the environment. Alternatively, when a user visits the environment, the environment can retrieve a "cookie" from the user's computer to determine whether the user is authorized to access the environment. If no cookie is available, the user could be prompted to supply certain authentication information (e.g., the company for whom he or she works, etc.) In yet another approach, authentication could occur by way of e-mail address (i.e., when the user first visits the environment, he or she is prompted to enter an e-mail address). If the e-mail address does not match one of those selected for the group, access to the environment would be denied.

Turning to FIG. 14B, prospective group members can also be "invited" to join the group. The user creating the environment can specify one or more e-mail addresses to which an invitation will be sent. The invitation can be a simple text message, or it could be a more sophisticated video or audio message. An expiration date can also be associated with the invitation, such that responses to the invitation received after the date will not be accepted. Software resident in web server 1201 (FIG. 12) receives responses to the invitations and adds members to the appropriate group or drops them if the expiration date has passed or the prospective group member declines participation. Prospective members can join the group by sending a reply with a certain word in the message (e.g., "OK" or "I join"); by clicking on a button in an e-mail message; or by visiting a web site identified in the invitation.

Turning to FIG. 14C, group members can also be solicited by creating an advertisement directed primarily at potential group members that are unknown. The advertisement could include, for example, a banner ad comprising text, video, and/or audio clips. The graphic should conform to the size designated for the ad on the web page. The ad could be posted on a web site by uploading the graphic through a web interface and, optionally providing a URL on the screen of FIG. 14C to link to if the

Petitioner Apple Inc. - Exhibit 1026, p. 216

advertisement is clicked. Software on the group page can render advertisements on a page either (a) every time the page is displayed, (b) in rotation with other ads; or (c) when characteristics of the user match criteria specified for the ad.

The advertisement can include an expiration date after which responses would no longer be accepted. Advertisements could range from the very specific (e.g., an advertisement posted on a school's home page advertising participation in Joe's research project on drug use at the school) to more general (e.g., an advertisement that says "we're looking for minority contractors looking to establish a long-term relationship with us" that is posted on web sites that cater to the construction industry.

A qualification option can also be provided to screen prospective group members. For example, if an advertisement seeks minority contractors to participate on a particular construction project, selecting the "qualify" option would screen responses by routing them to the user that created the group (or some other authority) before the member is added to the group. Those responding to the advertisement could be notified that they did not pass the qualifications for membership in the group, or that further information is required (e.g., documents evidencing qualifications) before participation in the group will be permitted. Alternatively, an automatic qualification process can be provided to allow a prospective member to join if the person fills in certain information on the response (e.g., e-mail address, birthdate that meets certain criteria, or the like).

As shown in FIG. 15, a banner ad displayed on a web site invites minority contractors to join a group that bids on information technology contracts. Those interested in the advertisement click a button, which leads them to another site (not shown) requiring that they provide certain information (qualification information, name, age, company registration information, etc.) This information is then forwarded to web server 1201 which either pre-screens the information according to pre-established criteria, or notifies the user creating the group that a prospective member has requested access to the group. In the latter case, the user could screen the applicant and grant access to the group.

FIG. 16 shows one possible user interface for selecting communication tools to be made available to group members. This screen can be presented to the user creating the environment after the group has been identified and its members

Petitioner Apple Inc. - Exhibit 1026, p. 217

selected. It is contemplated that a variety of communication tools can be provided, including a bulletin board service; advertisements; white pages (e.g., a listing of members, their e-mail addresses, telephone numbers, and the like); yellow pages (e.g., a listing of services or companies represented by group members, with promotional and contact information); document security (e.g., shared access secure document storage services); anonymous e-mail (described above with respect to the first embodiment); threaded dialogs; a group newsletter creation tool; videoconferencing; and even other user-provided applications that can be specified by name and location (e.g., URL). Details of these services are provided below.

According to various preferred embodiments, dynamic collaborative environments are designed to integrate tools from multiple sources provided that they are web-accessible (i.e., they operate according to Internet Protocol and/or HTML-type standards). The categories listed above provide a reasonable taxonomy of the tools necessary for collaboration, but this list can be extended to include virtually every class of software such as computer-assisted design, engineering and financial analysis tools and models, office applications (such as word processing and spreadsheets), access to public or proprietary databases, multimedia processing and editing tools, and geographic information systems. The following describes some of the communication tools that can be provided:

Bulletin boards. A bulletin board (see, e.g., FIG. 2) lists notices posted by group members, which may be offers to buy or sell, but need not be limited to such offers. Many types of bulletin board services are of course conventional and no further discussion is necessary in order to implement one of these services. Nevertheless, in one embodiment the following data items (attributes) can be provided for each notice appearing on the bulletin board: an item number, a title, the date posted, and one or more special attributes defined by the user. The attributes may include a field to indicate whether a listing is a "buy" or "sell " offer. The board can be provided with an integrated sorting capability. By clicking on the heading of each column, the user can sort the entries in, alternately, ascending or descending order. Thus, it is possible to organize the records from oldest to newest or newest to oldest, or to separate buy and sell offers. To limit the values on a board, a search capability can also be provided, such that only those entries that meet the search criteria are displayed.

Petitioner Apple Inc. - Exhibit 1026, p. 218

Advertisements. In a typical environment of a dynamically created network there are a number of fixed places for advertisements – the top of a page for a banner, the bottom of a page for a banner, and space on the side for small ads. The creator of the environment may choose to use none, any, or all of these spaces for advertisements. Once a space is designated for advertising, group members may place adds by completing a template that provides payment information (if required), the text for the ad (any standard image format), and a link to be executed if the ad is clicked by someone viewing the ad.

Each user is responsible for providing functionality behind the link. The ad may be displayed persistently (every time a page is displayed), in rotation with other ads for the same place, or may be triggered on the basis of user characteristics including purchasing history. Revenue can be collected for placement (fixed price regardless of how many times an ad is displayed), per time that the ad is displayed, or per click on the ad. The virtual private network provides the front-end to facilitate online placement of the ad. Display can be done by linking pages to standard ad display code, available off the shelf from several sources. This code provides for rotation of the ads. Software for customization (i.e. choosing the ad based on user characteristics) is available commercially from several sources.

White pages. White pages provide a comprehensive listing or directory of members with information about them and information regarding how to contact them. Various types of commercially available software can be used to manage such directories, and it is elementary to code typical directories that have fixed contents for each member.

A web-accessible directory can be used in accordance with various embodiments of the invention. One type of directory that can be provided differs from directories having fixed structures. The key differences are as follows:

(a) User control over information Users enter and maintain their own information directly, rather than through a central organization. This provides more immediate update of data and reduces transcription errors. It makes it simple, for example, for people to change their phone number when they are temporarily working at another location.

(b) Multiple points for quality control. The data regarding each user can be displayed to the user periodically (e.g.30, 60, and 90 days), and the user prompted to

Petitioner Apple Inc. - Exhibit 1026, p. 219

update and verify the data. A feedback capability can be provided for members of a group to report errors they find. Email addresses can be "pinged" periodically to determine if they still exist. In addition, server management staff can periodically review accounts that have had recent activity.

(c) Object structure. A directory entry consists of a collection of data elements. These elements include such things as name for addressing (Dr. John D. Smith), sort name (Smith, John D), or primary work telephone (800-555-1212). Traditional mail systems have a fixed number of rigidly formatted elements. In one embodiment, a more flexible approach can be used in that individuals identify which elements they wish to add to the collection comprising their directory entry. For example, a person can add 3, 4, 5 or more telephone numbers attaching a note to each explaining its use (e.g. "for emergencies after 8PM").

(d) Direct link to communications tools. Where a directory refers to a contact method (e.g. a telephone number), the method can be invoked directly from an entry if the necessary software is available. For example, phone number can be dialed, email messages initiated, or a word processing session initiated with letter and envelope templates, preloaded with address information.

(e) Descriptive information. In addition to contact information, each directory can contain information describing the entry (individual or business). The description can be different in each group or it can be the same. The descriptive is free form, with the exception that the user may drop in terms from a group-specific lexicon. This lexicon can include terms specific to the industry (e.g. "fuel system") for the automotive industry, or preferred forms of standard terms (e.g. "California" rather than "CA", "Ca", or "Calif."). Standardization of terms in this way makes search the directory more reliable.

Yellow pages. Conventional "yellow pages" products provide a one level classification of directory entries designed to facilitate identification of and access to an individual or organization with specific interests and capabilities. Within industries, and particularly online, multi-level hierarchical directories are common, with the multiple levels providing more precise classification. There are numerous commercial products for maintaining online yellow page type classification systems.

Any web-accessible directory can be connected to a DVPN group. A preferred method offered with the system integrates the classification system with the

Petitioner Apple Inc. - Exhibit 1026, p. 220

descriptive field in a directory entry. Every time a standard term pertaining to a classification is pulled from the lexicon, the entry is added to that classification in the hierarchical sort. In addition to hierarchical access, this correspondence between the traditional hierarchical sort and the free-form description with standardized terms makes it possible to access records via search rather than browsing the hierarchy. Searching makes it possible to identify an organization with multiple capabilities (e.g. "brake repair" and "frame straightening"). This search capability is much like a general web-search using a tool like AltaVista's or Inktomi's search engine and can use the same search engine, but differs in that material being search is in a precisely defined domain (group members), the information being searched is limited and highly quality controlled (i.e. group directory entries), and has a precision rooted in a precise vocabulary (the lexicon used in preparing the description).

Document repository. Any commercial web-enabled document repository can be integrated into a group. Examples are Documentum and PC DOCs. An improved version offered specifically with the DVPN package was described above.

Document security. Within the document repository various tools can be provided to protect the security of documents. These include (1) limiting access to a document to certain people or groups; (2) only displaying the directory entry for documents to people who can access it; (3) password protection; (4) encryption; (5) secure archive in read only mode on a third-party machine; (6) time-limited access and (7) a secure hash calculation.

All of the above are conventional except for time-limited access and the secure hash calculation. Software for limiting access to a document to a certain period is available from Intertrust, among others. A secure hash is a number that is characteristic of the document calculated according to a precisely defined mathematical algorithm. There are several secure hash algorithms, and implementers can develop their won. They are "trap door" in nature. That is, the calculation can be performed with reasonable effort, but the inverse of the function is computationally intractable. The classic example of a trap door function is multiplication of very large prime number (on the scale of hundreds of digits). The product can be calculated with relative ease, but factoring the product (the inverse function) is very time consuming, making if effectively impossible with generally available hardware. This method is used in public key encryption, but can be applied

Petitioner Apple Inc. - Exhibit 1026, p. 221

equally well in secure hash, though other trap door functions are preferred, in particular, the one specified by the U.S. Department of Commerce as FIPS standard 180. Code to implement this standard can be developed from published algorithms.

Anonymous e-mail (described above with respect to the first embodiment);

Threaded dialogs. Threaded dialogs are a collection of messages addressing a specific topic, added serially, not in real time. They are threaded in the sense that new topics can branch off from a single topic, and topics can merge. According to one embodiment, threaded dialogs differ from conventional news group functionality in that (1) users can initiate new topics; (2) users can post a message to one topic, then indicate that the message pertains to other topic as well; (3) browsers reading a message may continue down the original thread or one of the alternates if other topics are suggested.

Group newsletter creation tool. A newsletter creation tool can be used to link columns provided by multiple users (and maintained as separate web documents) into a whole through an integrating outline maintained by an "editor". The purpose of the tool is to provide the look and feel of an attractive single document to a disparate collection. To create the newsletter the editor generates an outline identifying an author for each component and a layout. Art for the first page can be provided. Through messaging, the authors are provided a link to upload their content. Content is templated to include a title, date, a by line, one or more graphic elements, a summary for the index, and text. The editor may allow documents to go directly to "publication" or require impose a review and editing step.

Chat groups. Real time chat room software is widely available from many sources including freeware and shareware.

Audio and videoconferencing. Commercially available tools for web-based audio and video conferencing can be included in the group functionality. Examples are Net Meeting and Picture Tel software.

FIG. 17 shows one possible user interface for selecting research tools to be made available to group members. As shown in FIG. 17, various tools such as a mortgage calculator, LEXIS/NEXIS access, news services, Valueline, and other research tools can be provided by checking the appropriate box on the display. All of these research tools are conventional and commercially available (via web-based links and the like).

Petitioner Apple Inc. - Exhibit 1026, p. 222

FIG. 18 shows one possible user interface for selecting transaction engines to be made available to group members. As shown in FIG. 18, many different types of transaction engines can be provided to group members, including electronic data interchange (EDI) ordering; online catalog ordering; various types of auctions; sealed bids; bid and proposal tools; two-party negotiated contracts; brain writing (moderated online discussion) and online Delphi (collaborative estimation of a numerical parameter). The following describes various types of transaction engines in more detail. Enhanced features (i.e., those that differ from conventional products) are highlighted in gray text.

A. Order placement (online catalog) transaction engine

An order placement or online catalog engine allows the buyer to place an order for a quantity of items at a stated fixed price, essentially ordering from an online catalog. The catalog contains the description and specification of the offerings. The catalog may be publicly accessible (Subtype 1a) or provided for a specific customer (Subtype 1b). Prices are included in the catalog but may be customer specific, may vary with quantity purchased, terms of delivery and performance (e.g. cheaper if not required immediately). The catalog can represent a single company's offering or an aggregate of the offerings from several companies. The catalog can range from a sales-oriented web site designed for viewing by customers, to a engine designed only accept orders sent via electronic data interchange (EDI). Note that the catalog can be shopper oriented (i.e. designed to sell) or a simple, machine-readable list of available items and prices. The following describes in more detail steps that can be executed to create an online catalog:

1. Enter and maintain a framework for catalog
    1.1. Enter / delete / edit categories. Categories are titles for groups of items, such as "furniture" or "solvents"
    1.2. Enter / delete / edit subcategories. Subcategories are categories within categories, effectively establishing a hierarchy of products. Example: furniture/dining room/tables.
    1.3. Create groups of categories and subcategories (e.g. "see also...."). The grouping allows a person browsing items to be referred to another category that may contains items of interest. For example, someone may reach the furniture/dining room/tables and then be referred to

Petitioner Apple Inc. - Exhibit 1026, p. 223

furniture/office/conference room tables where other suitable tables may be listed, or to furniture/dining room/chairs to buy chairs that make the table. This cross-referencing transforms the hierarchical arrangement of categories into a web.

2. Enter / edit / delete items in catalog by entering and updating the information listed below. The system allows users to enter this information and provides basic quality assurance.
   - 2.1. Catalog item number
   - 2.2. Supplier part number(s)
   - 2.3. Name of item
   - 2.4. Description
   - 2.5. Photos and drawings
   - 2.6. Specifications (depends on item type). Different items have different specifications. For example, a computer printer can have color vs. black and white, dots per inch resolution, paper size, etc. In contrast to a fixed, hard coded catalog, the specification section of the general purpose catalog engine the user prepares the specification section by selecting parameters from a list and then specifying a value for that parameter. The parameter list contains values such as length, width, height, voltage, color, resolution etc. It is can be extended by the manager of the auction environment. A lister selects a necessary parameter (e.g. length, then enter the value, such as 14"). The specification section is a concatenation of individual specifications.
   - 2.7. First available date
   - 2.8. Last available date
   - 2.9. Category (categories) into which the item fits
   - 2.10. Alternate suggestion(s) if product not available
   - 2.11. Related and associated products (e.g. printer supplies for a printer or other household items with the same pattern.
   - 2.12. Additional information at the option of the individual or organization listing the item.
3. Enter / update pricing information
   - 3.1. Simple price. The fixed prices is per item or per unit. The price must

Petitioner Apple Inc. - Exhibit 1026, p. 224

specify the

3.2. Pricing algorithm -- link to code for pricing algorithm

4. Take Orders

There are two variants: 4a: manual purchase in which a person browses a catalog and selects and item for purchase and 4b: automated order in which a purchase is initiated by an electronic message.

Variant 4a: Manual Purchase

4.1. Potential buyers access the catalog by drilling down through the category / subcategory tree or

4.2. Buyers search fields in catalog to identify the appropriate item. The search may examine the title, description, or any of the specification fields.

4.3. Display general information for item(s) meetings specifications

4.4. Allow user to modify search or to select specific item if the items displayed to do not meet his requirements

4.5. Display detailed information for selected item

4.6. Display the fixed price or calculate price if prices is based on an algorithm. The pricing algorithm may include parameter such as characteristics or affiliation of the users (e.g. affiliated with a pre-negotiated discount program) , delivery date and mode, and quantity.

4.7. Offer the option to purchase or search again if they choose not to purchase.

4.8. If the buyer opts to proceed with the purchase, then check the availability of the item by linking to the sellers inventory system

4.8.1. If the item is available then execute an 'add to basket'. That is, place it on a list of items designated for purchase.

4.8.2. If the item is not available, then execute the contingent response:

4.8.2.1. Offer delivery at predicted date

4.8.2.2. Terminate the sale, but offer to deliver or notify when next the item is next available.

4.8.2.3. Suggest alternate items

4.8.2.4. Report 'sorry' and abort transaction

4.9. Offer option to purchase addition options

4.9.1. If offer is accepted, execute from step 4.1

4.9.2. If offer is not accepted, proceed with step 4.10

Petitioner Apple Inc. - Exhibit 1026, p. 225

4.10. Conclude the transaction

4.10.1. Collect shipping information, offer options

4.10.2. Collect payment information

4.10.3. Validate payment

4.10.4. Summarize order

4.10.5. Obtain final authorization

4.10.6. Generate receipt

Variant 4b: automated order, done using an EDI (electronic data interchange) message

4.1 Accept requests for item

4.2 Return price and confirmation of availability

Note that users may conduct transactions without employing EDI. It is possible, however, for members to agree on a transaction EDI format either by completing a template within the system or selecting a pre-established EDI format from a library. This library can include formats developed by recognized standards organizations (e.g. UNEDIFACT or ANSI) or formats developed specifically for an industry or a trading environment. Once there is agreement on a format, transactions can be initiated, concluded, and confirmed through the exchange of appropriate EDI messages. As many commercial ordering, accounts payable, accounts receivable and enterprise resource planning systems have an EDI interface the collaborative environment should have the capability to forward the message to the order fulfillment system.

B. English Auction Transaction Engine

In an English Auction, a single item is offered for sale to many buyers. The auction can be open or limited to pre-qualified bidders. The buyers offer bids in turn, each succeeding all prior bids. The highest bid received at any point in the auction is visible to all buyers. The identity of the highest bidder may or may not be visible to traders. Buyers may increase their bids in response to this information. Award is to the highest bidder at the end of trading. The end of trading is reached when there are no higher bids during an interval that may be formally defined or determined by the manager of the auction at the time of execution.

There are two models for the access to the transactions. In the first model, all buyers and sellers are members of the group. In the second model, all sellers are

Petitioner Apple Inc. - Exhibit 1026, p. 226

members of the group, but buyers can include members and non-members. If non-members are allowed to buy, the creator the transaction must enter a new URL for buyers. This is a sub-URL of the main group URL. A registration process may be established for the buyer URL.

In live auctions (as opposed to online) all traders are connected at the same time, and the duration of the auction is brief – typically only a few minutes. In online trading, it is not necessary for all of the bidders to be present (i.e. connected at the same time). To distinguish between these two options they are designated (a) concurrent (everyone bidding at the same time) and (b) batch (not everyone connected simultaneously. The manager of the auction can set the minimum bid and the minimum increment.

1. The first step in conducting an auction is to collect information on the items being offered for sale. This is done online. The information collected includes:
    1.1. Identity of seller. Note that the business rules of the auction may require advance registration of sellers to verify their identity.
    1.2. Descriptions, optionally including attachments and photographs, independent certifications or appraisals, and anything else in digital form necessary or useful in determining the value of the item.
    1.3. Reserve price
    1.4. Minimum increment
    1.5. Time offered for sale
    1.6. Time bidding is scheduled to end
    1.7. Verify the seller's consent to the rules of the auction house regarding delivery, payment, responsibility for non payment, etc.
2. If the business rule of the auction house is to require payment up front, collect payment either by:
    2.1. Debiting a deposit account
    2.2. Charging to account for billing
    2.3. Collecting online payment such as through a credit card.
3. Post information about auction, including:
    3.1. Description of items to be auction
    3.2. Auctions rules:
        3.2.1. Qualification process for bidders

Petitioner Apple Inc. - Exhibit 1026, p. 227

3.2.2. Time of bidding

3.2.3. Criterion for ending bidding – time between bids

3.2.4. Legal statement – responsibilities of buyer and seller, limitation of liability

4. Execute qualification process (optional)

4.1. Admit bidders who are qualified based on past participation

4.2. Provide fill-in-the blank qualification form new bidders

4.3. Collect information

4.4. Conduct automated review or manual review

4.5. Inform prospective bidder of qualification or not

Variant (a): concurrent auction

5. Conduct Auction

5.1. Fifteen minutes prior to appointed time for auction, display "Welcome" screen with space for qualified bidder to enter an alias or handle to be used in the auction. Screen should have a description of the object. Show time until auction starts. Auto refresh at 15 second intervals.

5.2. At appointed time, display the main auction page with the following information:

5.2.1. Description / picture of item for auction stored in a separate, static frame of the PC so that it does not need to be downloaded each cycle.

5.2.2. Current bid (initially the reserve price)

5.2.3. Suggested next bid (e.g. current + 3 * increment)

5.2.4. Button to accept suggested next bid

5.2.5. Field to enter bid higher than suggested next

5.2.6. Handle of the highest bidder

5.3. Refresh main auction page at 15 second intervals

5.4. Collect bids, either

5.4.1. Notice that the suggested bid was accepted

5.4.2. Bid higher than accepted bid

5.4.3. If new bid is lower than current highest, disgard

5.4.4. If higher than current highest then

5.4.4.1. Log identity of highest bidder

5.4.4.2. Update highest bid

Petitioner Apple Inc. - Exhibit 1026, p. 228

5.4.4.3. Update next suggested bid

6. If nobody accepts the suggested bid, then

6.1. Reduce suggested next bid

6.2. If accepted, resume normal sequence

6.3. If not accepted, reduce suggested next bid

6.4. If accepted, resume normal sequence

6.5. If not, begin close

6.6. "Going once ...", if response, resume normal sequence, else

6.7. "Going twice ..." if response, resume normal sequence, else

6.8. Done. Display closing screen

7. Settle with winning bidder, two models

7.1. Connect buyer to seller for direct settlement

7.2. Collect money from buyer, deduct fee, convey amount to seller

Variant (b): batch (i.e. time limited) auction

Conventional on-line batch (time limited) auctions are common. E-bay is the most prominent example. This process description continues from step 4 of the English auction description as the startup of the concurrent and batch auctions are the same.

5. Conduct auction: Until closing time for an item:

5.1. On entry to system display the following for the potential buyer:

5.1.1. Latest listing

5.1.2. Categories

5.1.3. Search screen

5.2. On selection of categories:

5.2.1. Execute dill down

5.2.2. Retrieve count of items that meet criteria

5.2.3. If more count is less than 25 (or other small number (n) consistent with the layout of the screen) retrieve all items that meet criterion

5.2.4. If count is more than n, retrieve n auctions with nearest expiration time

5.2.5. Display link list to all items in list, sort order should be auction with nearest deadline to most distant

Petitioner Apple Inc. - Exhibit 1026, p. 229

5.2.5.1. Item name
5.2.5.2. Time till end of auction
5.2.5.3. Highest current bid
5.2.6. On user selection of the item, display same information as above plus
5.2.6.1. Description
5.2.6.2. Photo (if any)
5.2.6.3. Attachments (if any)
5.2.7. If count is more than n, display further drill-down options as well as item information above
5.3. Accept new bid through the display screen
5.3.1. Log bids in order, reject if bid is not higher than last high bid by increment.
5.3.2. If bid is rejected, tell bidder that their bid is not sufficient
5.3.3. Update database recording highest bid, bidder, time of bid
5.3.4. Display screen to user to confirm that their bid is the highest
6. When the time limit is reached, determine if a new bid has been received in the last 3 minutes (or other short time period). If so, extent the bidding time by 3 minutes (or other short time period) and execute step 5 with a new closing time.
7. When the time limit is reached, including all extensions under step 6, then
7.1. Email message to highest bidder that they won
7.2. Add transaction to completed deals
7.3. Update splash and add screens
7.4. Settle with winning bidder-- two models:
7.4.1. Connect buyer to seller for direct settlement
7.4.2. Collect money from buyer, deduct fee, convey amount to seller

C. Dutch Auction Transaction Engine

A Dutch auction, like a standard auction, involves the sale of a single item or batch with fixed specifications. There is one seller, and many potential buyers. The seller sets the prices, ideally higher than any buyer's maximum bid price. The offered price is reduced by a fixed increment at fixed intervals until a buyer accepts the price. The purchase goes to the first buyer in to accept the price. In the physical world (as opposed to the online world), Dutch auctions are rarely if ever run concurrently. In a live trading room, it could be difficult to determine which buyers

Petitioner Apple Inc. - Exhibit 1026, p. 230

was first to commit to a price when several are willing to pay the same amount. The Dutch auction is relatively simple to implement in an electronic environment. There are, at present, no online Ducth Auctions of which the inventors are aware.

1. Enter and maintain a framework for catalog
    1.1. Enter / delete / edit categories. Categories are titles for groups of items, such as "furniture" or "solvents"
    1.2. Enter / delete / edit subcategories. Subcategories are categories within categories, effectively establishing a hierarchy of products. Example: furniture/dining room/tables.
    1.3. Create groups of categories and subcategories (e.g. see also....). The grouping allows a person browsing items to be referred to another category that may contains items of interest. For example, someone may reach the furniture/dining room/tables and then be referred to furniture/office/conference room tables where other suitable tables may be listed, or to furniture/dining room/chairs to buy chairs that make the table. This cross referencing makes transforms the hierarchical arrangement of categories into a web.
2. Execute qualification process (optional)
    2.1. Admit bidders who are qualified based on past participation
    2.2. Provide fill-in-the blank qualification form new bidders
    2.3. Collect information
    2.4. Conduct automated review or manual review
    2.5. Inform prospective bidder of qualification or not
3. Collect information on items to be auctioned and owners, including
    3.1. Identity of seller
    3.2. Descriptions, optionally including attachments and photographs, independent certifications or appraisals, or other information necessary to establish the value of the tiem
    3.3. Categorization
    3.4. Starting price
    3.5. Increment, Interval for reduction
    3.6. Minimum price
    3.7. Obtain consent to rules (possibly as part of registration/qualification process)

Petitioner Apple Inc. - Exhibit 1026, p. 231

3.8. Collect to conduct auction if item is

3.9. Calculate time to take item off auction by determining the number of steps (intervals) necessary to reduce price from the starting price to the minimum

3.10. Record all of the above information in the Dutch auction database

4. Cull expired options

4.1. Search database periodically for items where current time is later than time to take item off auction (2.9)

4.2. Inform owner that item was not sold

4.3. Delete entry from database

4.4. Prompt for revised terms start of another auction, create new entry if user takes option

5. When the buyer enters the system display a list of high level categories, a prompt for search criteria, and/or a link to a search page. Allow user to drill down through categories or enter search parameters.

5.1. Retrieve count of items that meet criteria

5.2. If more count is less than 25 (or other small number (n) consistent with the layout of the screen) retrieve all items that meet criterion

5.3. If count is more than n, retrieve n auctions with nearest expiration time

5.4. Display link list to all items in list, sort order should be auction with nearest deadline to most distant

5.4.1. Item name

5.4.2. Time till end of auction

5.4.3. Current price:

5.4.3.1. Retrieve starting price (SP) and increment (I$)

5.4.3.2. Calculate number of intervals since start of auction (INT)

5.4.3.3. Determine price = SP – (INT * $)

5.5. On click, display same information as above plus

5.6. Description

5.7. Photo (if any)

5.8. Attachments (if any)

5.9. The display screen should include a button that allows the buyer to purchase the item at the selected price.

Petitioner Apple Inc. - Exhibit 1026, p. 232

6. When the user clicks the "buy" button
    6.1. Email message to highest bidder that they won
    6.2. Add transaction to completed deals database
    6.3. Settle with winning bidder-- two models:
        6.3.1. Connect buyer to seller for direct settlement
        6.3.2. Collect money from buyer, deduct fee if any for auction and payment services, convey the remainder to seller.

D. Reverse English Auction Transaction Engine

In a reverse auction, there are multiple buyers to one seller. Prices come down rather than up. There are many variants of a reverse auction. The variant discussed here is a reverse English auction. Reverse auctions have been implemented on line in Open Markets.

The process for posting an item for bid and for qualifying bidders is the same as for other auctions. The difference here is that the buyer may optionally set a maximum price.

1. Accessing the list of items sought
    Potential bidders access items sought by working through a hierarchy of categories and subcategories or entering search criteria, as for other auctions. A list of items within the category/subcategory and/or meeting the search criteria is displayed. The user may then
    1.1. Terminate the session on finding no suitable items
    1.2. Revise the search criteria
    1.3. Select an item on which to bid
2. If the user selects an item on which that may wish to bid, detailed information about the items is displayed. This item may include the following information:
    2.1. Name
    2.2. Seller
    2.3. Description
    2.4. Detailed specifications for items
    2.5. Delivery requirements
    2.6. Proposed terms
    2.7. Current low bid
3. If the user determines that they should bid, he accesses the bid entry screen from

Petitioner Apple Inc. - Exhibit 1026, p. 233

the detailed description in Step 2 above. Making a bid consists of entering the following information:

3.1. New, lower bid

3.2. Comments pertaining to any special terms, features, or conditions

3.3. Attachments containing relevant additional information and any certifications required by the buyer

4. On receipt of bid, there are two options – either all bids are accepted, or bids are accepted only after review of information by the buyer.

4.1. Case 1: all bids are accepted

4.1.1. New bid is checked to determine if it is lower than prior bid

4.1.2. If so, then

4.1.2.1. bidder is notified that their bid is currently the lowest

4.1.2.2. seller is notified of new low bid

4.1.2.3. bid database is updated

4.1.3. If not, then

4.1.3.1. Bidder is notified that their bid is not the lowest

4.1.3.2. Bid screen is displayed so that bidder may lower bid

4.2. Case 2: bids are accepted after review by buyer

4.2.1. Buyer is notified of bid via email or online message

4.2.2. Buyer accesses complete information on the proposed bid through the system

4.2.3. Buyer select accept bid or reject bid.

4.2.4. If bid is accepted, then

4.2.4.1. Bidder is notified that their bid is currently the lowest

4.2.4.2. Bid database is updated

4.2.5. If bid is not accepted, then

4.2.5.1. Buyer enters reason for not accepting bid

4.2.5.2. Bidder is informed that bid is rejected with reason stated above

4.2.5.3. Bidder may access the bid screen to revise offer

5. When time period has expired and there have been no bids within a short specified interval, then

5.1. If at least one bid less than the maximum has been received, then:

Petitioner Apple Inc. - Exhibit 1026, p. 234

5.1.1. Notify low bidder that their offer was successful

5.1.2. Add transaction to completed deals database

5.1.3. Settle with winning bidder-- two models:

5.1.3.1. Connect or introduce buyer to seller for direct settlement

5.1.3.2. Collect money from buyer, deduct fee if any for auction and payment services, and convey the remainder to seller.

5.2. If no bid less than the maximum has been received, the

5.2.1. Notify buyer

5.2.2. Allow buyer to revise bid criteria

E. Sealed Bid Transaction Engine

In a sealed bid system, the buyer publishes or distributes detailed, fixed specification to a number of potential bidders (who may or may not be prequalified). Bidders submit binding bids by a specified deadline, in a specific format that allows ready comparison. The competitive bidding process is distinguished from the bid and proposal process by the complexity of the specifications and the bids. In a simple competitive bid, competition among the bidders is along one or two readily quantified dimensions (always including price) and there is little or no room for variation in the form or specifications of the offering. Comparison of the bids is elementary.

The process for posting an item for bid and for qualifying bidders is the same as for other transactions as is the method to identify items on which to bid either using the hierarchy of categories and subcategories or a search engine.

1. If the user selects an item on which he may wish to bid, detailed information about the items is displayed. This item may include the following information:

1.1. Name

1.2. Seller

1.3. Description

1.4. Detailed specifications for items including all information necessary to prepare a bid

1.5. Bid instruction including specification for any documentation the buyer may required with a bid (e.g. proof of bonding or license)

1.6. Notice of any fees for bid registration

1.7. Delivery requirements

Petitioner Apple Inc. - Exhibit 1026, p. 235

1.8. Proposed terms

2. After review of the bid requirements, the user may choose not to bid or may enter a bid. The process for entering a bid consists of preparing a bid package, including the price offered and any necessary supporting documentation. This is done by completing an online form, with provision for attachments. The bid is submitted through the system where it goes into a database of bids that are not opened to the closing time for the bidding process.

3. At the closing time, all bid packages are conveyed to the buyer.

3.1. If there are no bids, the buyer is offered the opportunity to revise the request for bids.

3.2. If there are multiple bids, the buyer reviews the bids and selects the lowest priced qualifying bid. They buyer informs the seller and arranges payment and delivery in accord with the terms stated in the bid package.

F. Order Matching Transaction Engine

In an order-matching system there are many potential buyers. Each posts binding offer to buy (bid amount) or sell (asked amount). The process proceeds in real time. The order matching system constantly compares bid and asked and, when a match is found within a specified spread, the deal is concluded. No accepted offer can be repudiated, but offers may be withdrawn before a deal is consummated. The strike price is posted so that buyers and sellers can modify their offerings in real time. The items traded are fungible so that price is the only decision. For the market to operate efficiently the items traded must be tightly defined and the terms of sale must be fixed and determined in advance. This is typically done by the operation or an exchange, with the order-matching engine operating in the background. To insure that the items traded are well defined, and the terms of sale are rigid example of an order matching process in stock trading on an exchange.

Users of an order-matching engine are all potential buyers and seller. They are qualified in advance using a process like that outlined by for auction with the extension that deposit accounts are frequently required given the speed of transactions in exchange environments.

1. Establish and maintain items to be traded. All functions in this category are reserved to the manager of the exchange or a designee.

To add (i.e. "list" and idem), enter

Petitioner Apple Inc. - Exhibit 1026, p. 236

1.1. Unique item number or symbol

1.2. Description of item (e.g. Sears Class A Common Stock)

1.3. Terms and conditions ownership (e.g. who can own) if any

1.4. Trading units (e.g. shares, blocks, etc.)

1.5. Additional information as required by the rules of the exchange

To delete (i.e. "delist" and item)

1.6. Select the item to be deleted

1.7. Confirm deletion

2. On entry to the system, potential buyers and sellers can review the price of the last transaction of any item, either through a list or a search by item name or symbol. The current highest asked and lowest bid price are also shown.

3. An offer to sell is posted by entering the following information:

3.1. Item number or symbol

3.2. Quantity offered

3.3. Proposed price ("asked")

3.4. Seller

3.5. Offers may be revise at any time prior to consummation of a deal

4. An offer to buy is posted by entering the following information

4.1. Item number or symbol

4.2. Quantity offered

4.3. Proposed price ("asked")

4.4. Buyer

4.5. Offers may be revised at any time prior to consummation of a deal

5. Offers to buy and sell are constantly reviewed by the software. When there is an offer to buy and sell at a price within a preset difference. When prices match, buyers and sellers are notified of the transaction, and the transaction is recorded. The display of the last transaction price, the highest bid and the lowest asked price is updated.

6. The transaction is conveyed to the backend accounting system of the exchange.

G. Bid and Proposal

The bid and proposal process is typically used for procurement of large or complex products or services, in which cost is not the only factor. Cost must be weighed against the buyer's assessment of the quality and suitability of an offering

Petitioner Apple Inc. - Exhibit 1026, p. 237

and the ability of the bidder to deliver the product or perform the specified services.

The bid and proposal process is conducted between one buyer (possibly representing a consortium) and many potential sellers, sometimes organized into teams. The buyer issues specifications that may be general or highly specific, brief or very lengthy. The specifications may be distributed freely or to a list of qualified buyers.

With physical RFPs, the size and the associated cost of distribution make it common practice to advertise the availability of the RFP first, sending copies only to those that request it. Frequently, the requestors are required to supply information to establish their qualifications to bid. While cost is not an issue in electronic dissemination of RFPs, the model of advertising prior to distribution is still useful in managing the qualification process. This is addressed as variant (a) is this description. Variant (b) requires no prequalification.

In a competitive bid on fixed requirements (sealed bid or auction), there is typically very little communication between buyer and seller between publication of the request and submission of the bids. The requirements are comparatively simple, clear, and unambiguous. In contrast, the bid and proposal process may involve considerable communication between buyer and seller. The process may begin with a bidders' conference to answer questions about the requirements. Additional questions from bidders may be accepted, though not all need be answered. Questions and answers may be made available to all bidders or the response may be in private. This dialog is crucial for two reasons. First, it helps the bidders understand the requirements and to be responsive in their bids. Second, it is not unusual for the bidders' questions to identify some point of ambiguity, error, or contradiction in the specifications, leading to a modification of the RFP. The diverse perspectives of the bidders, and the close attention required on their part to prepare a bid inherently provides an excellent review of the RFP.

The initial phase of the RFP process concludes with submission of the bids, but this is far from the conclusion of the process. Commonly, questions arise from the review of the proposals. These may relate to a specific submission or have broader implications, leading to modification of the requirements. The list of bidders can be culled to the best candidates. These are asked to answer questions about their proposals and to provide additional and clarifying information.

Petitioner Apple Inc. - Exhibit 1026, p. 238

The process described here is built around the document repository described elsewhere in this application. Through this process of refinement, the list of bidders is narrowed to one or two with whom a contract is negotiated. The process of negotiation is addressed as a separate transaction type (Negotiation Engine) as it may be conducted without the bid and proposal process.

Variant (A): with pre-qualification

1. Software supports the user in creating a web site for the proposal process. Initially this site manages the process for requesting the request for proposal (RFP), qualifying bidders, and disseminating the RFP.
2. Supported by the system software, the bidder creates and RFP advertisement by
   2.1. entering a summary of the RFP.
   2.2. entering a summary of the information needed to qualify as a bidder or
   2.3. attaching a form (HTML web page or template for paper form) for entering qualifying information
3. The RFP advertisement includes file transfer software for uploading qualifying information to the repository.
4. Disseminate RFP advertising
   4.1. Post on public bulletin board or
   4.2. Disseminate via mail to selected users
5. When users access the system, issue them an encryption key and PIN to be used for subsequent uploads and communications to verify their identity.
6. Receive requests for RFP in repository
   6.1. Prompt for key
   6.2. Encrypt submission
   6.3. Upload
   6.4. Generate receipt – should include an authentication number
7. Disseminate RFP to selected user, either:
   7.1. Attach to return Email or
   7.2. Post the RFP in a repository from which qualified prospective bidders may download the file. If the repository model is used, provide notice of the posting via email including any necessary PINs and codes to access the repository
   7.3. When a prospective bidder downloads an RFP, issue an encryption key to be

Petitioner Apple Inc. - Exhibit 1026, p. 239

used in submitting proposal

8. The RFP site also includes a page through which prospective bidders can submit questions. Questions and answers are posted to the site.
9. Updates to the schedule and amendments to the RFP are posted to the site
10. All access to the site is recorded to verify that prospective bidders have received critical information. Direct contact may be used when it is determined that a bidder had not accesses the site since critical new information was posted.
11. Bidders prepare their proposal and then upload them to a repository for proposals using software built into the proposal site.
    - 11.1. Prompt for key
    - 11.2. Encrypt submission
    - 11.3. Upload
    - 11.4. Generate secure hash number to prevent tampering with the submission
    - 11.5. Generate receipt including secure hash number and authentication code
12. After initial proposals are received, the process moves into a phase commonly termed the "best and final process" in which the proposals are reviewed, the list narrowed, and the proposals refined.
    - 12.1. Create separate secure environment (i.e. web site with repository) for each respondent
    - 12.2. Exchange materials through repository (described elsewhere in this filing)
    - 12.3. Records and receipt each access
    - 12.4. Generate key for revised proposal
    - 12.5. Receive proposal using process in 11
    - 12.6. Repeat from step 11 as many times as necessary

The remainder of the process is completed as a negotiated deal, described below.

Variant B: no pre-qualification:

Proceed as above, beginning with Step 6 and not requiring a key for download of the RFP.

Petitioner Apple Inc. - Exhibit 1026, p. 240

H. Negotiation Deal Engine

An engine for negotiating a deal can be built around the capability of the system to create a temporary virtual private network through the web. A temporary network is created for the negotiation. Access to the network is limited to the parties of the negotiation, their advisors and counsel, and, potentially, arbitrators and regulators. The members of the negotiating environment have access to the complete set of tools described in this filing including those for communications (email, anonymous mail, online chat, threaded dialogs, and audio and video collaboration), the library of standard contract instruments, the tools for document signature and authentication, and the document repository. Using these tools in a secure environment they can negotiate, close, and register a deal.

FIG. 19 shows one possible user interface for selecting participation engines to be made available to group members. The term "participation engine" refers generally to collaboration tools that provide features beyond merely communicating among group members. Various services such as an on-line survey tool, a DELPHI model tool; brain writing tool; and real-time polling can be provided.

A. Online Survey

In online polling or surveying, the person creating the poll uses and automated tool (new to this application) to build simultaneously an online questionnaire and a database to collect the results. The user builds the questionnaire by entering a series of questions and an associated data collection widget for each. The polling tool builds the database and the data entry screen. The data entry screen consists of two columns. The left column is a series of questions. The right column is the data entry tool appropriate to the question. Various data entry tools can be provided to respond to the query, including such things as:

1. yes / no radio buttons
2. true / false radio buttons
3. slider with scale from 1-5, 1-10, etc.
4. fill-in-the-blank text box
5. numeric field
6. multiple check boxes (e.g. strongly disagree, disagree, agree, strongly agree)

Other data entry types may be added.

Petitioner Apple Inc. - Exhibit 1026, p. 241

As each question / data collection widget is added, the polling tool creates the database. The database includes one record per data collection form. Creating the database structure simply means adding one new field to each record definition for each question. The type of data collection widget defines the format of the field, as follows:

1. yes / no radio buttons: one character field, limited to "y" or "n"
2. true / false radio buttons: one character field, limited to "y" or "n"
3. slider: real number field, with appropriate range check
4. fill-in-the-blank text box: text box
5. numeric field: real number or integer
6. multiple check boxes: integer field with range check from 1 to number of boxes

Every data entry screen provides a "save" and "cancel" button. Save writes to the database. Cancel exits the entry screen without saving.

The survey, once composed as described above exists as a web page. This page can be embedded in web applications. It can be made available on a site available to the entire Internet, on an Intranet, or in a dynamically created environment. Alternatively, it can be distributed via e-mail. When the form is completed, the submit button transmits the value entered to the database that is created at the time the form is generated. Access to the database is controlled by the rules of the database system. It may be limited to the individual who creates the survey form and database, but it may be accessible other users in the survey developers organization, as determined by the database administrator. Distribution of the result of the analysis is at the discretion and control of the individual managing the survey. This manager may be the individual who creates the survey, but the actual creator may be acting on behalf of the survey manager. Results may be kept private, posted to the Internet, and intranet, or a collaborative environment, distributed via e-mail within an organization, or, if the information is available, sent via e-mail to the participants in the survey.

B. Online Delphi Engine

The online Delphi engine allows real-time collaboration in estimating or predicting an outcome that can be expressed numerically. For example, the method can be used to develop a consensus forecast of grain prices. The method has been

Petitioner Apple Inc. - Exhibit 1026, p. 242

in used since the 1970s, but has not previously been adapted to online processes. One possible method is as follows:

1. Establish the session
    1.1. Within an online community, the moderator of the session creates the brain writing session by entering the following information:
        1.1.1. Name of moderator
        1.1.2. Title of the session
        1.1.3. Description of the session
        1.1.4. Background reading as references or attachments
        1.1.5. Start date for the session
        1.1.6. Scheduled end for the session
        1.1.7. Access to the session:
            1.1.7.1. URL for access
            1.1.7.2. Open to all or invitees only for observation
            1.1.7.3. Open to all or invitees only for participation
        1.1.8. Payment information if required
2. Optionally, the session may be advertised on line
3. If the session is private, invitations with logon keys must be distributed via email, actual mail, or download.
4. Optionally, the moderator may run on online applications and qualification process
5. Prior to the start of the session, the moderator must describe precisely the value to be estimated. The definition must be completely unambiguous.
6. Each participant connects at the start of the session. On connecting, they question is posed (e.g. "What will be the price of West Texas intermediate oil in December?")
7. Each participant enters a number a brief (1 paragraph maximum) explanation of their reasoning.
8. When the participant is done entering their estimate, they click "Done".
9. Each participant's estimate and explanation is recorded.
10. Each participant then sees the summary screen.

Petitioner Apple Inc. - Exhibit 1026, p. 243

11. Estimates are arrayed graphically from top to bottom of the screen, from lowest to highest. The value is stated as is the associated comment, but the source of the comment is not revealed.
12. Participants can review the estimates and comments, send an anonymous message to the author or any comment, or amend their answers.
13. The session terminates when the time expires, or when the moderator determines that there it is no longer appropriate to continue. The operator may determine this is based on declining participation or, if participation is high, the moderator may extend the deadline.
14. Participants and observers may access the final display of estimates, again arrayed from top to bottom, lowest to highest.

C. Brain Writing

Brain writing is a variant of a method for facilitated group discussion termed brainstorming. The objective of brainstorming is to maintain the focus of the discussion while encouraging creative input and recognizing the contributions of all members of the group. It seeks to avoid problems with a few individuals dominating the discussion, with junior staff deferring to senior staff, and with new ideas being abandoned before than can be developed fully. Brain storming has been commonly used since the late 1960s. Brain writing is a more intense method that relies on joint writing rather than discussion. What is presented here is adaptation of that method to an online environment. It is believed to be the first such adaptation.

1. Establish the session
    1.1. Within an online community, the moderator of the session creates the brain writing session by entering the following information:
        1.1.1. Name of moderator
        1.1.2. Title of the session
        1.1.3. Description of the session
        1.1.4. Background reading as references or attachments
        1.1.5. Start date for the session
        1.1.6. Scheduled end for the session
        1.1.7. Access to the session:
            1.1.7.1. URL for access
            1.1.7.2. Open to all or invitees only for observation

Petitioner Apple Inc. - Exhibit 1026, p. 244

1.1.7.3. Open to all or invitees only for participation

1.1.8. Payment information if required

2. Optionally, the session may be advertised on line
3. If the session is private, invitations with logon keys must be distributed via email, actual mail, or download.
4. Optionally, the moderator may run on online applications and qualification process
5. Prior to the start of the session, the moderator must list some number (typically 5-10) of questions or hypotheses to be explored. (e.g. " Our company should create a spinoff to develop and commercialize the new breast cancer vaccine") This may be done by the moderator alone, in consultation with the participants, or with other outside the session.
6. Each question or hypothesis becomes a "Card".
7. Participants may enter the session any time after the start. A password may be required if the session is not open.
8. On entry into the system, a user if given a card at random. The card consists of the initial question or hypothesis plus all comments entered on the card by other participants.
9. After reviewing the card, the participant may add his or her own comments to the bottom. After entering comments, the participant clicks "Done" to return the card to the pile.
10. When a participant returns a card to the pile, they received another card, chosen at random (preferably) or selected by the user. This process continues until the opt to exit. They may reenter at any time up to the conclusion of the session.
11. When a card is returned to the pile, it is become available for assignment to the next participant. The card includes the additions of the most recent participant.
12. A participant may opt to return the card without addition if he or she has nothing to add.
13. Participants may create new cards when new ideas come to mind. These are treated in exactly the same way as original cards.
14. Observers may view any card but may not add to them.
15. The moderator may limit participation to a set number at any time so that there is a sufficient number of cards to keep the participants fully occupied.

Petitioner Apple Inc. - Exhibit 1026, p. 245

16. The session terminates when the time expires, or when the moderator determines that there it is no longer appropriate to continue. The operator can determine this based on declining participation or, if participation is high, the moderator may extend the deadline.

17. The raw cards are distributed at the conclusion to all participants. The moderator or another individual is charged preparing a summary and arranging follow-up.

FIG. 22 shows one possible scheme for storing brain card writing data elements. In accordance with one embodiment, each brain writing card comprises a data structure including the following elements:

1. Brain writing session number: Serially assigned number to differentiate brainwriting sessions. A session is the set of all cards pertaining to a particular topic.
2. Card number: A Serially assigned sequence number
3. Initial Comment : The question or comment used to initiate the discussion (e.g. "SAIC should purchase a company that produces Internet server software"
4. Date and time card started
5. Date and time card closed
6. Comments: A collection (i.e. a set of unlimited length) containing the comments added by participants in the brainwriting session.
7. Date of additional comment: Date and time that each additional comment was added.
8. Commenter: Name or user ID of the person adding each additional comment. Ideally, brainwriting should be anonymous to encourage open dialog. Accordingly, this field may be omitted from an implementation. Some organizations, however, may wish to track this information without making it visible to users, or in some cases to attribute comments.

When the user has finished defining the group and specifying its functions, environment generator 1201a (FIG. 12) creates an environment accessible to the group members and including the functions specified during the environment definition process. As shown in FIG. 20A, for example, a web page can be created for the newly created environment, including those functions that were selected by the user that created the group. All group members are notified of the existence and

Petitioner Apple Inc. - Exhibit 1026, p. 246

location of the environment, and each group member can use the functions provided in the environment to collaborate on a project or conduct business.

FIG. 20B shows what an environment might look like to a group member after entering the environment. As shown in FIG. 20B, for example, a news banner announces the latest news for the group. Additionally, specific communication tools, research tools, transaction engines, and participation engines are made available to group members, which can be executed by appropriate mouse clicks in accordance with the inventive principles. According to various inventive principles, each tool shown on the web page is accessible through a hyperlink to a web-based program that performs predefined functions as set forth above. For example, clicking on "online catalog" would link the group member to a web page that implements an online ordering engine as described previously. Users can navigate through the various tools using conventional web browser features (i.e., forward, backward, etc.). It may be desirable to implement some or all of such software using server-side scripting or other similar means consistent with the system configuration of FIG. 12.

FIG. 21 shows how environment generator 1201a can create multiple environments including virtual private facilities, which can be implemented through web pages that contain hyperlinks to functions available to members of each group or environment. An environment definition software component 2106 implements steps 1101 through 1103 of FIG. 11 in order to create one or more environments 2107. (In one embodiment, each group can also be provided with a copy of an environment generator 2106 in order to create sub-groups that draw on the applications and directory structure created for the group). As a user identifies group members and selects functions to be provided for the environment in which the group will collaborate, environment definition component 2106 stores information relating to the selected members and functions in databases. Each environment can include a web page (not shown in FIG. 21) and directories, tools and other applications specific for each created group.

Based on user selections of the type illustrated in FIGS. 13 through 19, environment generator 2106 creates an environment 2107 containing one or more web pages with links to the selected tools. Environment generator 2106 retrieves information from various information sources including a directory of communication tools 2101 (e.g., including descriptions of tools and URL/IP

Petitioner Apple Inc. - Exhibit 1026, p. 247

addresses of web applications to set up each communication tool); directory of transaction engines 2102 (e.g., including descriptions of transaction engines and the URL/IP addresses of web-based applications to set up each transaction engine); directory of research tools 2103 (similar to above); list of global data objects 2104 (e.g., a dictionary of data elements from which the directory of each group can be composed); and a directory of applications 2105 (e.g., a description of available applications and URL/IP addresses of pages to set up access to applications).

Petitioner Apple Inc. - Exhibit 1026, p. 248

WE CLAIM:

1. A method of negotiating a deal over a network of computers, the network including at least one or more computers connected to the Internet, the method comprising the steps of:

(1) posting, on an electronic list that can be viewed over the Internet, information regarding one or more offers to form a contract;

(2) posting on the electronic list one or more responses to the one or more offers;

(3) researching the one or more responses to determine whether they satisfy one or more contract criteria;

(4) negotiating over the network between at least two parties to accept or modify one or more of the responses; and

(5) electronically signing a document to consummate the contract.

2. The method of claim 1, wherein step (1) comprises the step of displaying offers and responses in a parent-daughter spatial relationship on a computer display.

3. The method of claim 1, further comprising the step of sorting the one or more offers and one or more responses according to a user-selected sort order.

4. The method of claim 1, wherein steps (1) and (2) are done anonymously, such that each party to the contract cannot determine the identity of the other party to the contract.

5. The method of claim 4, further comprising the step of simultaneous revealing the identity of each party prior to step (5).

6. The method of claim 4, wherein steps (1) and (4) comprise the step of sharing a single anonymous e-mail alias among a plurality of users.

7. The method of claim 1, further comprising the steps of:

(6) registering keywords with an electronic agent that monitors the one or more offers and providing an e-mail address to be notified upon a keyword match; and

(7) in response to the electronic agent detecting the keyword match, transmitting a message to the e-mail address provided in step (6).

8. The method of claim 1, wherein step (2) comprises the step of clicking on a hyperlink linking the information posted in step (1) to a reply card.

9. The method of claim 7, wherein step (2) comprises the step of requiring

Petitioner Apple Inc. - Exhibit 1026, p. 249

the submission of certain information before the reply card will be accepted.

10. The method of claim 1, wherein steps (3) and (4) are performed a plurality of times for a single contract, such that modifications are made to the one or more responses.

11. The method of claim 1, further comprising the step of electronically registering a plurality of entities that have signatory authority and correlating the registered entities with one or more documents to which signatures can be affixed.

12. A method of displaying information on a computer display, comprising the steps of:

(1) displaying a first plurality of graphical objects each having a shape of a file folder comprising a folder face and a labeled tab, wherein the first plurality of graphical objects are stacked in a cascading arrangement; and

(2) in response to user activation of a "flip" tab, changing the graphical objects displayed in step (1) to show a second plurality of graphical objects each having a shape of a file folder comprising a folder face and a labeled tab,

wherein each of the first and second plurality of graphical objects can be brought to a foreground position in front of other graphical objects by clicking on a corresponding labeled tab.

13. The method of claim 12, wherein each of the first and second plurality of graphical objects has associated therewith one or more functions displayed on the folder face thereof, wherein user can activate the one or more functions by clicking thereon.

14. A method of creating a user-defined networked environment across a plurality of computers without requiring system administrator-level privileges, comprising the steps of:

(1) creating a group by providing a group identifier, a group description, and by specifying a plurality of group members entitled to use the user-defined networked environment;

(2) selecting a plurality of web-based communication, collaboration, and transaction tools from a list of available tools, wherein the selected tools are to be made available to the plurality of group members specified in claim 1; and

(3) through the use of computer software, automatically creating the user-defined networked environment by creating a web page accessible to the plurality

Petitioner Apple Inc. - Exhibit 1026, p. 250

of group members selected in step (1), wherein the web page provides access to the plurality of tools selected in step (2).

15. The method of claim 14, wherein step (1) comprises the step of inviting a plurality of individuals to join the group by transmitting an invitation to prospective group members.

16. The method of claim 14, wherein step (1) comprises the step of advertising an invitation to join the group by posting an advertisement for prospective group members, wherein at least some of the prospective group members are unknown to the user creating the networked environment.

17. The method of claim 14, further comprising the step of screening prospective members that respond to the advertisement in order to determine whether they should be added to the group.

18. The method of claim 14, further comprising the steps of electronically collaborating among group members using the user-defined networked environment.

19. The method of claim 14, further comprising the step of destroying the user-defined networked environment when it is no longer needed.

20. The method of claim 14, wherein step (2) comprises the step of selecting a transaction engine that implements an auction to members of the group.

21. The method of claim 14, wherein step (2) comprises the step of selecting a transaction engine that implements an on-line electronic survey comprising survey questions that are to be answered electronically by survey participants.

22. The method of claim 14, wherein step (2) comprises the step of selecting a transaction engine that implements a bid-and-proposal tool that permits group members to electronically submit bids on one or more proposals.

23. The method of claim 14, wherein step (2) comprises the step of selecting an online ordering engine that permits group members to electronically order goods or services in the user-defined networked environment.

24. The method of claim 14, wherein step (2) comprises the step of selecting an Electronic Data Interchange (EDI) compatible interface that executes electronic commercial transactions between two or more group members.

Petitioner Apple Inc. - Exhibit 1026, p. 251

25. The method of claim 14, wherein step (2) comprises the step of a selecting an electronic brain-writing tool that permits participants to brainstorm using electronic idea cards.

26. A system for implementing a user-defined networked environment that can be created without the need for system administrator-level privileges, comprising:

a plurality of networked computers that communicate using Internet Protocol;

a plurality of web browsers executing on the plurality of networked computers;

a database that stores information concerning the user-defined networked environment; and

a computer program executing on one or more of the plurality of networked computers, wherein the computer program performs the steps of:

(1) permitting a user to create a group comprising a plurality of group members;

(2) permitting the user to select a plurality of web-based communication, collaboration, and transaction tools from a list of available tools, wherein the selected tools are to be made available to the plurality of group members; and

(3) automatically generating a web page accessible to the plurality of group members, wherein the web page provides access to the plurality of tools selected in step (2) to the plurality of group members.

Petitioner Apple Inc. - Exhibit 1026, p. 252

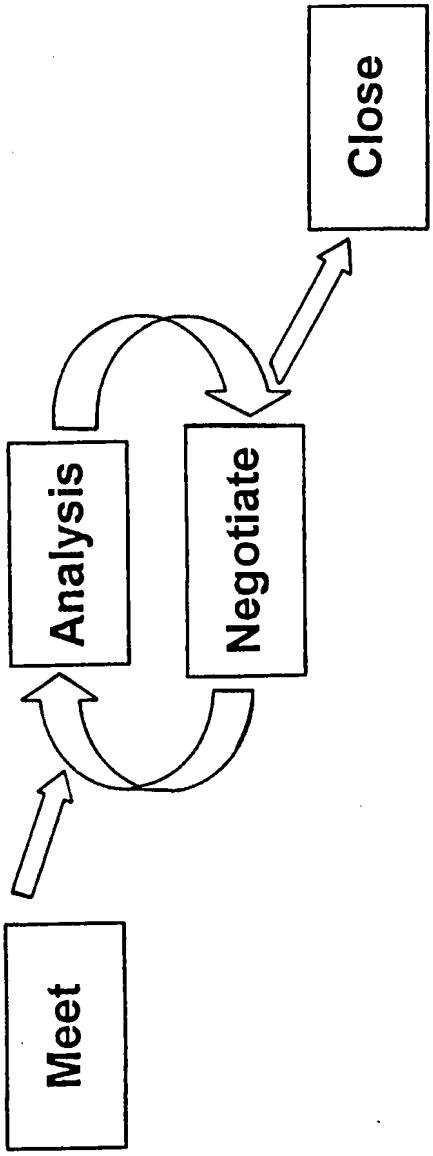


FIG. 1A

Petitioner Apple Inc. - Exhibit 1026, p. 253

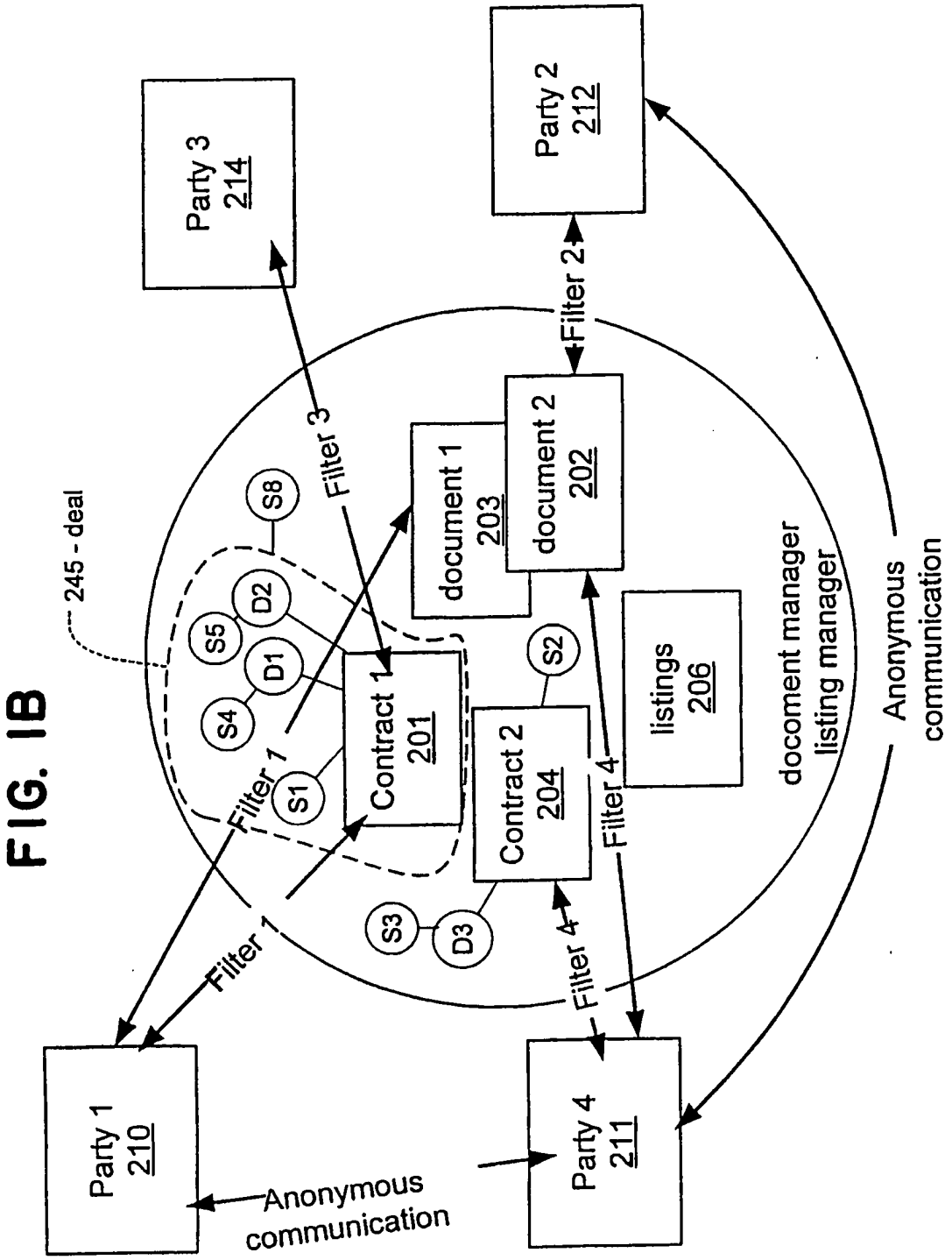
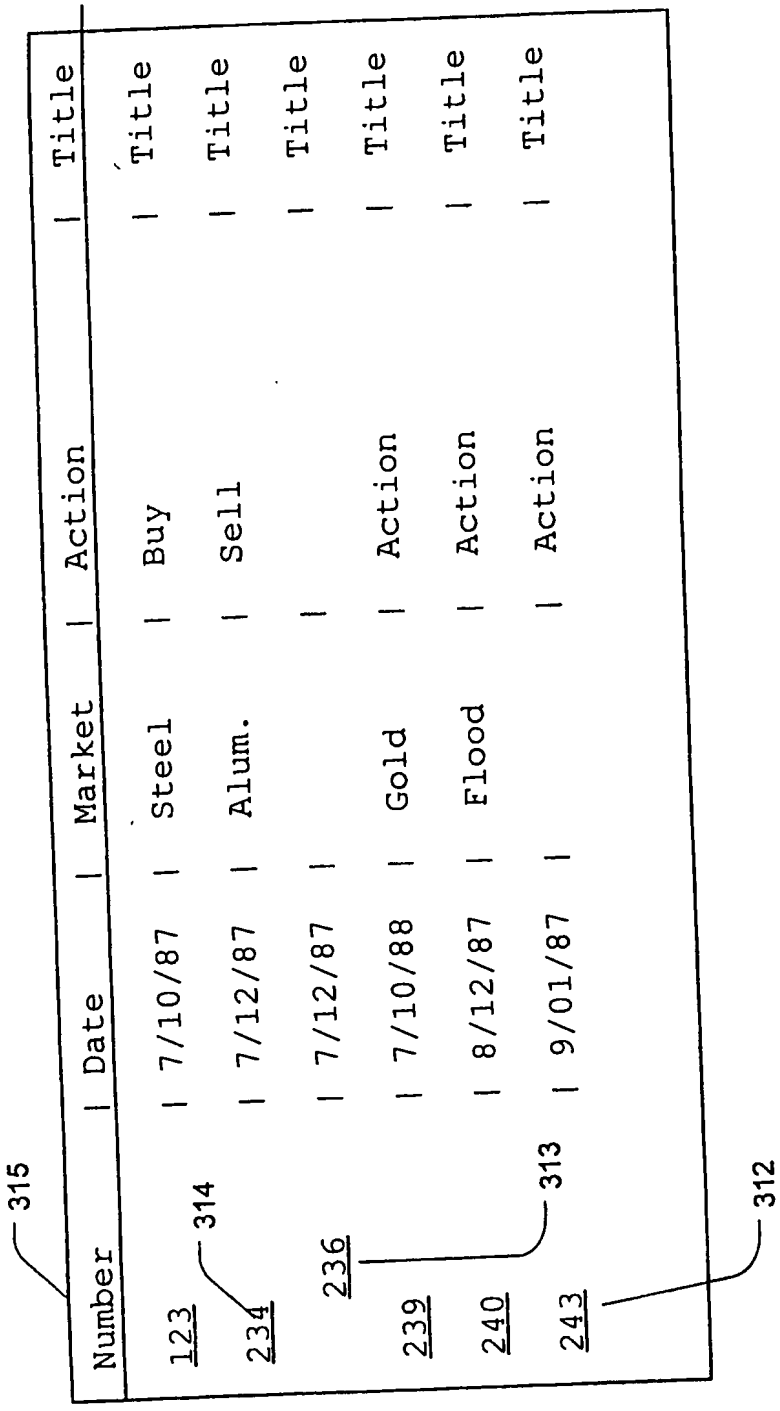


FIG. 1B

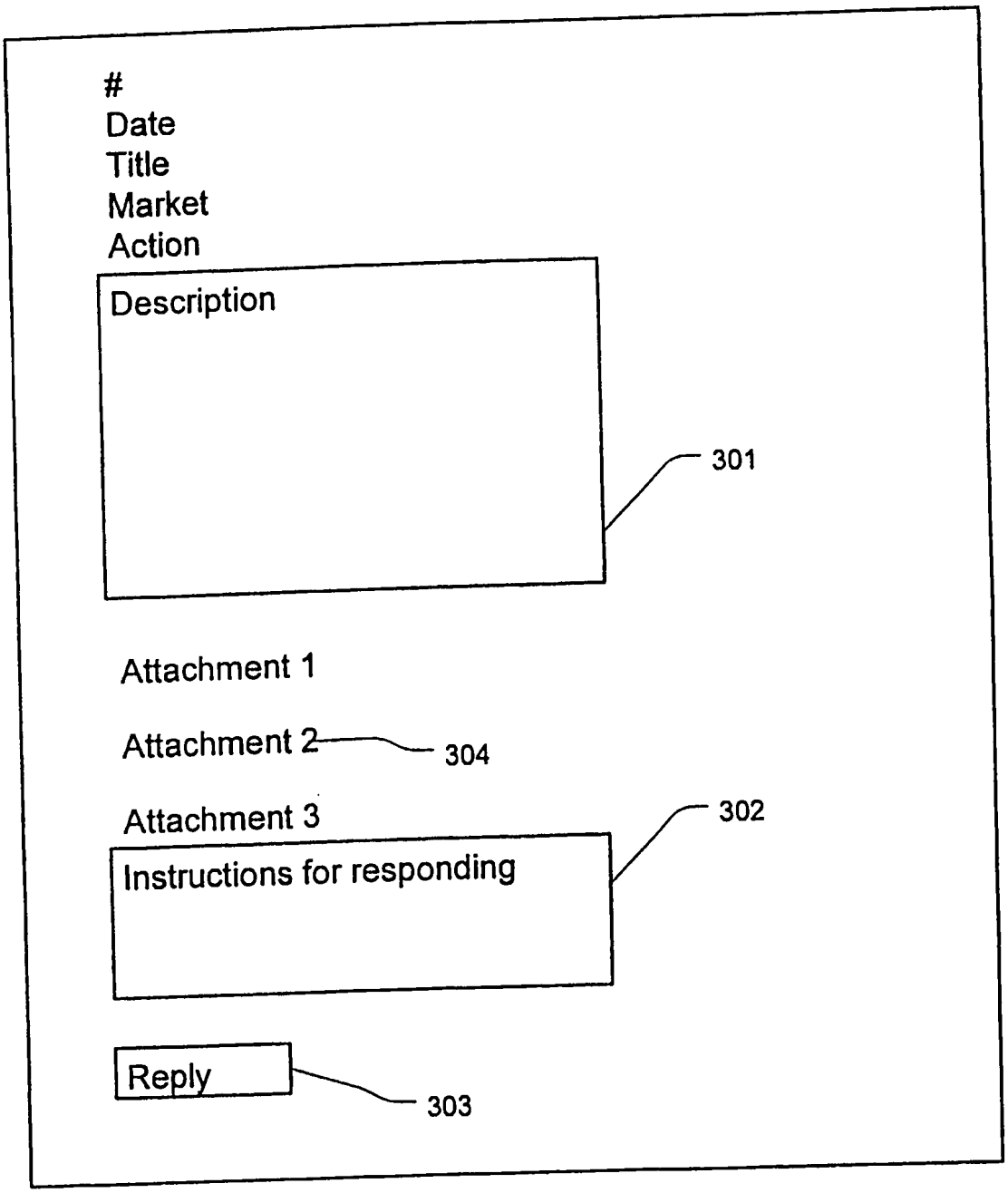
Petitioner Apple Inc. - Exhibit 1026, p. 254

FIG. 2



Petitioner Apple Inc. - Exhibit 1026, p. 255

FIG. 3



Petitioner Apple Inc. - Exhibit 1026, p. 256

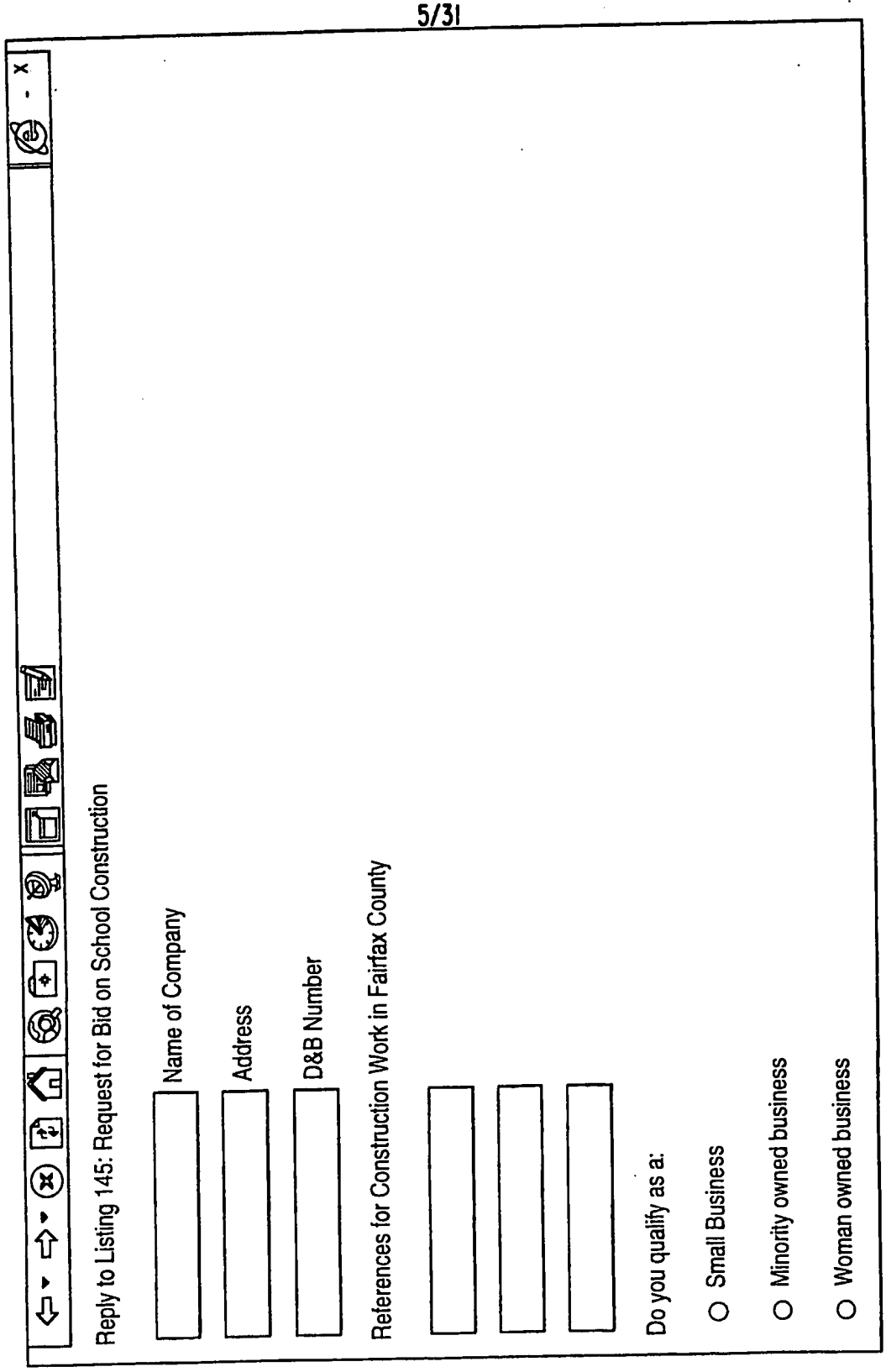


FIG. 4

Petitioner Apple Inc. - Exhibit 1026, p. 257

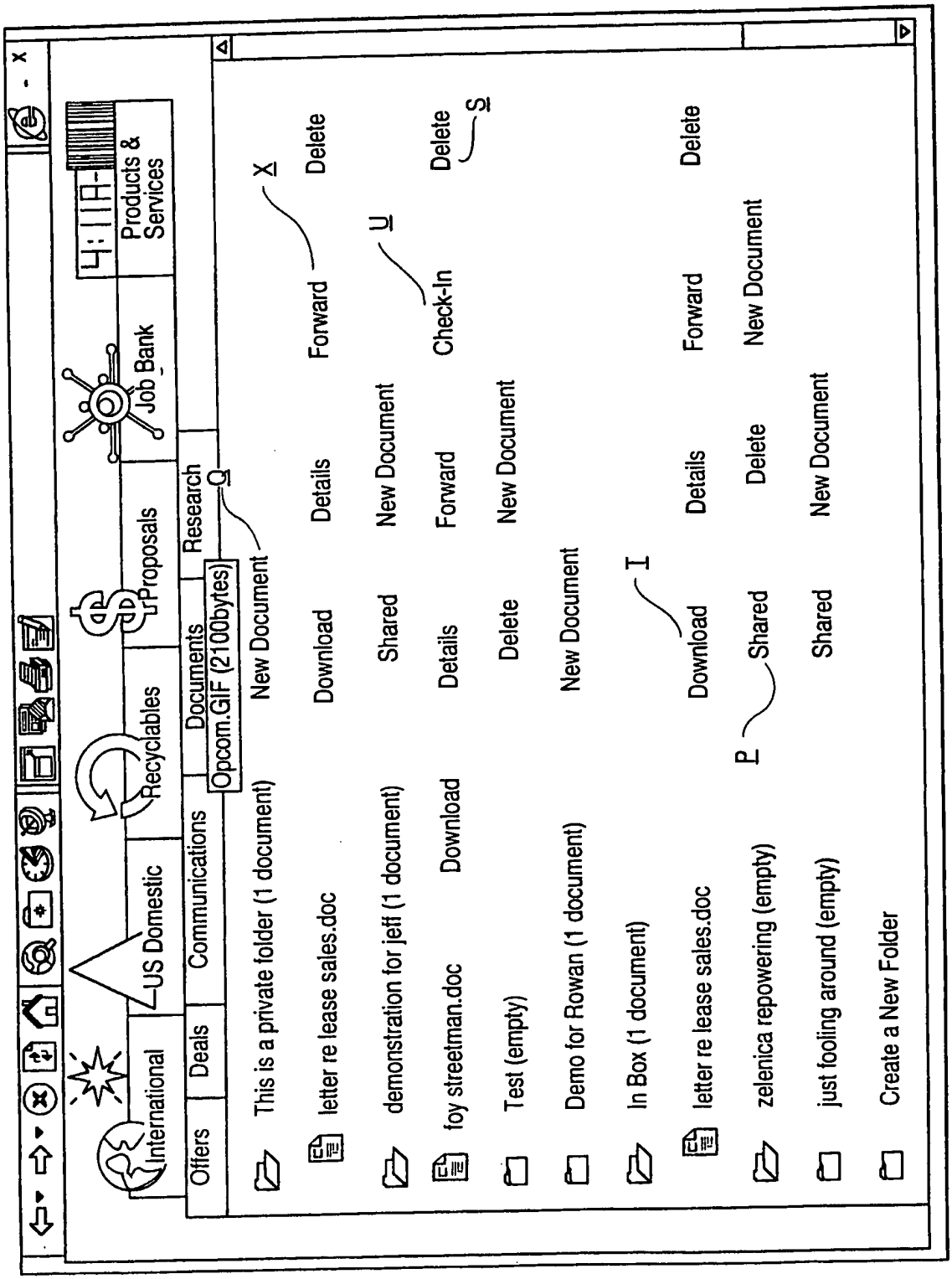


FIG. 5

Petitioner Apple Inc. - Exhibit 1026, p. 258

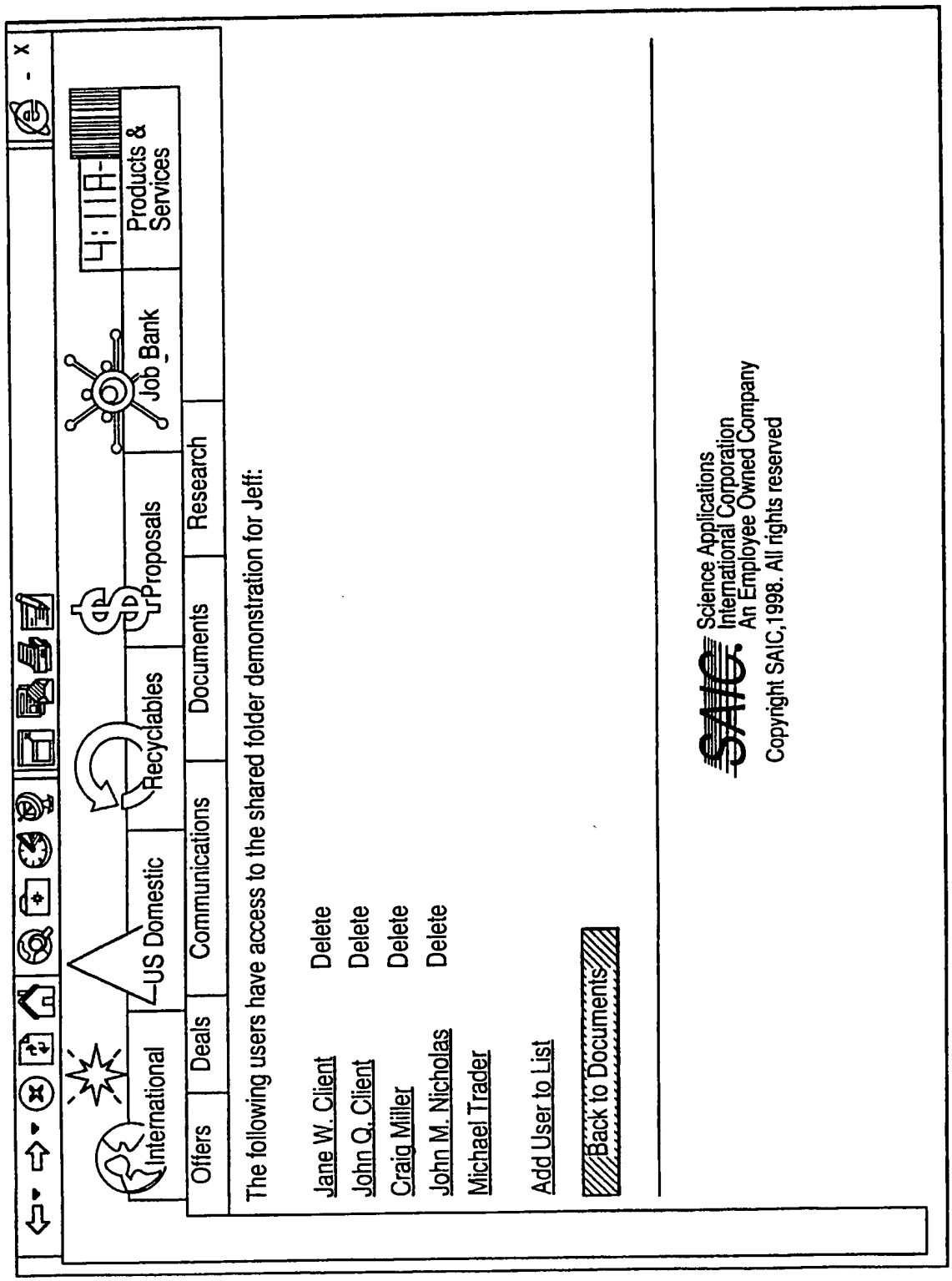
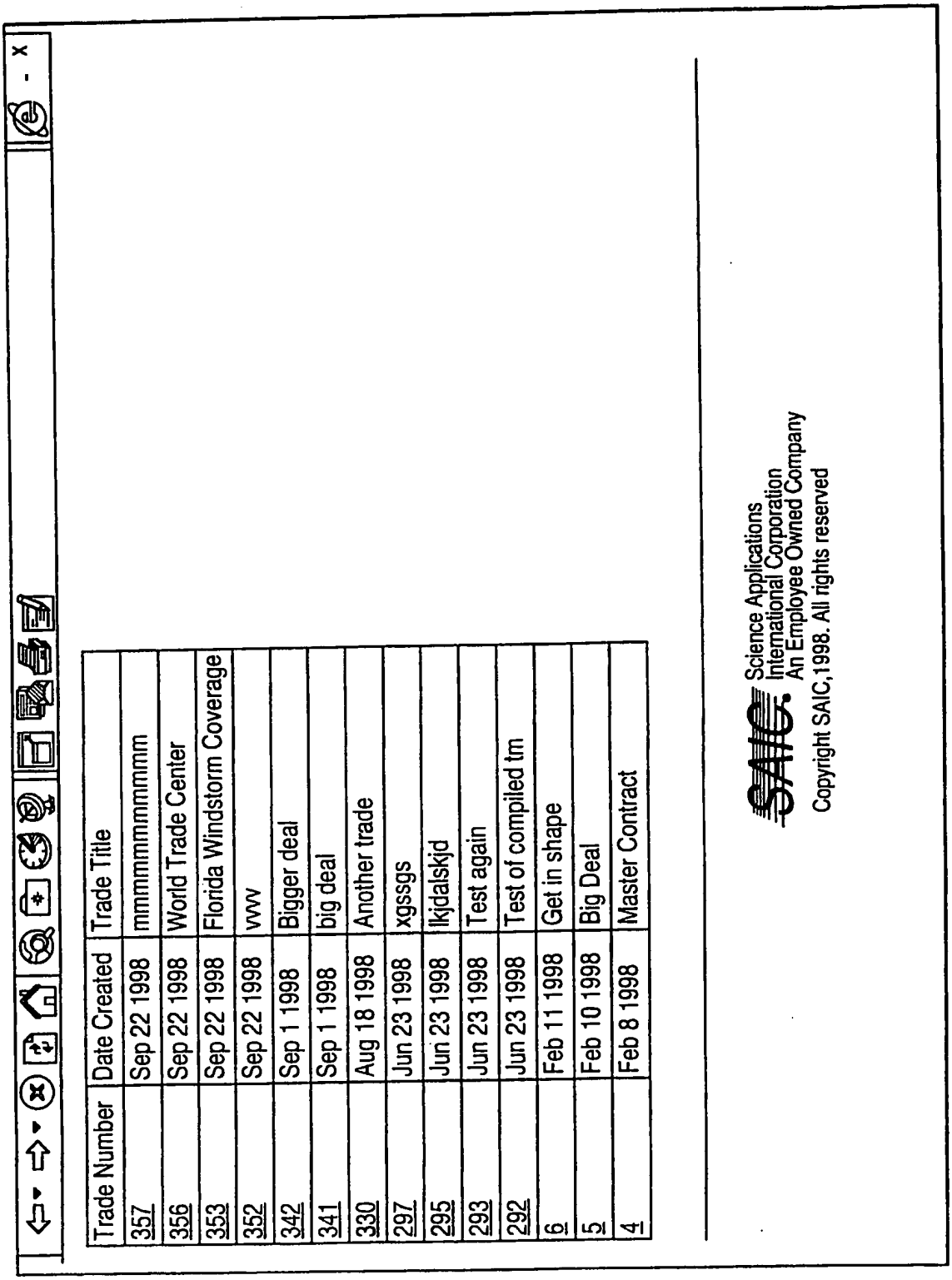


FIG. 6

Petitioner Apple Inc. - Exhibit 1026, p. 259

FIG. 7



Trade Number	Date Created	Trade Title
357	Sep 22 1998	mmmmmmmmmm
356	Sep 22 1998	World Trade Center
353	Sep 22 1998	Florida Windstorm Coverage
352	Sep 22 1998	vvv
342	Sep 1 1998	Bigger deal
341	Sep 1 1998	big deal
330	Aug 18 1998	Another trade
297	Jun 23 1998	xgssgs
295	Jun 23 1998	Ikjdalskjd
293	Jun 23 1998	Test again
292	Jun 23 1998	Test of compiled tm
6	Feb 11 1998	Get in shape
5	Feb 10 1998	Big Deal
4	Feb 8 1998	Master Contract

Petitioner Apple Inc. - Exhibit 1026, p. 260

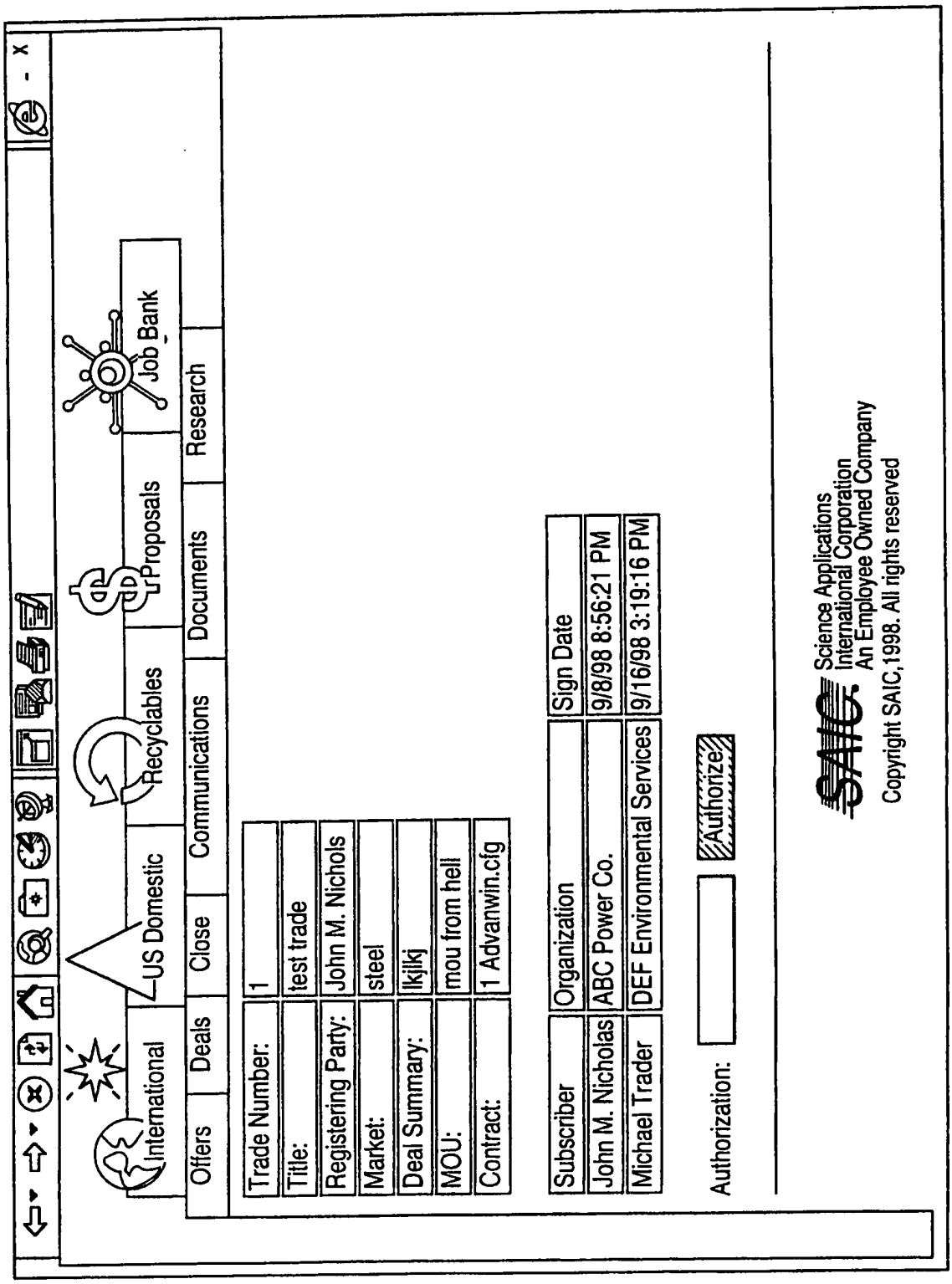


FIG. 8A

Petitioner Apple Inc. - Exhibit 1026, p. 261

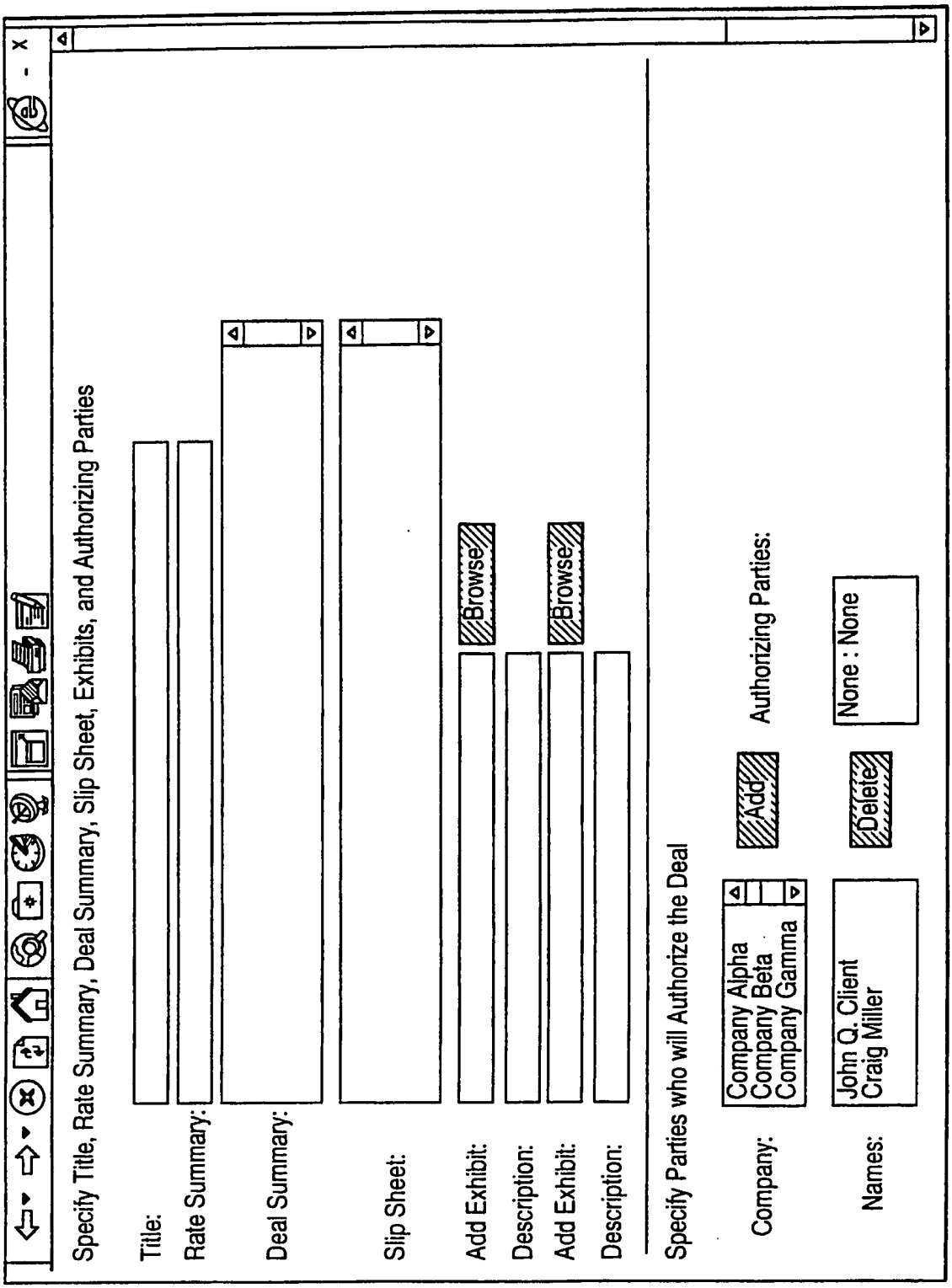


FIG. 8B

Petitioner Apple Inc. - Exhibit 1026, p. 262

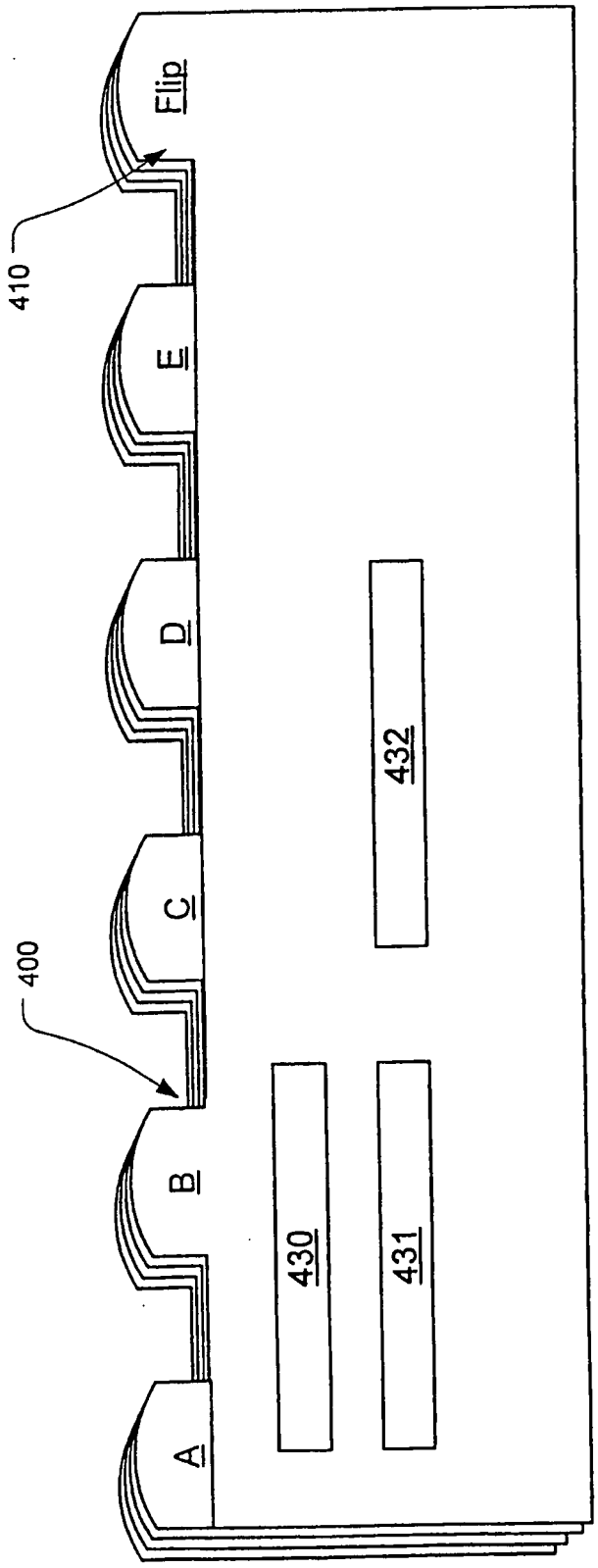


FIG. 9

Petitioner Apple Inc. - Exhibit 1026, p. 263

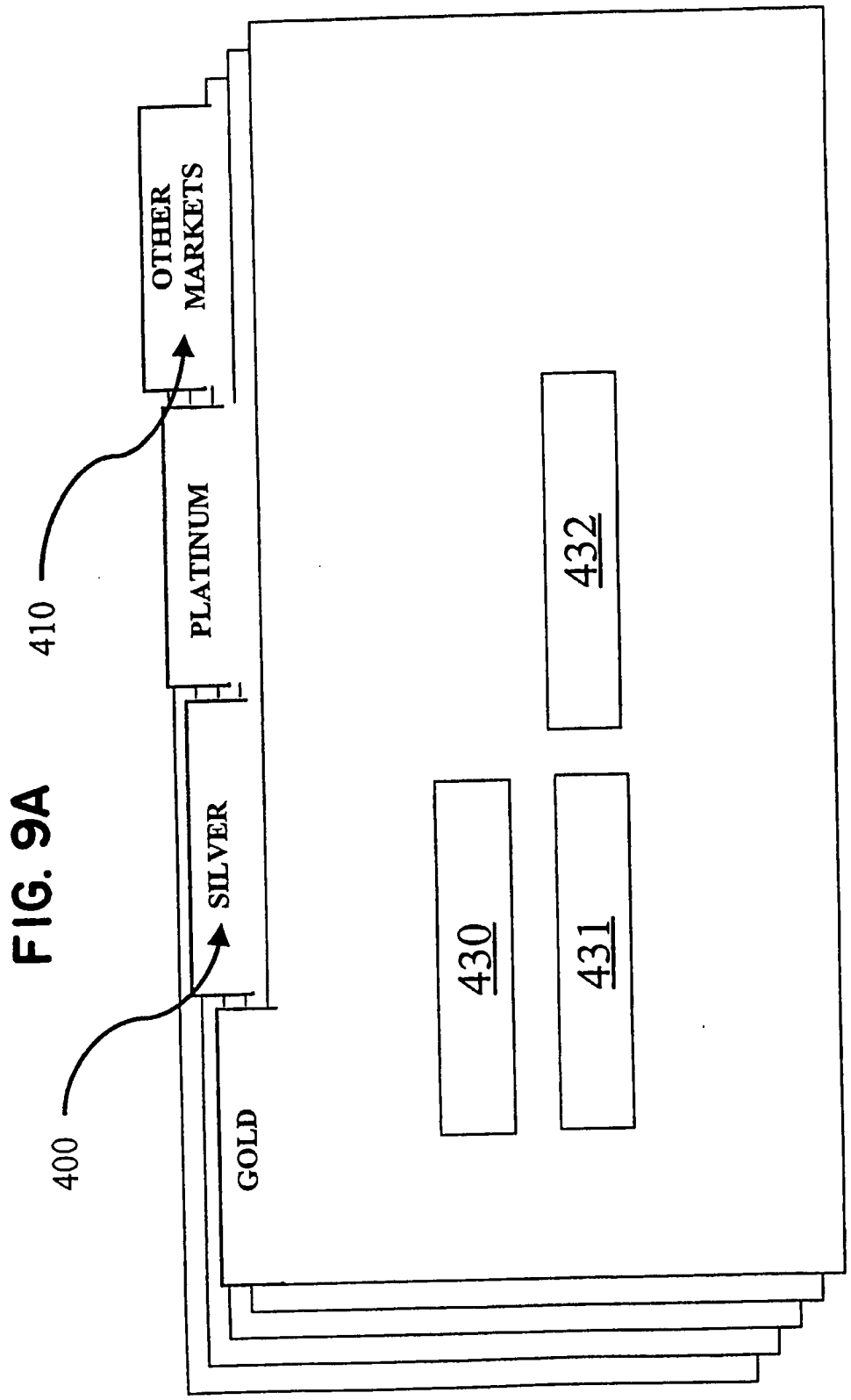
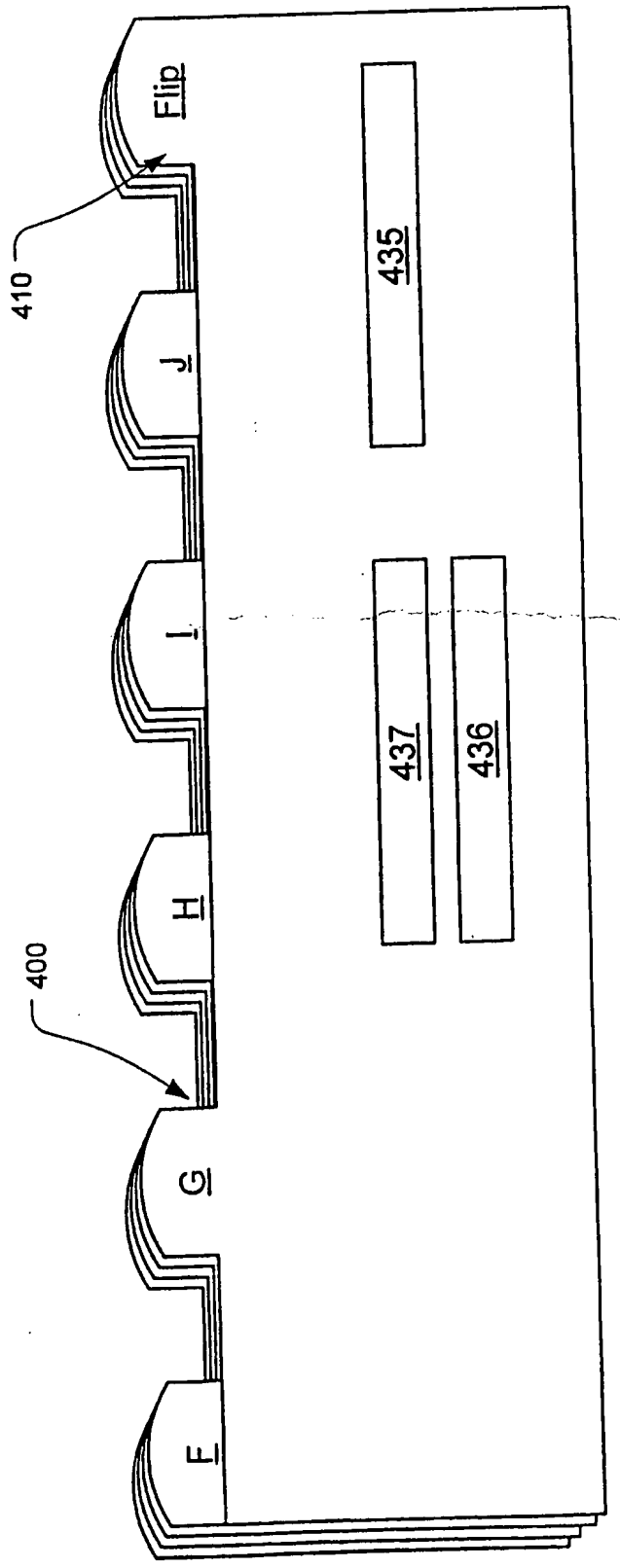


FIG. 9A

Petitioner Apple Inc. - Exhibit 1026, p. 264

FIG. 10



Petitioner Apple Inc. - Exhibit 1026, p. 265

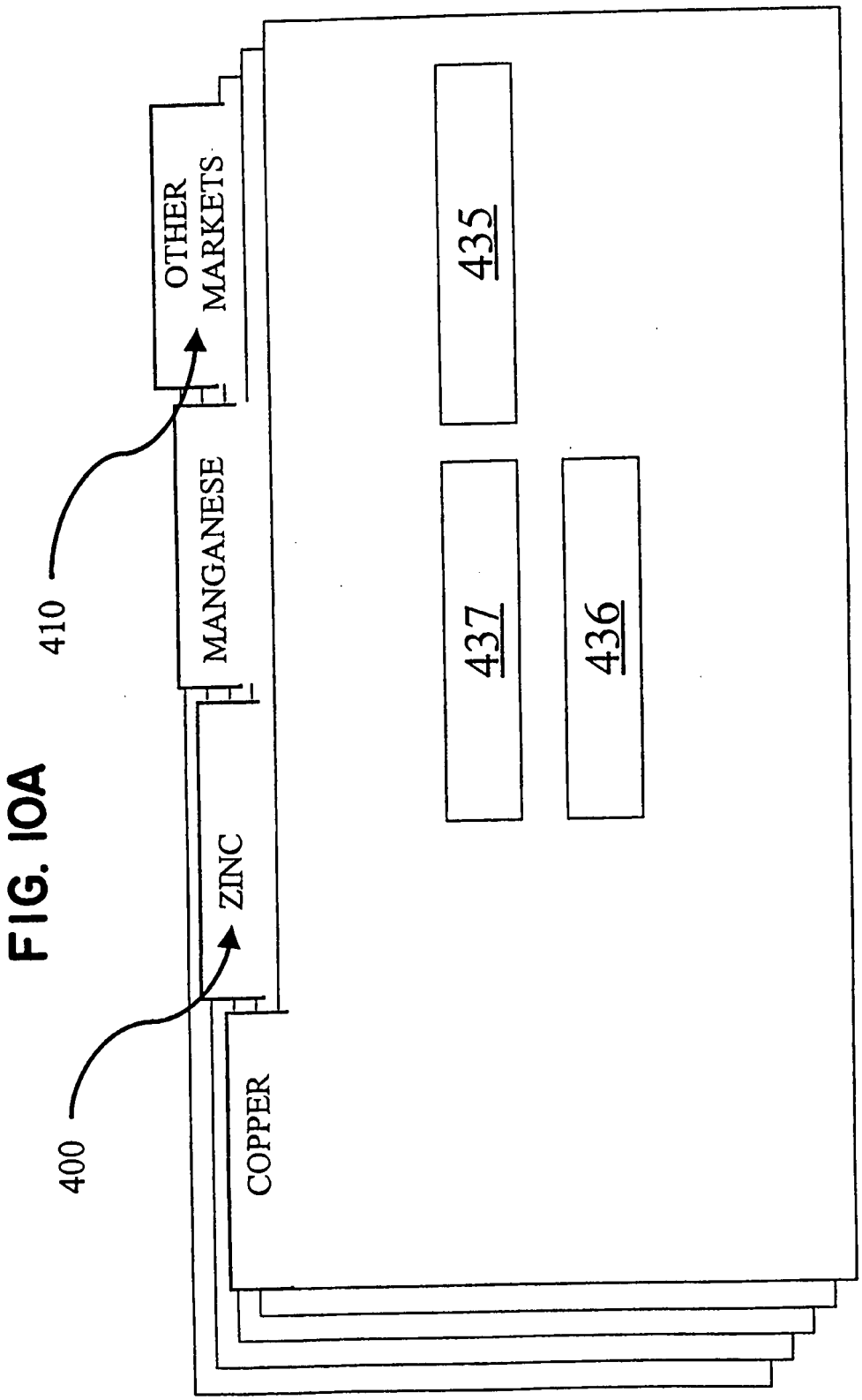


FIG. 10A

Petitioner Apple Inc. - Exhibit 1026, p. 266

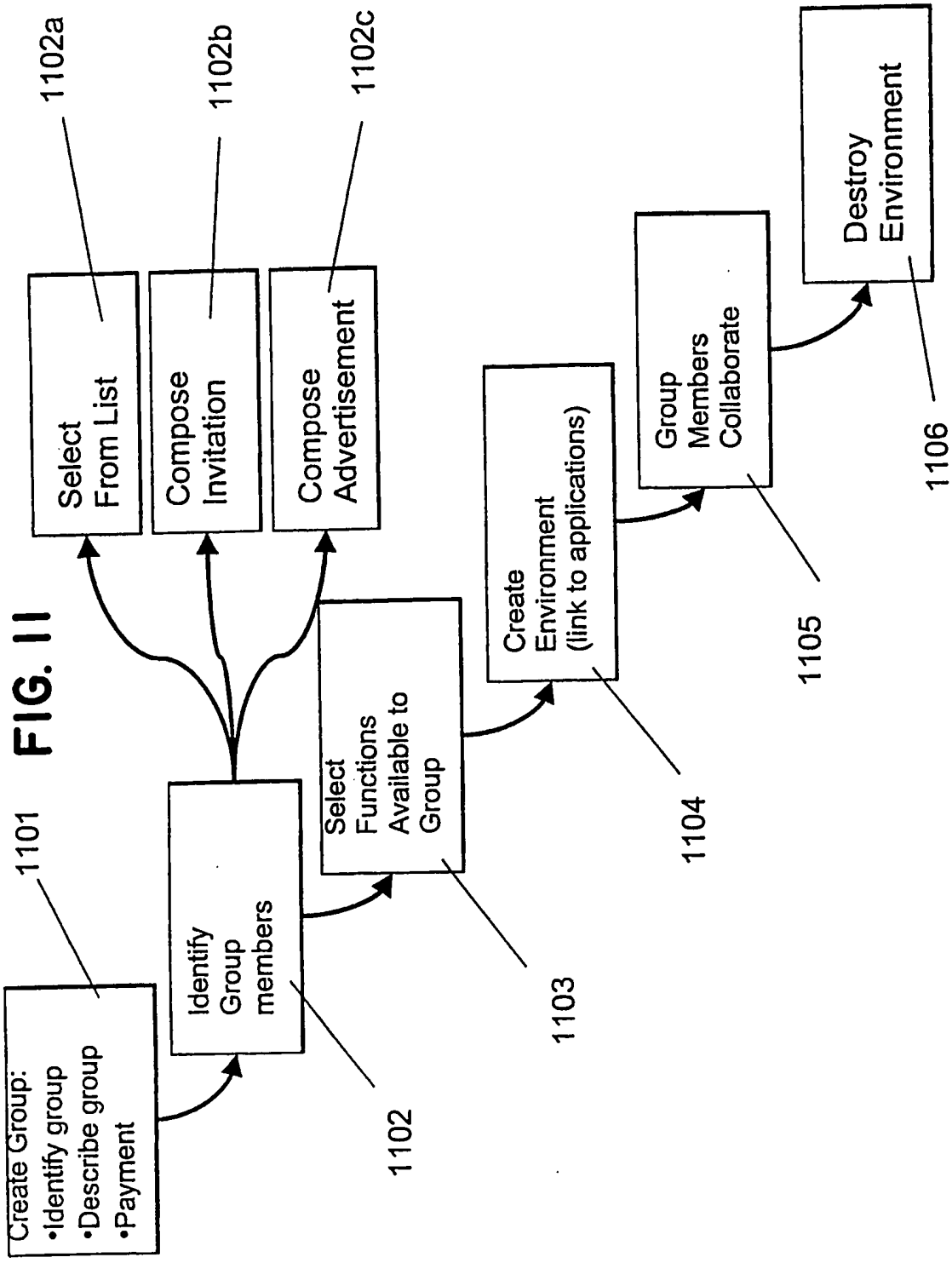


FIG. 11

Petitioner Apple Inc. - Exhibit 1026, p. 267

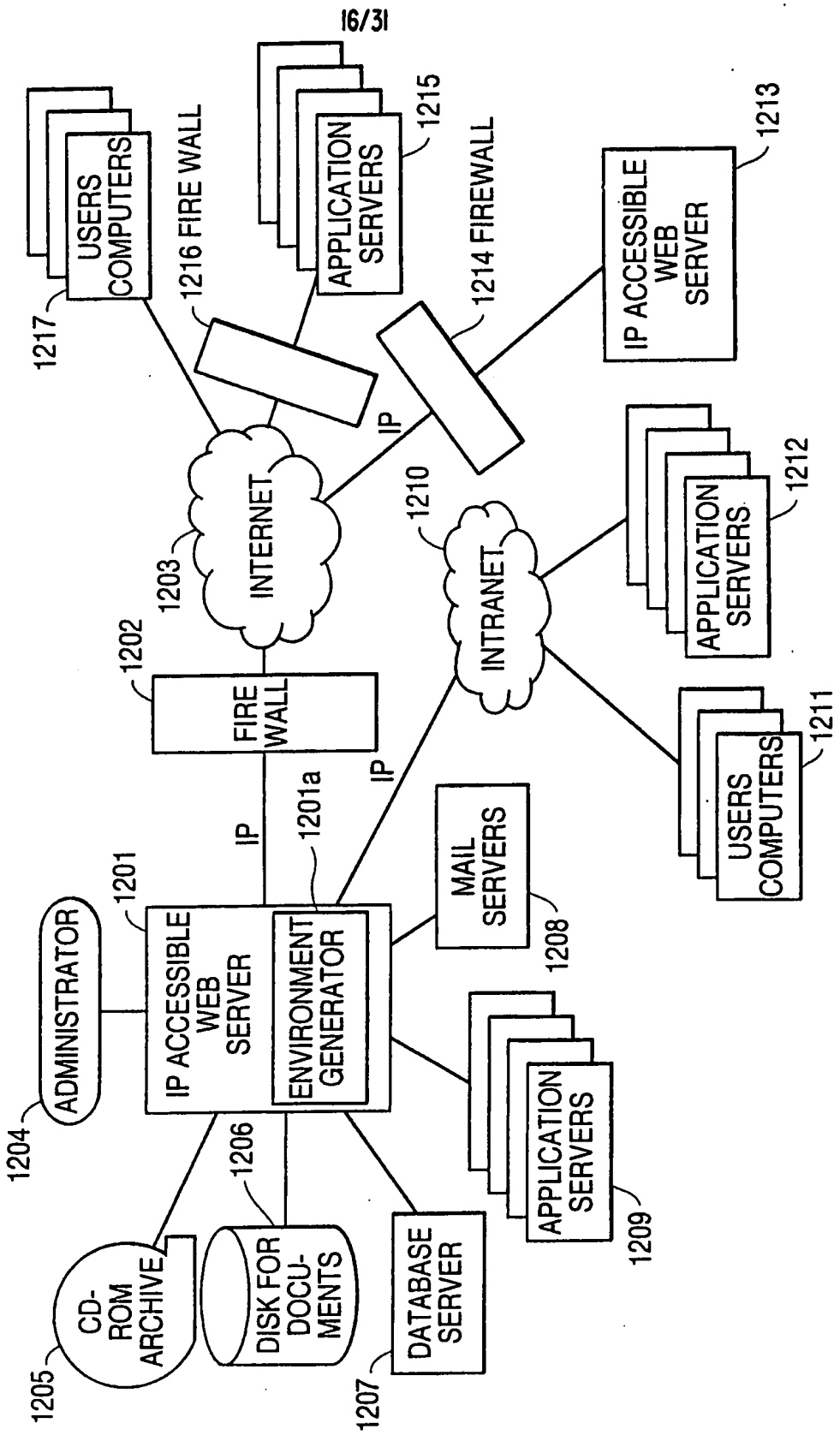


FIG. 12

Petitioner Apple Inc. - Exhibit 1026, p. 268

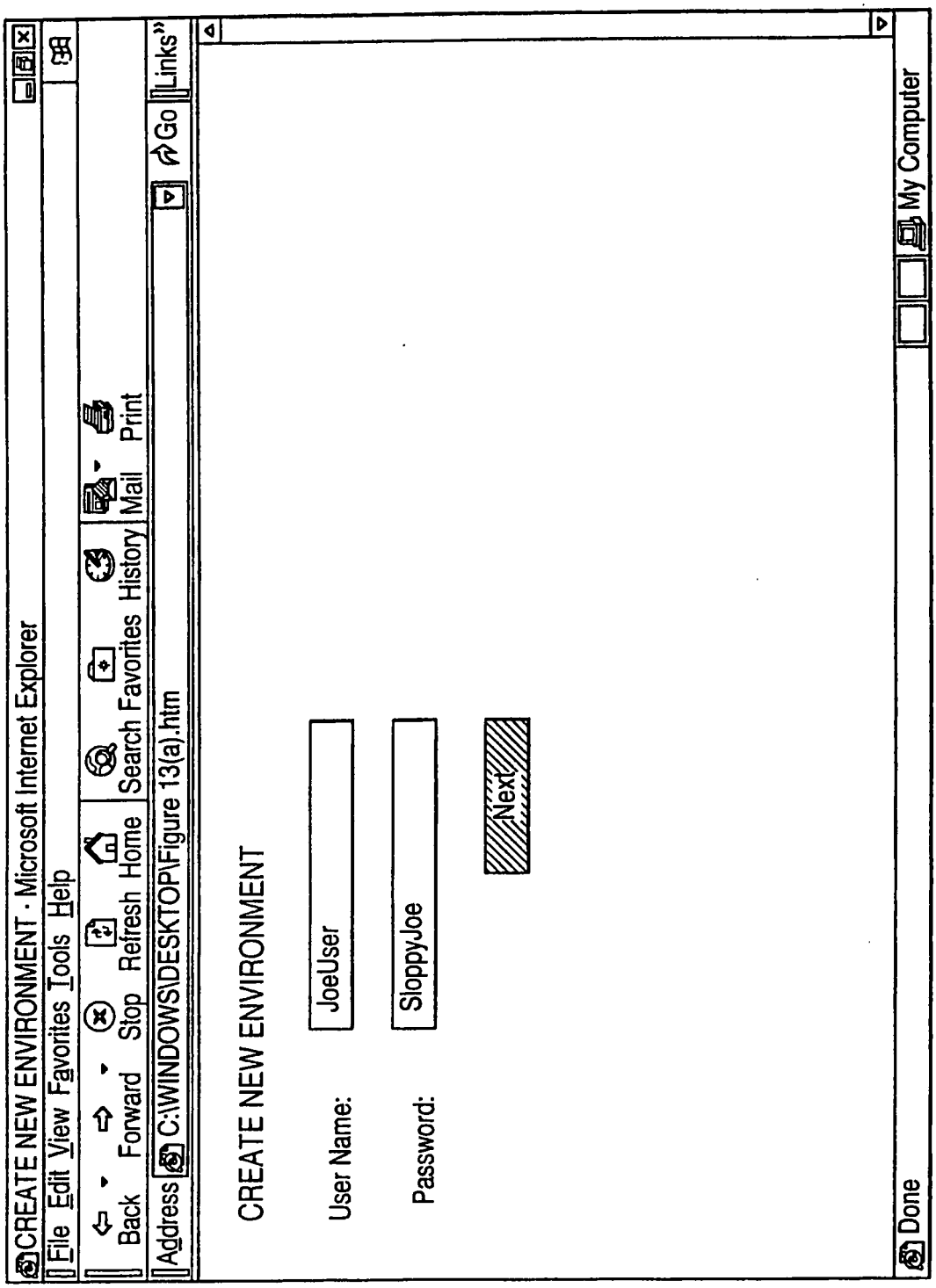


FIG. 13A

Petitioner Apple Inc. - Exhibit 1026, p. 269

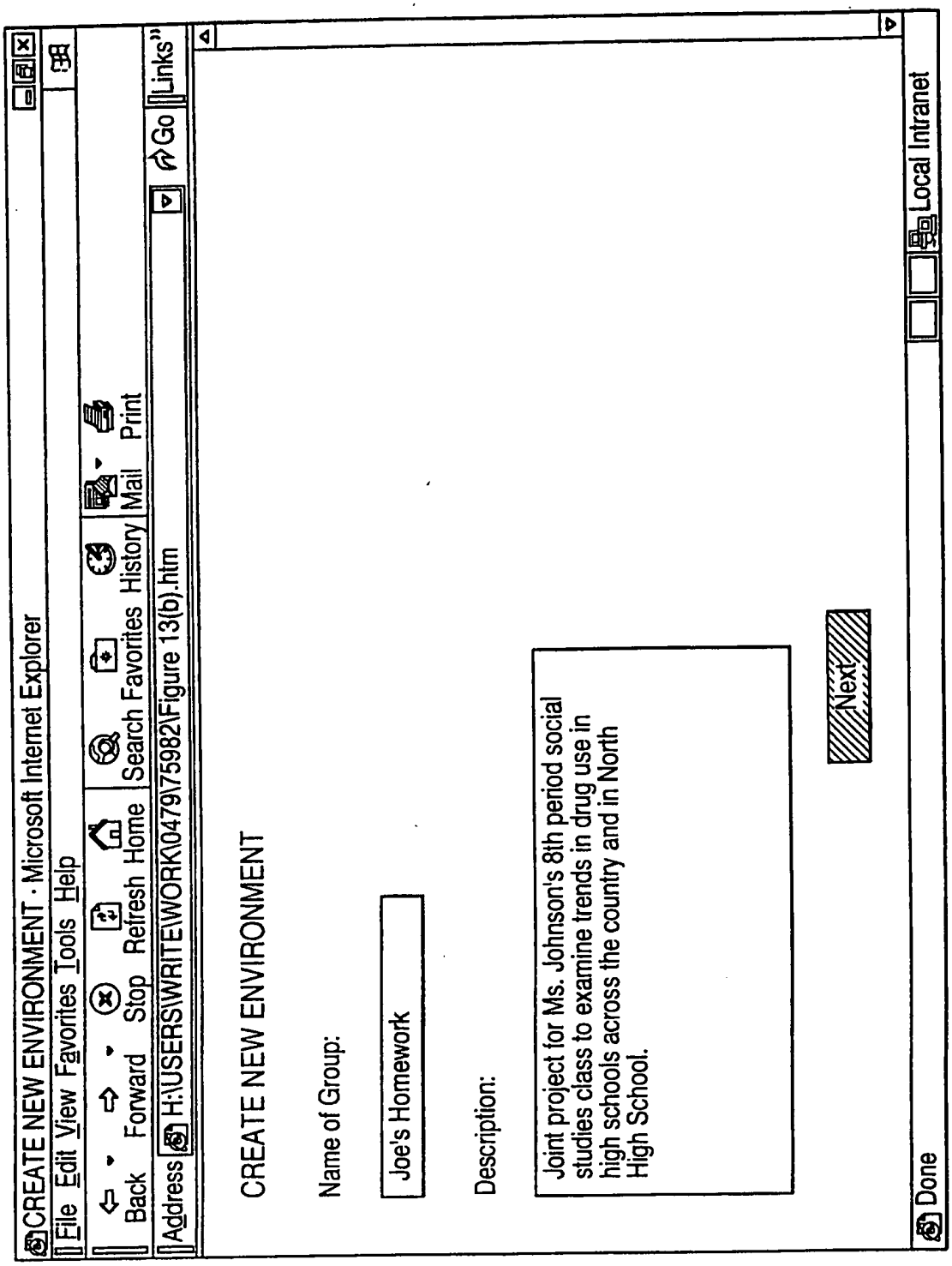


FIG. 13B

Petitioner Apple Inc. - Exhibit 1026, p. 270

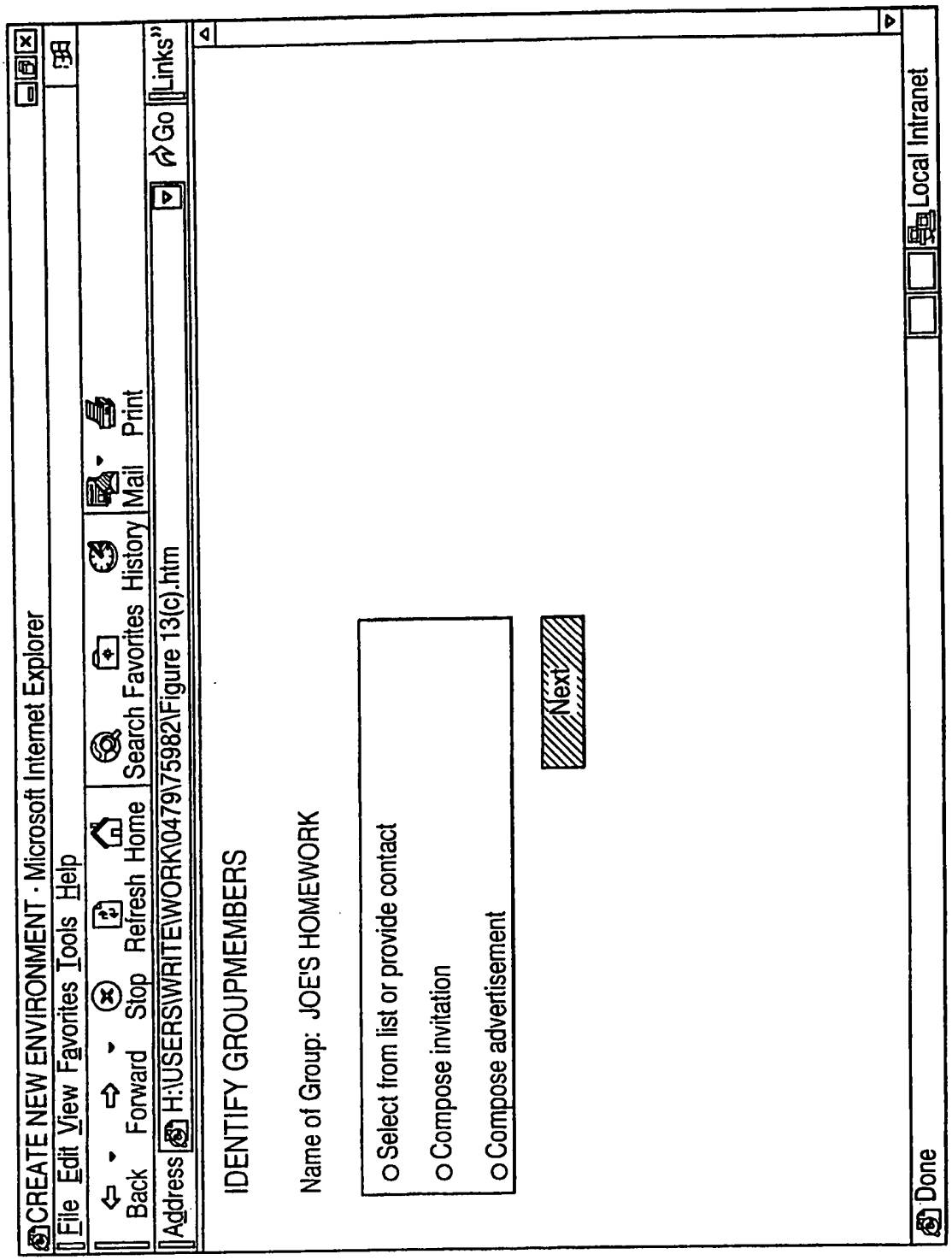


FIG. 13C

Petitioner Apple Inc. - Exhibit 1026, p. 271

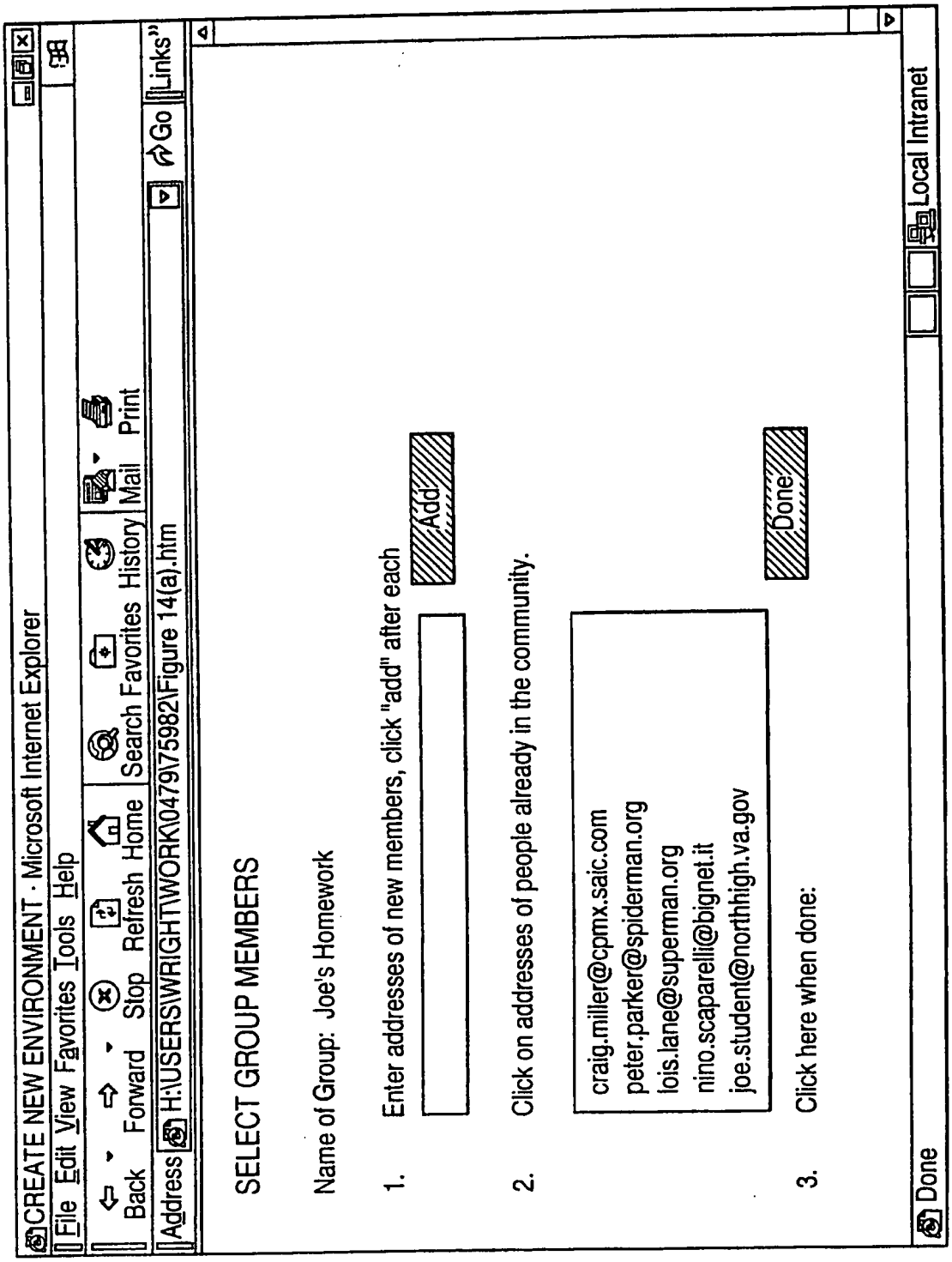


FIG. 14A

Petitioner Apple Inc. - Exhibit 1026, p. 272

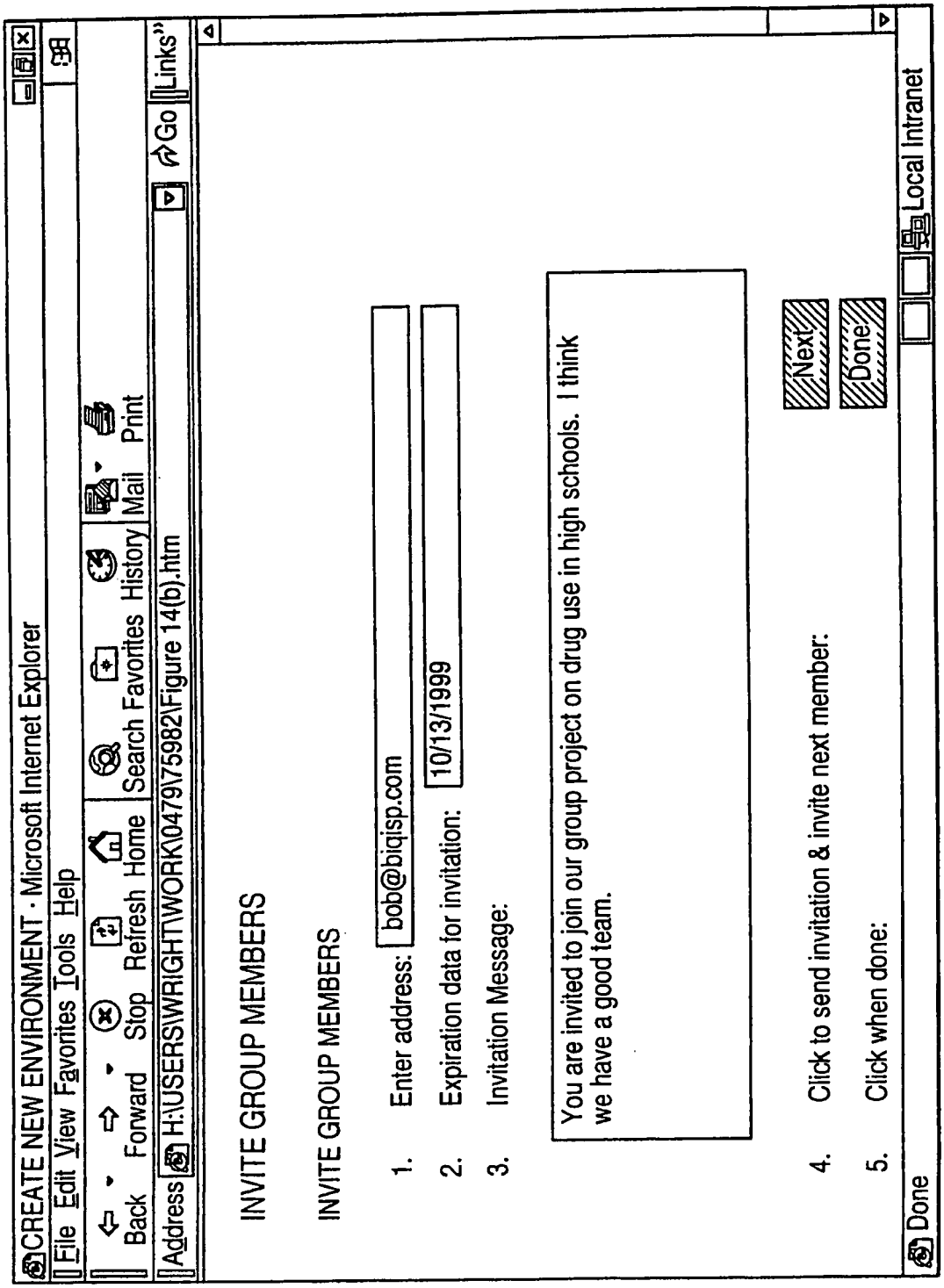


FIG. 14B

Petitioner Apple Inc. - Exhibit 1026, p. 273

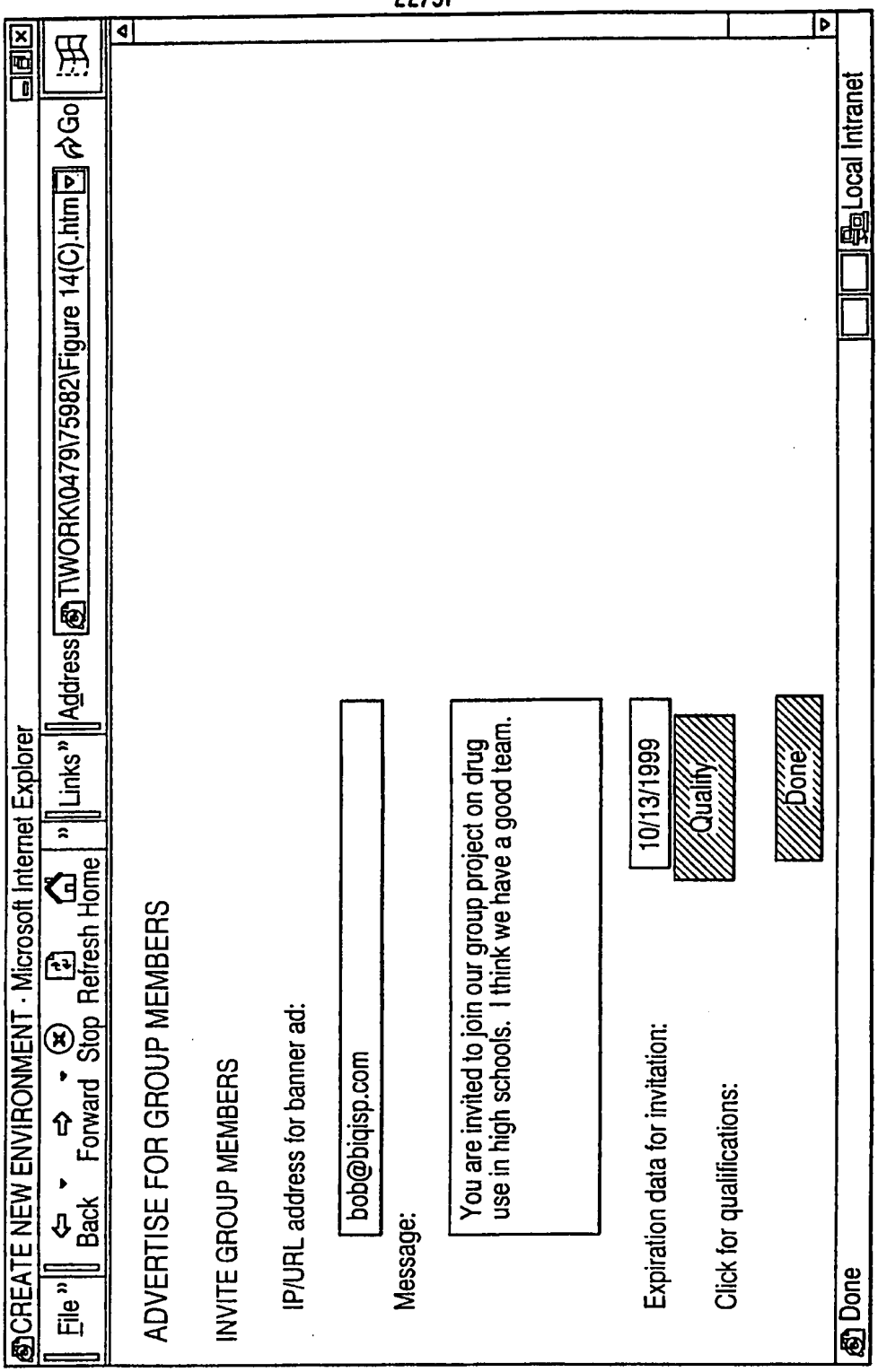


FIG. 14C

Petitioner Apple Inc. - Exhibit 1026, p. 274

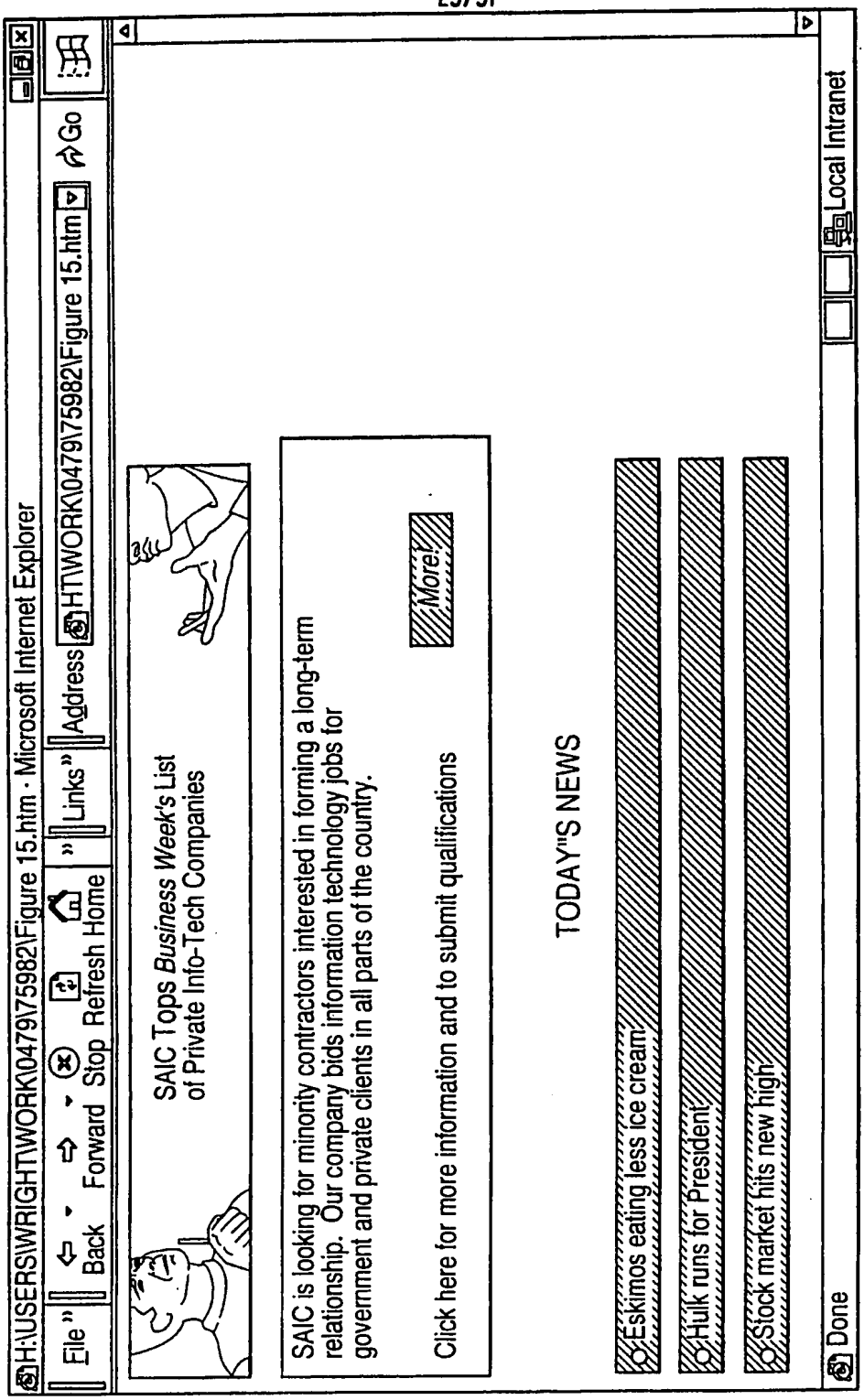
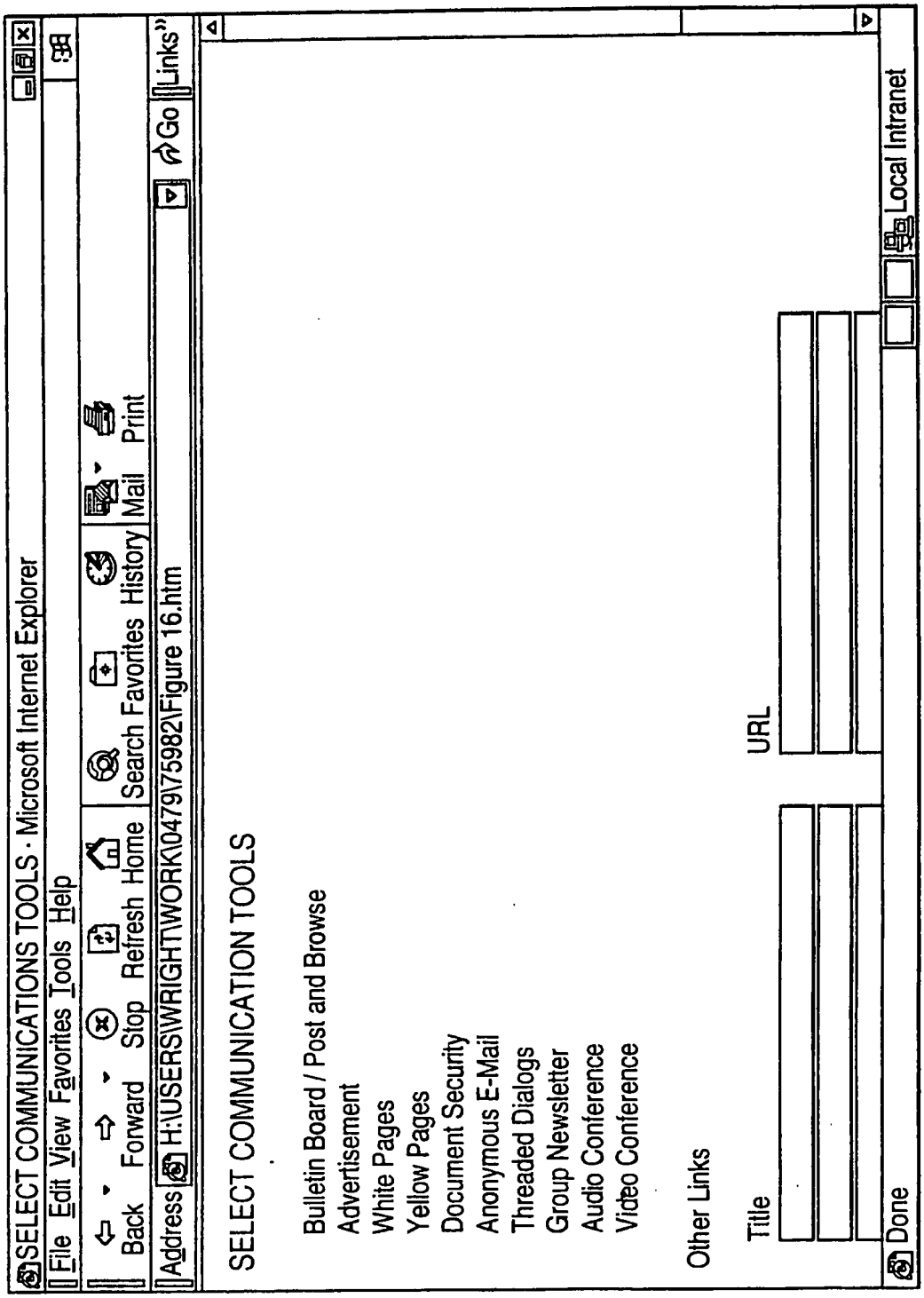


FIG. 15

Petitioner Apple Inc. - Exhibit 1026, p. 275

FIG. 16



Petitioner Apple Inc. - Exhibit 1026, p. 276

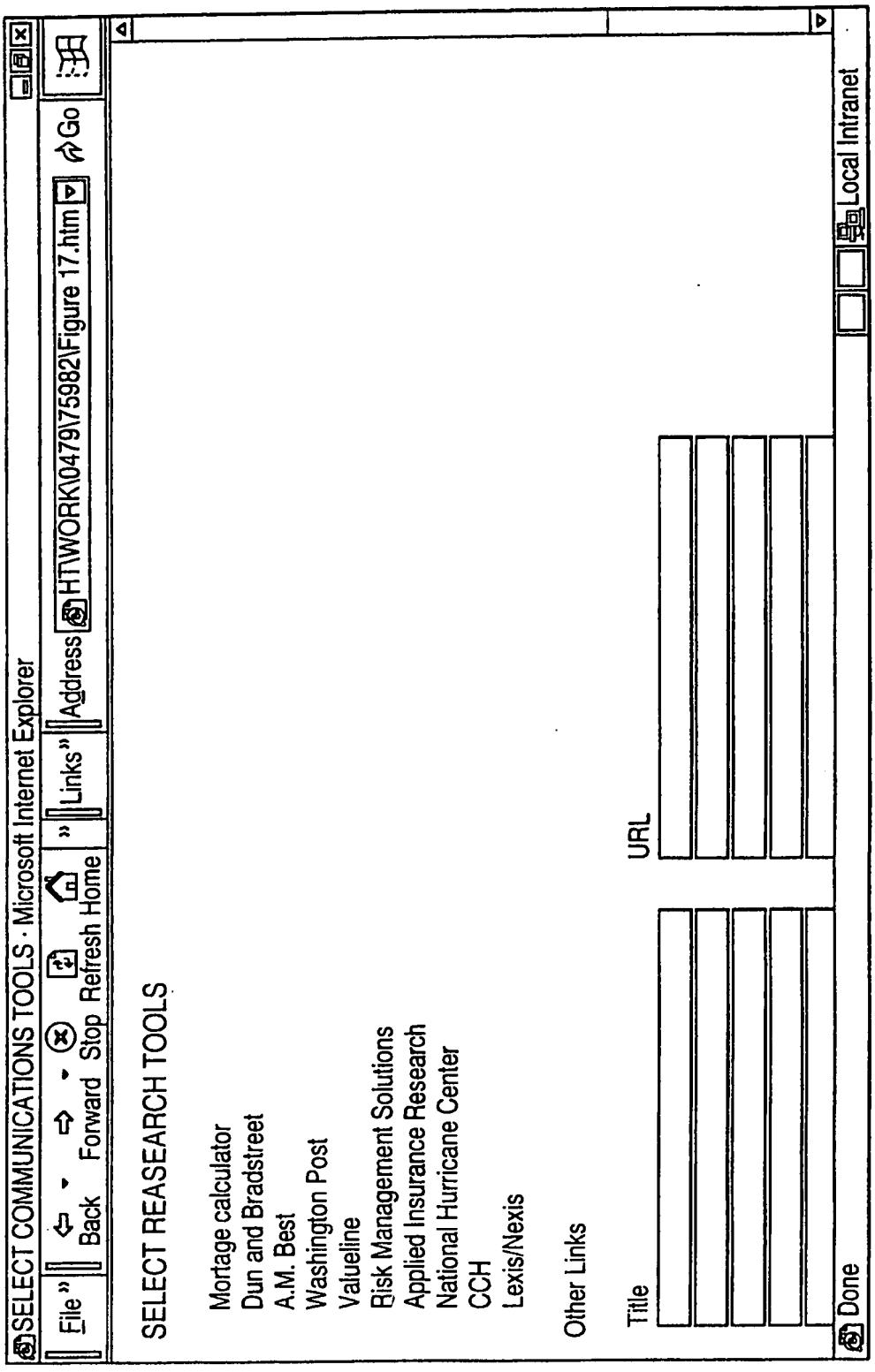


FIG. 17

Petitioner Apple Inc. - Exhibit 1026, p. 277

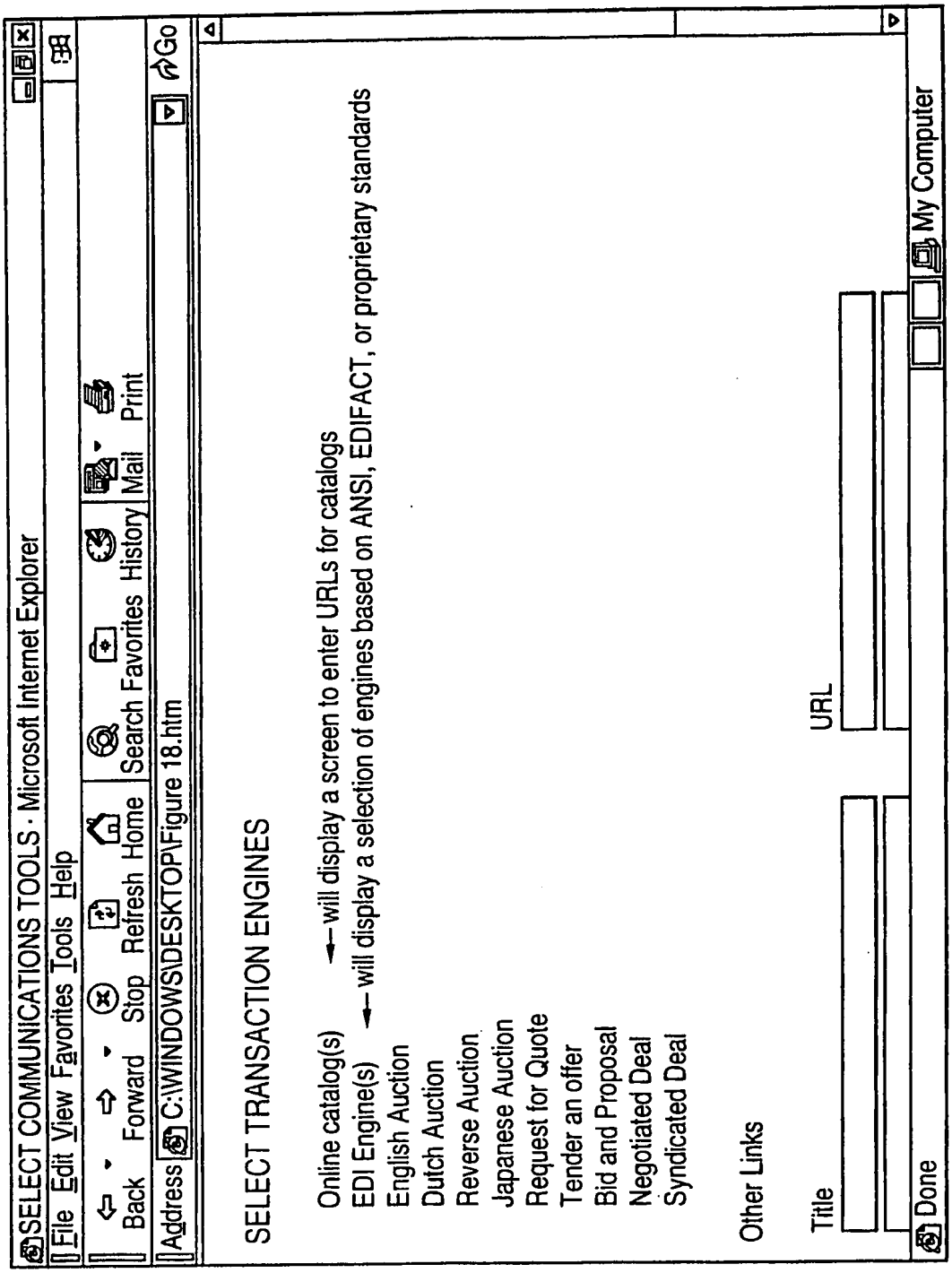


FIG. 18

Petitioner Apple Inc. - Exhibit 1026, p. 278

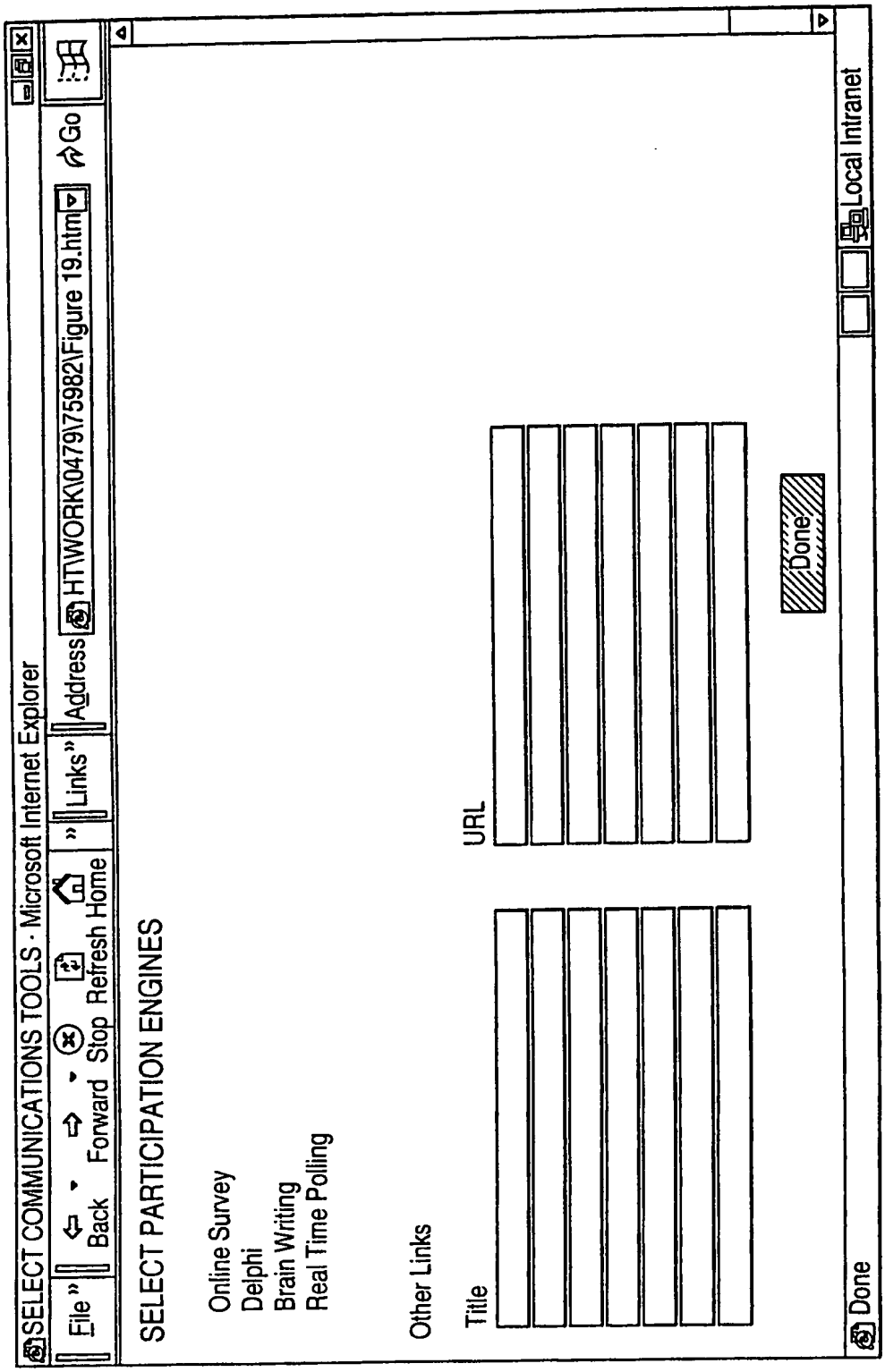


FIG. 19

Petitioner Apple Inc. - Exhibit 1026, p. 279

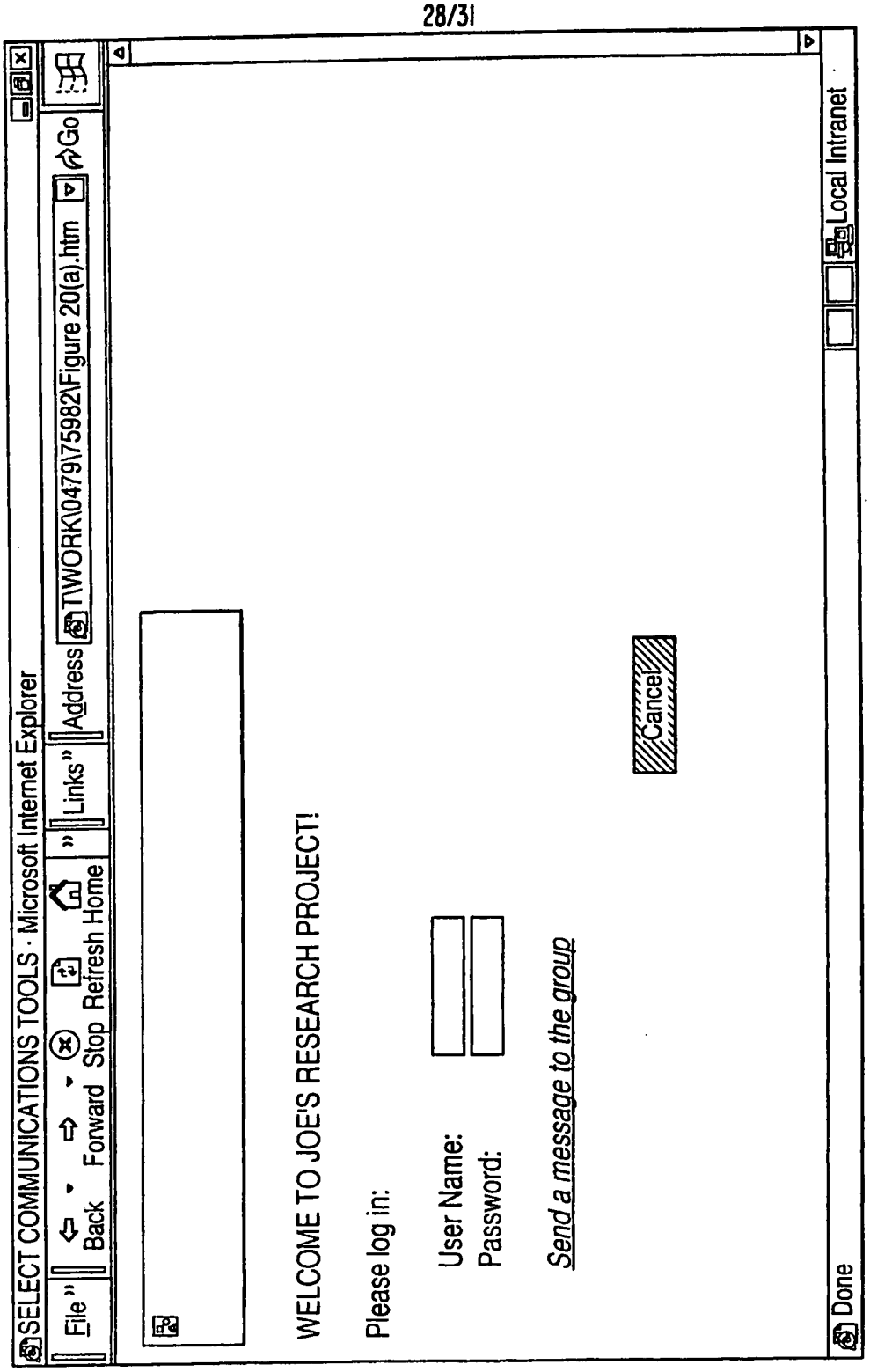


FIG. 20A

Petitioner Apple Inc. - Exhibit 1026, p. 280

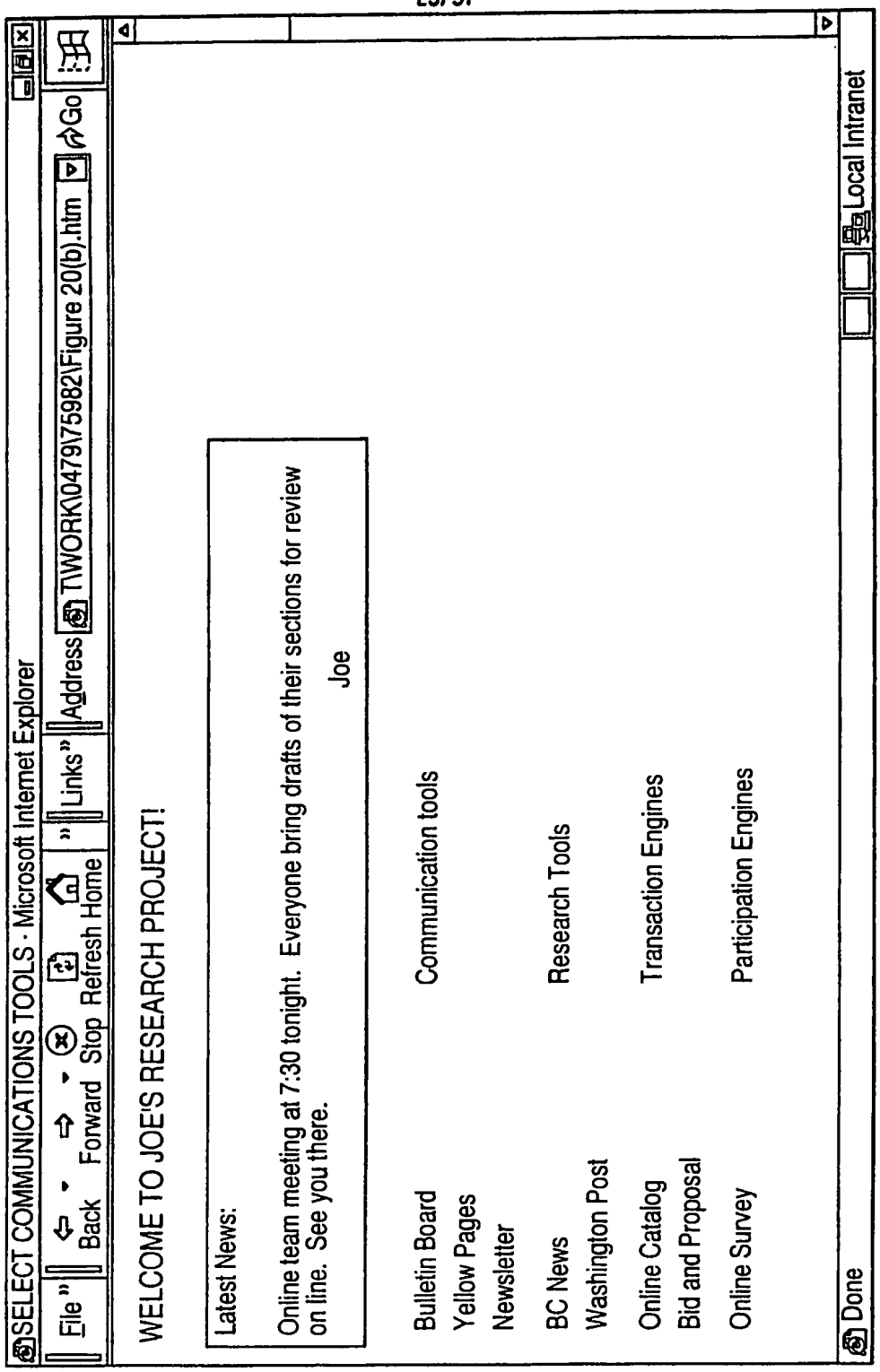


FIG. 20B

Petitioner Apple Inc. - Exhibit 1026, p. 281

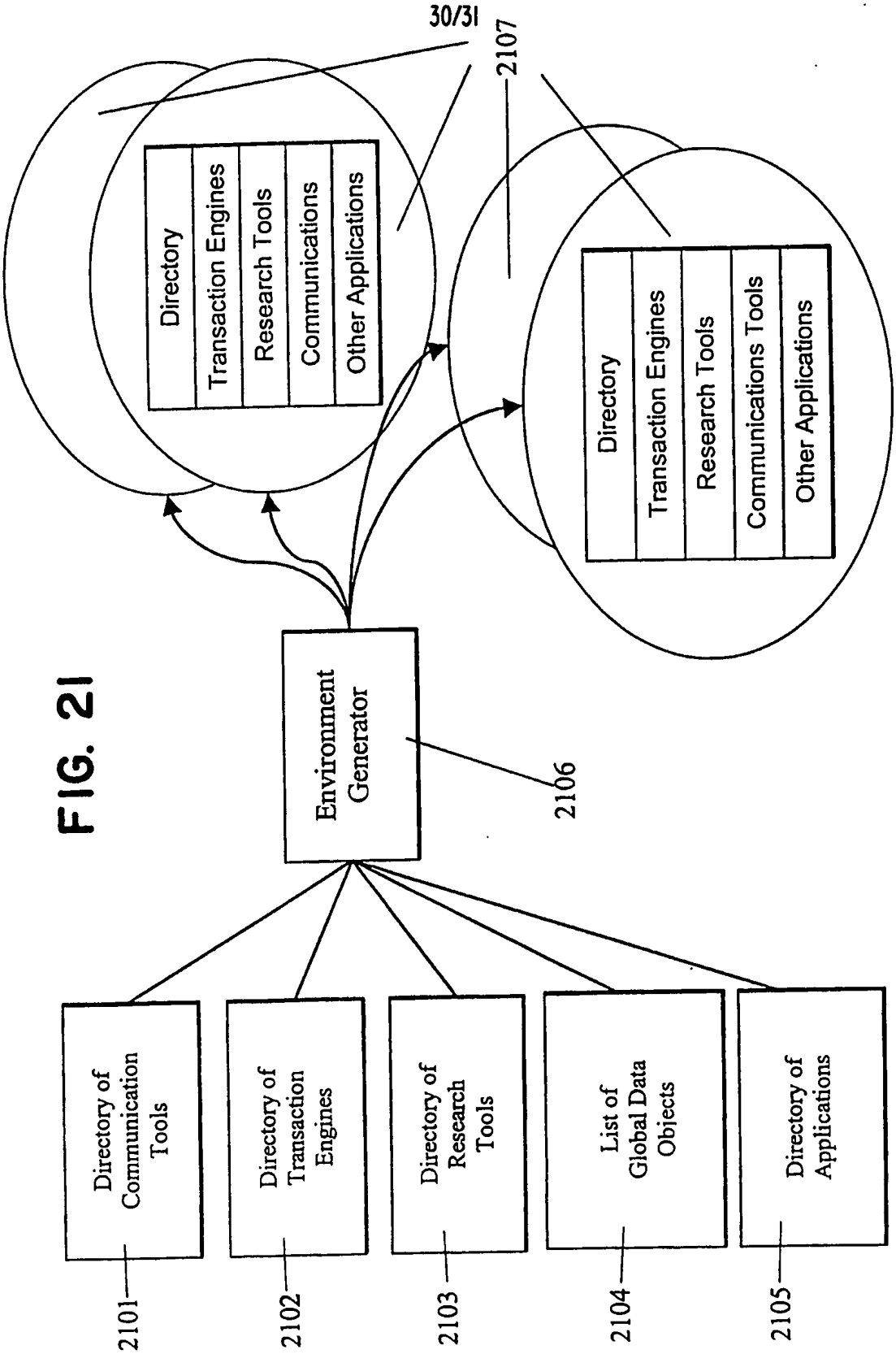
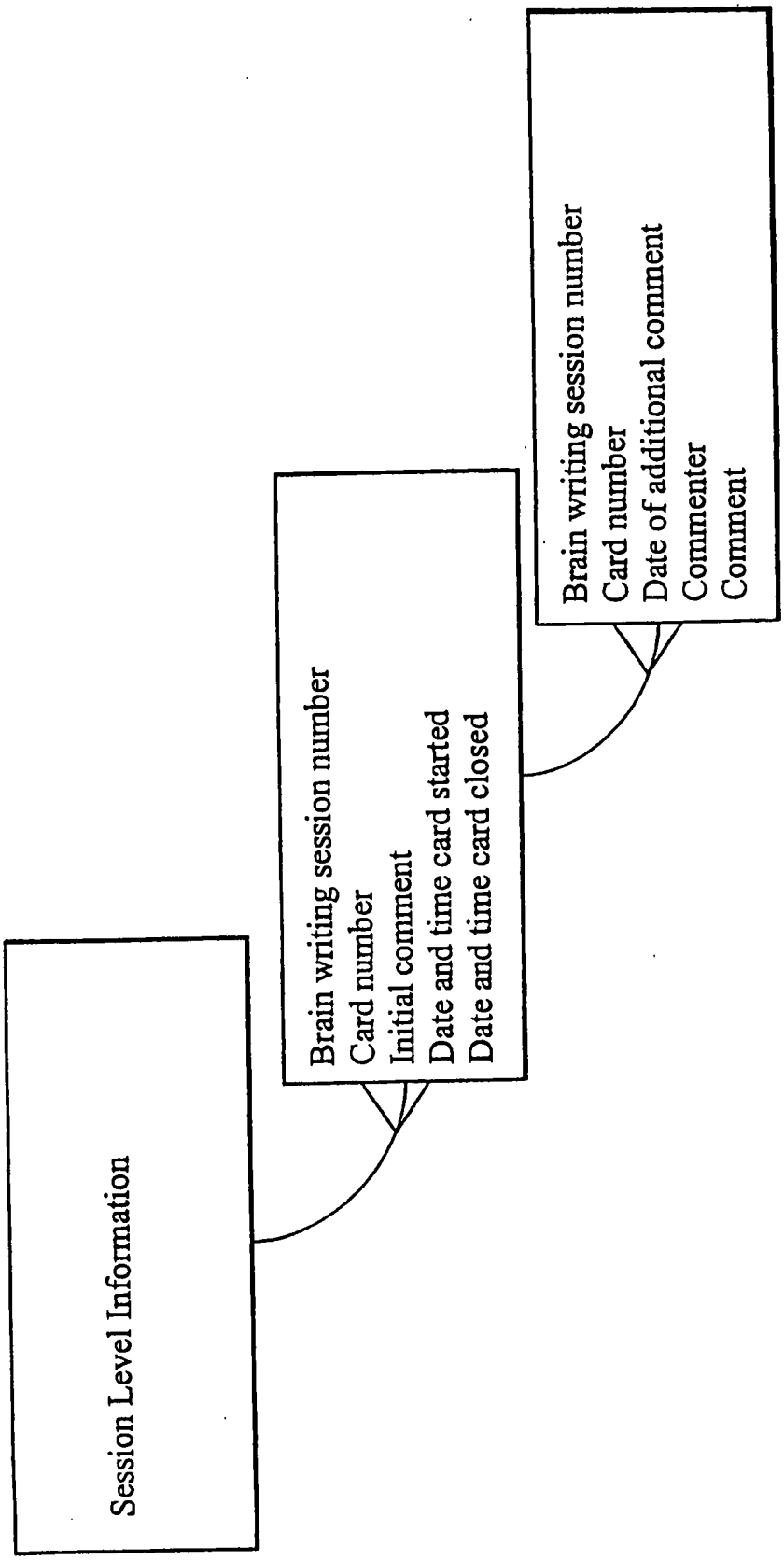


FIG. 21

Petitioner Apple Inc. - Exhibit 1026, p. 282

FIG. 22



Petitioner Apple Inc. - Exhibit 1026, p. 283

B10

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 11/00

A1

(11) International Publication Number: WO 00/70458

(43) International Publication Date: 23 November 2000 (23.11.00)

(21) International Application Number: PCT/US00/08219

(22) International Filing Date: 15 May 2000 (15.05.00)

(30) Priority Data:
60/134,547 17 May 1999 (17.05.99) US

(71) Applicant: COMSEC CORPORATION [US/US]; 10217 Cedar Pond Drive, Vienna, VA 22182 (US).

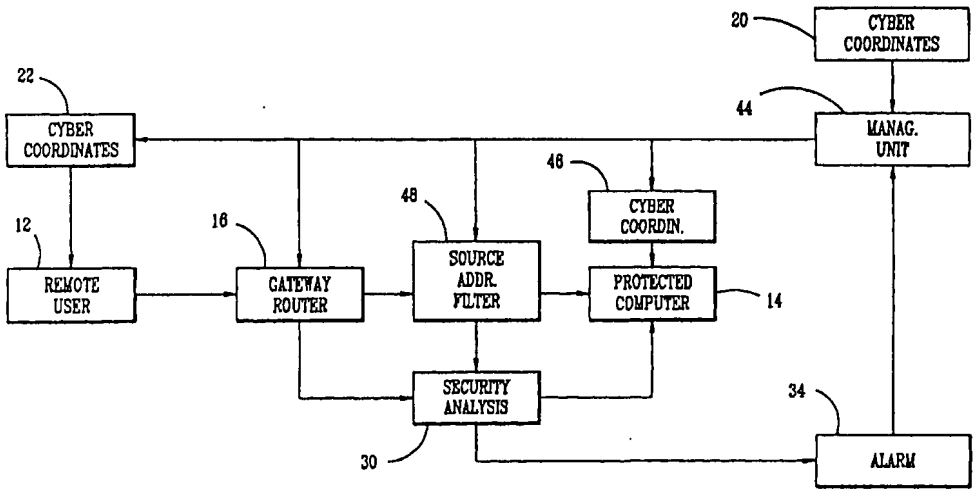
(72) Inventor: SHEYMOV, Victor, I.; 10217 Cedar Pond Drive, Vienna, VA 22182 (US).

(74) Agent: SIXBEY, Daniel, W.; Nixon Peabody LLP, Suite 800, 8180 Greensboro Drive, McLean, VA 22102 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD OF COMMUNICATIONS AND COMMUNICATION NETWORK INTRUSION PROTECTION METHODS AND INTRUSION ATTEMPT DETECTION SYSTEM



(57) Abstract

The intrusion protection method and system for a communication network provides address agility wherein the cyber coordinates of a target host (14) are changed both on a determined time schedule and when an intrusion attempt is detected. The system includes a managment unit (18) which generates a random sequence of cyber coordinates and maintains a series of tables containing the current and next set of cyber coordinates. These cyber coordinates are distributed to authorized users (12) under an encryption process to prevent unauthorized access.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD OF COMMUNICATIONS AND COMMUNICATION NETWORK INTRUSION PROTECTION METHODS AND INTRUSION ATTEMPT DETECTION SYSTEM

This application is a continuation-in-part application of U.S. Serial No. 60/134,547 filed May 17, 1999.

Background Art

Historically, every technology begins its evolution focusing mainly on performance parameters, and only at a certain developmental stage does it address the security aspects of its applications. Computer and communications networks follow this pattern in a classic way. For instance, first priorities in development of the Internet were reliability, survivability, optimization of the use of communications channels, and maximization of their speed and capacity. With a notable exception of some government systems, communications security was not an early high priority, if at all. Indeed, with a relatively low number of users at initial stages of Internet development, as well as with their exclusive nature, problems of potential cyber attacks would have been almost unnatural to address, considering the magnitude of other technical and organizational problems to overcome at that time. Furthermore, one of the ideas of the Internet was "democratization" of communications channels and of access to information, which is almost contradictory to the concept of security. Now we are faced with a situation, which requires adequate levels of security in communications while preserving already achieved "democratization" of communications channels and access to information.

All the initial objectives of the original developers of the Internet were achieved with results spectacular enough to almost certainly surpass their expectations. One of the most remarkable results of the Internet development to date is the mentioned "democratization". However in its unguarded way "democratization" apparently is either premature to a certain percentage of the Internet users, or contrary to human nature, or both. The fact remains that this very percentage of users presents a serious threat to the integrity of national critical infrastructure, to privacy of information, and to further advance of commerce by utilization

of the Internet capabilities. At this stage it seems crucial to address security issues but, as usual, it is desirable to be done within already existing structures and technological conventions.

Existing communications protocols, while streamlining communications, still lack underlying entropy sufficient for security purposes. One way to increase entropy, of course, is encryption as illustrated by U.S. Patent No. 5,742,666 to Finley. Here each node in the Internet encrypts the destination address with a code which only the next node can unscramble.

Encryption alone has not proven to be a viable security solution for many communications applications. Even within its core purpose, encryption still retains certain security problems, including distribution and safeguarding of the keys. Besides, encryption represents a "ballast", substantially reducing information processing speed and transfer time. These factors discourage its use in many borderline cases.

Another way is the use of the passwords. This method has been sufficient against humans, but it is clearly not working against computers. Any security success of the password-based security is temporary at best. Rapid advances in computing power make even the most sophisticated password arrangement a short-term solution.

Recent studies clearly indicate that the firewall technology, as illustrated by U.S. Patent No. 5,898,830 to Wesinger et al., also does not provide a sufficient long-term solution to the security problem. While useful to some extent, it cannot alone withstand the modern levels of intrusion cyber attacks.

On the top of everything else, none of the existing security methods, including encryption, provides protection against denial of service attacks. Protection against denial of service attacks has become a critical aspect of communication system security. All existing log-on security systems, including those using encryption, are practically defenseless against such attacks. Given a malicious intent of a potential attacker, it is reasonable to assume that, even having failed with an intrusion attempt, the attacker is still capable of doing harm by disabling the system with a denial of service attack. Since existing systems by definition have to deal with every log-on attempt, legitimate or not, it is certain that these systems cannot defend themselves against a denial of service attack.

The deficiencies of existing security methods for protecting communications systems leads to the conclusion that a new generation of cyber protection technology is needed to achieve acceptable levels of security in network communications.

Summary of the Invention

It is a primary object of the present invention to provide a novel and improved method of communications, and a novel and improved communication network intrusion protection method and systems and novel and improved intrusion attempt detection method and systems, adapted for use with a wide variety of communication networks including Internet based computers, corporate and organizational computer networks (LANs), e-commerce systems, wireless computer communications networks, telephone dial-up systems, wireless dial-up systems, wireless telephone and computer communications systems, cellular and satellite telephone systems, mobile telephone and mobile communications systems, cable based systems and computer databases, as well as protection of network nodes such as routers, switches, gateways, bridges, and frame relays.

Another object of the present invention is to provide a novel and improved communication network intrusion protection method and system which provides address agility combined with a limited allowable number of log-on attempts.

Yet another object of the present invention is to provide a novel and improved intrusion protection method for a wide variety of communication and other devices which may be accessed by a number, address code, and/or access code. This number, address code, and/or access code is periodically changed and the new number, address code, or access code is provided only to authorized users. The new number, address code, or access code may be provided to a computer or a device for the authorized user and not be accessible to others. This identifier causes the user's computer to transmit the otherwise unknown and inaccessible number, address code, and/or access code.

A still further object of the present invention is to provide a novel and improved communication network intrusion protection method and system wherein a plurality of different cyber coordinates must be correctly provided before access is granted to a protected communications unit or a particular piece of information. If all or some cyber coordinates

are not correctly provided, access is denied, an alarm situation is instigated and the affected cyber coordinates may be instantly changed.

For the purposes of this invention cyber coordinates are defined as a set of statements determining location of an object (such as a computer) or a piece of information (such as a computer file) in cyber space. Cyber coordinates include but are not limited to private or public protocol network addresses such as an IP address in the Internet, a computer port number or designator, a computer or database directory, a file name or designator, a telephone number , an access number and/or code, etc.

These and other objects of the present invention are achieved by providing a communication network intrusion protection method and system where a potential intruder must first guess where a target computer such as a host workstation is in cyber space and to predict where the target computer such as a workstation will next be located in cyber space. This is achieved by changing a cyber coordinate (the address) or a plurality of cyber coordinates for the computers such as workstations on a determined or random time schedule and making an unscheduled cyber coordinates change when the system detects an intrusion attempt. A limited number of log-on attempts may be permitted before an intrusion attempt is confirmed and the cyber coordinates are changed. A management unit is provided for generating a random sequence of cyber coordinates and which maintains a series of tables containing current and the next set of addresses. These addresses are distributed to authorized parties, usually with use of an encryption process.

The present invention further provides for a piece of information, a computer or a database intrusion protection method and system where a potential intruder must first guess where a target piece of information such as a computer file or a directory is in cyber space and to predict where the target piece of information will be next in cyber space. This is achieved by changing a cyber coordinate or a plurality of cyber coordinates for the piece of information on a determined or random time schedule and making an unscheduled cyber coordinates change when the system detects an intrusion attempt. A limited number of log-on attempts may be permitted before an intrusion attempt is confirmed and the coordinates changed. A management unit is provided for generating a random sequence of cyber coordinates and which maintains a series of tables containing current and the next set of cyber coordinates. These coordinates are distributed to authorized parties, usually by means

of an encryption process.

The intrusion attempt detection methods and systems are provided to the protected devices and pieces of information as described above by means of categorizing a log-on attempt when all or some of the correct cyber coordinates are not present as an intrusion attempt and by instigating an alarm situation.

Brief Description of the Drawings

Figure 1 is a block diagram of the communication network protection system of the present invention;

Figure 2 is a flow diagram showing the operation of the system of Figure 1;

Figure 3 is a block diagram of a second embodiment of the communication network protection system of the present invention;

Figure 4 is a flow diagram showing the operation of the system of Figure 3;

Figure 5 is a block diagram of a third embodiment of the communication network protection system of the present invention;

Figure 6 is a flow diagram showing the operation of the system of Figure 5; and

Figure 7 is a block diagram of a fourth embodiment of the communication network protection system of the present invention.

Description of the Preferred Embodiments

Existing communications systems use fixed coordinates in cyber space for the communications source and communications receiver. Commonly accepted terminology for the Internet refers to these cyber coordinates as source and destination IP addresses. For

purposes of an unauthorized intrusion into these communication systems, the situation of a cyber attack might be described in military terms as shooting at a stationary target positioned at known coordinates in cyber space. Obviously, a moving target is more secure than the stationary one, and a moving target with coordinates unknown to the intruder is more secure yet. The method of the present invention takes advantage of the cyber space environment and the fact that the correlation between the physical coordinates of computers or other communication devices and their cyber coordinates is insignificant.

While it is difficult to change the physical coordinates of computers or other communications devices, their cyber coordinates (cyber addresses) can be changed much easier, and in accordance with the present invention, may be variable and changing over time. In addition to varying the cyber coordinates over time, the cyber coordinates can immediately be changed when an attempted intrusion is sensed. Furthermore, making the current cyber coordinates available to only authorized parties makes a computer or other communications device a moving target with cyber coordinates unknown to potential attackers. In effect, this method creates a device which perpetually moves in cyber space.

Considering first the method of the present invention as applied to computers and computer networks, the computer's current cyber address may serve also as its initial log-on password with a difference that this initial log-on password is variable. A user, however, has to deal only with a computer's permanent identifier, which is, effectively its assigned "name" within a corresponding network. Any permanent identifier system can be used, and an alphabetic "name" system seems to be reasonably user-friendly. One of such arrangements would call for using a computer's alphabetic Domain Name System, as a cyber address permanent identifier, while subjecting its numeric, or any other cyber address to a periodic change with regular or irregular intervals. This separation will make the security system transparent to the user, who will have to deal only with the alphabetic addresses. In effect, the user's computer would contain an "address book" where the alphabetic addresses are permanent, and the corresponding variable addresses are more complex and periodically updated by a network's management. While a user is working with other members of the network on the name or the alphabetic address basis, the computer conducts communications based on the corresponding variable numeric or other addresses assigned for that particular time.

A variable address system can relatively easily be made to contain virtually any level of entropy, and certainly enough entropy to defy most sophisticated attacks. Obviously, the level of protection is directly related to the level of entropy contained in the variable address system and to the frequency of the cyber address change.

This scenario places a potential attacker in a very difficult situation when he has to find the target before launching an attack. If a restriction on a number of allowable log-on tries is implemented, it becomes more difficult for an attacker to find the target than to actually attack it. This task of locating the target can be made difficult if a network's cyber address system contains sufficient entropy. This difficulty is greatly increased if the security system also limits the number of allowable log-on tries, significantly raising the entropy density.

For the purpose of this invention, entropy density is defined as entropy per one attempt to guess a value of a random variable.

Figure 1 illustrates a simple computer intrusion protection system 10 which operates in accordance with the method of the present invention. Here, a remote user's computer 12 is connected to a protected computer 14 by a gateway router or bridge 16. A management system 18 periodically changes the address for the computer 14 by providing a new address from a cyber address book 20 which stores a plurality of cyber addresses. Each new cyber address is provided by the management system 18 to the router 16 and to a user computer address book 22. The address book 22 contains both the alphabetic destination address for the computer 14 which is available to the user and the variable numeric cyber address which is not available to the user. When the user wants to transmit a packet of information with the alphabetic address for the computer 14, this alphabetic address is automatically substituted for the current numerical cyber address and used in the packet.

With the reference to Figures 1 and 2, when a packet is received by the gateway router or bridge 16 as indicated at 24, the cyber address is checked by the gateway router or bridge at 26, and if the destination address is correct, the packet is passed at 28 to the computer 14. If the destination address is not correct, the packet is directed to a security analysis section 30 which, at 32 determines if the packet is retransmitted with a correct address within a limited number of log-in attempts. If this occurs, the security analysis section transmits the packet to the computer 14 at 28. However, if no correct address is

received within the allowed limited number of log-in attempts, the packet is not transmitted to the computer 14 and the security analysis section activates an alarm section 34 at 36 which in turn causes the management section to immediately operate at 38 to change the cyber address.

Sophisticated cyber attacks often include intrusion through computer ports other than the port intended for a client log-on. If a system principally described in connection with Figures 1 and 2 is implemented, the port vulnerability still represents an opening for an attack from within the network, that is if an attacker has even a low-level authorized access to a particular computer and thus knows its current variable address.

Computer ports can be protected in a way similar to protection of the computer itself. In this case port assignment for the computer becomes variable and is changed periodically in a manner similar to that described in connection with Figures 1 and 2. Then, a current assignment of a particular port is communicated only to appropriate parties and is not known to others. At the same time, similarly to methods described, a computer user would deal with permanent port assignments, which would serve as the ports' permanent "names".

This arrangement in itself may not be sufficient, however, to reliably protect against a port attack using substantial computing power because of a possible insufficient entropy density. Such a protection can be achieved by implementing an internal computer "port router" which would serve essentially the same role for port identifiers as the common gateway router or bridge 16 serves for computer destination addresses.

With reference to Figures 3 and 4 wherein like reference numerals are used for components and operations which are the same as those previously described in connection with Figures 1 and 2, a port router 40 is provided prior to the protected computer 14, and this port router is provided with a port number or designator by the management unit 18. This port number or designator is also provided to the user address book 22 and will be changed when the cyber address is changed, or separately. Thus, with reference to Figure 4, once the cyber address has been cleared at 26, the port number or designator is examined at 42. If the port number is also correct, the data packet will be passed to the computer 14 at 28. If the port number is initially incorrect, the packet is directed to the security analysis section 30 which at 32 determines if the packet is retransmitted with the correct port number within the limited number of log-in attempts.

The port protection feature can be used independently of other features of the system. It can effectively protect nodes of the infrastructure such as routers, gateways, bridges, and frame relays from unauthorized access. This can protect systems from an attacker staging a cyber attack from such nodes.

The method and system of the present invention may be adapted to provide security for both Internet based computer networks and private computer networks such as LANs.

Internet structure allows the creation of an Internet based Private Cyber Network (PCN) among a number of Internet-connected computers. The main concern for using the Internet for this purpose as an alternative to the actual private networks with dedicated communication channels is security of Internet-based networks.

The present invention facilitates establishment of adequate and controllable level of security for the PCNs. Furthermore, this new technology provides means for flexible structure of a PCN, allowing easy and practically instant changes in its membership. Furthermore, it allows preservation of adequate security in an environment where a computer could be a member of multiple PCNs with different security requirements. Utilizing the described concept, a protected computer becomes a "moving target" for the potential intruders where its cyber coordinates are periodically changed and the new coordinates are communicated on a "need to know" basis only to the other members of the PCN authorized to access this computer along with appropriate routers and gateways. This change of cyber coordinates can be performed either by previous arrangement or by communicating future addresses to the authorized members prior to the change. Feasible frequency of such a change can range from a low extreme of a stationary system changing cyber coordinates only upon detection of a cyber attack to an extremely high frequency such as with every packet. The future coordinates can be transmitted either encrypted or unencrypted. Furthermore, each change of position of each PCN member can be made random in terms of both its current cyber coordinates and the time of the coordinates change. These parameters of a protected PCN member's cyber moves are known only to the PCN management, other PCN members with authorization to communicate with this particular member, and appropriate gateways and routers. PCN management would implement and coordinate periodic cyber coordinates changes for all members of the PCN. While the PCN management is the logical party to make all the notification of the cyber coordinates changes, in certain instances it

could be advantageous to shift a part of this task to a PCN member computer itself. With certain limitations, the routers and gateways with the "need to know" the current address of the protected computer are located in cyber space in the general vicinity of the protected computer. In such instances the protected computer could be in a better position to make the mentioned notifications of nearby routers and gateways.

The address changes could be done simultaneously for all the members of the PCN, or separately, particularly if security requirements for the members substantially differ. The latter method is advantageous, for instance, if some of the computers within the PCN are much more likely than others to be targeted by potential intruders. A retail banking PCN could be an example of such an arrangement where the bank's computer is much more likely to be attacked than a customer's computer. It should be noted that, while in certain cases some members of the PCN may not require any protection at all, it still is prudent to provide it as long as the computer belongs to a protected PCN. The correct "signature" of the current "return address" would serve as additional authenticity verification. In the above example of the retail banking, while many customers' computers may not require any protection, assigning variable addresses to them would serve as an additional assurance to the bank that every log-on is authorized. In fact, this system automatically provides two-tier security. In order to reach a protected computer, the client computer has to know the server computer current cyber address in the first place. Then, even if a potential intruder against odds "hits" the correct current address the information packet is screened for the correct "signature" or return address. If that signature does not belong to the list of the PCN's current addresses, the packet is rejected. In high security instances this should trigger an unscheduled address change of the protected computer.

With the reference to Figures 5 and 6 which illustrate this two-tier security system, a network management unit 44 provides different unique cyber coordinates to the address books for each computer in the system (two computers 12 and 14 with address books 22 and 46 respectively being shown). Now when the computer 12 sends a data packet to the computer 14, the gateway router or bridge 16, first checks for the correct current destination address for the computer 14 at 26 in the manner previously described. If the destination address is correct, a source address sensor 48 checks at 50 to determine if the correct source address (i.e. return address) for the computer 12 is also present. If both correct addresses are

present, the data packet is passed to the computer 14 at 28, but if the correct source address is not present, the data packet is passed to the security analysis section 30 where at 32 where it is determined if a correct source address is received within the acceptable number of log-on tries. If the correct return address is not received, an alarm situation is activated at 36 and the network management system operates at 38 to change the cyber address of the computer 14

In addition to the penetration (hacking) detection and protection, the system above provides real-time detection of a cyber attack and protection against "flooding" denial of service attacks. A gateway router or bridge 16 filters all the incorrectly addressed packets thus protecting against "flooding". Further yet, since the "address book" of the protected network contains only trusted destinations, this system also protects against instructive viruses or worms if such are present or introduced into the network. For the purpose of this invention, an instructive virus or worm is defined as a foreign unit of software introduced into a computer system so it sends certain computer data to otherwise unauthorized parties outside of the system.

Elements of the system described above are: a gateway router or bridge 16, a computer protection unit, and a management unit. A gateway router or bridge represents an element of collective defense for the network, while the source address filter and the "port router" and filter represent a unit of individual defense for a member computer. This individual defense unit (server unit) can be implemented either as a standalone computer, as a card in the protected computer, as software in the protected computer, or imbedded into the protected computer operating system. For further improvement of the overall security, port assignments can be generated autonomously from the management unit thus creating a "two keys" system in a cryptographic sense. This would allow for security to still be in place even if a security breach happened at the security management level.

The method and system of the present invention minimize human involvement in the system. The system can be configured in such a way that computer users deal only with simple identifiers or names permanently assigned to every computer in the network. All the real (current) cyber coordinates can be stored separately and be inaccessible to the user, and could be available to the appropriate computers only. This approach both enhances security and makes this security system transparent to the user. The user deals only with the simple

alphabetic side of the "address book", and is not bothered with the inner workings of the security system. A telephone equivalent of this configuration is an electronic white pages residing in a computerized telephone set, which is automatically updated by the telephone company. The user just has to find a name, and push the "connect" button while the telephone set does the rest of the task.

A numeric cyber address system, based on the Internet host number could be relatively easily utilized for the discussed security purposes, however a limitation exists for this address system in its current form represented by the IPv.4 protocol. This limitation is posed by the fact that the address is represented by a 32-bit number. 32-bit format does not contain sufficient entropy in the address system to enable establishment of adequate security. This is a particularly serious limitation in regard to securing an entire network. The availability of the network numbers are limited to the extent that not only entropy, but a simple permanently assigned number is becoming more and more difficult to obtain with the rapid expansion of the Internet.

If this address system is to be used for the security purposes, than the format of the host number should be adequately expanded to create sufficient size of the address numbers field in the system. If this is done, than the corresponding address in the Domain Name System (DNS) could be conveniently used as permanent identifier for a particular computer and the Internet host number would be variable, creating a moving regime of a protected computer. Currently being implemented IPv.6 (IPNG) protocol solves this problem by providing sufficient entropy.

Another way to achieve the same goal is to use the DNS address as a variable for security purposes. This way, the traditional Internet DNS address system would not be affected and no change in format is required. The relevant part of the protected computer's DNS address would become a variable, utilizing more characters than the alphabet, with a very large number of variations, also creating sufficient level of entropy.

Yet another way to implement the same method is to utilize the geographic zone-based system. While its utilization is somewhat similar to the DNS system, it offers some practical advantages for security use. Naturally, when a computer is protected by a security system, it is still essential to preserve the communication redundancy of the Internet communications. However, the redundancy may suffer if only a limited number of the

routers and gateways are informed of the protected computer current cyber address. This effect could be particularly important with the members of a particular protected network vastly remote in geographic terms. The necessary notification of a large number of the routers and gateways can also become problematic, not only technically, but also because it can decrease the level of security. In this sense a geographic zone-based system offers advantages since the variable part of the computer's cyber address could be made to involve only certain geographic locale while initial routing of the information packet could be done by the traditional method. After the packet has been moved to the general vicinity of the addressee computer, it would get into the area of the "informed" routers and gateways. This scheme would simplify the notification process of the routers as well as improve security by limiting the number of the "need to know" parties. It is important to recognize that, after the "general" part of the cyber address caused the information packet to arrive in a cyber vicinity of the addressee, virtually any, even private, address system can be used for the rest of he the delivery. This would further increase the level of underlying entropy in the system.

While certain specific address systems have been discussed, it is an important quality of the present invention that it can be implemented with virtually any address system.

Corporate and organizational computer networks such as LANs or, at least those in closed configurations, do not possess as much vulnerability to cyber attacks as Internet-based networks. However, even in these cases, their remote access security is a subject of concern. This is especially visible when a private network (PN) contains information of different levels of confidentiality with access restricted to appropriate parties. In other words, along with other generally accessible organizational information, an organizational PN can contain information restricted to certain limited groups. Enforcement of these restrictions requires a remote access security system. Usually these security systems employ a password-based scheme of one type or another and, perhaps, a firewall. However, reliance on passwords may not be entirely justified since the passwords can be lost or stolen, giving a malicious insider with a low access level a reasonable chance of access to information intended only for higher levels of access. Furthermore, in some cases use of cracking techniques from such a position is not entirely out of the question. Such an occurrence can relatively easily defeat both the password and the firewall. This would prevent a LAN from a cyber attack launched from within the network.

The present invention provides adequate security to such PCNs without reliance on the passwords and to limit access to only appropriate computers. Then, the task of overall information access security practically would be narrowed down to control of physical access to a particular computer, usually a less complicated feat.

Similarly to the systems described for Internet-based networks, a "closed" LAN as well as an Internet-based LAN can be protected by implementation of periodic changes of the members' network addresses and communicating those changes to the appropriate parties. This way, the lowest access level computers would have the lowest rate of address change. The rate of the address change would increase with the level of access. This system would ensure that all the PCN computers with legitimate access to a particular computer within the PCN would be informed of its location. Furthermore, it will ensure that the current location of a computer with restricted information would be unknown to the parties without the legitimate access clearance. For instance, a superior's computer would be able to access his subordinate's computer but not vice versa.

Also similarly to the systems described for the PCNs, a PCN computer would contain an "address book" where the user can see and use only the permanent side of it with identifiers of all computers accessible to him while the actual communication functions are performed by the computer using the variable side of the "address book" periodically updated by the PN management. To further enhance security, in addition to the computer address system management, the PCN Administrator can implement an automatic security monitoring system where all wrongly addressed log-on attempts would be registered and analyzed for security purposes.

Thus the method and system of the present invention would allow reliable protection against unauthorized remote access to information from within a PN while providing a great deal of flexibility, where the granted access can be revised easily and quickly.

A greatly enhanced intrusion protection system and method can be achieved by combining the operating systems of Figures 1-6. Now an arriving data packet would first be screened by a gateway router or a similar device for a correct destination address. If the destination address is correct, the packet is passed for further processing. If the destination address is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

The packet with correct destination address is then screened for a correct source address. If the source address is correct, the packet is passed to the receiver computer. If the source address is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

Then, the packet with a correct destination address and a correct source address is screened for a correct allowed port coordinate such as port number. If the port coordinate is correct, the packet is passed for further processing. If the port coordinate is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

Finally, the packet with a correct destination and source addresses and a correct port designator is screened for data integrity by application of authentication check such as a checksum. If the authentication check is passed, the packet is passed to the addressee computer. If the authentication check is failed, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

The security managing unit analyses all the alarms and makes decisions on necessary unscheduled changes of addresses for appropriate network servers. Also, it can notify law enforcement and pass appropriate data on to it.

Figure 7 illustrates an enhanced computer intrusion protection system indicated generally at 52 for one or more network computers 54. A gateway router or a bridge 58 includes a destination address filter 60 which receives data packets which pass in through a load distribution switch 62. A non-interrogatable network address book 64 stores current network server addresses for the destination address filter 60, and the destination address filter checks each data packet to determine if a legitimate destination address is present.

Packets with legitimate destination addresses are forwarded to a source address filter 66, while packets with illegitimate destination addresses are sent to a security analysis section 68 in a management unit 70.

When a preset traffic load level is reached indicating that an attempt at flooding is being made, the destination address filter causes the load distribution switch 62 to distribute traffic to one or more parallel gateway routers or bridges which collectively forward legitimate traffic and dump the flooding traffic. An alternative arrangement would call for the load distribution function to be done irrespective of the load, utilizing all the parallel

The packet with correct destination address is then screened for a correct source address. If the source address is correct, the packet is passed to the receiver computer. If the source address is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

Then, the packet with a correct destination address and a correct source address is screened for a correct allowed port coordinate such as port number. If the port coordinate is correct, the packet is passed for further processing. If the port coordinate is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

Finally, the packet with a correct destination and source addresses and a correct port designator is screened for data integrity by application of authentication check such as a checksum. If the authentication check is passed, the packet is passed to the addressee computer. If the authentication check is failed, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

The security managing unit analyses all the alarms and makes decisions on necessary unscheduled changes of addresses for appropriate network servers. Also, it can notify law enforcement and pass appropriate data on to it.

Figure 7 illustrates an enhanced computer intrusion protection system indicated generally at 52 for one or more network computers 54. A gateway router or a bridge 58 includes a destination address filter 60 which receives data packets which pass in through a load distribution switch 62. A non-interrogatable network address book 64 stores current network server addresses for the destination address filter 60, and the destination address filter checks each data packet to determine if a legitimate destination address is present.

Packets with legitimate destination addresses are forwarded to a source address filter 66, while packets with illegitimate destination addresses are sent to a security analysis section 68 in a management unit 70.

When a preset traffic load level is reached indicating that an attempt at flooding is being made, the destination address filter causes the load distribution switch 62 to distribute traffic to one or more parallel gateway routers or bridges which collectively forward legitimate traffic and dump the flooding traffic. An alternative arrangement would call for the load distribution function to be done irrespective of the load, utilizing all the parallel

gateways all the time. A source address table 74 stores accessible server's designators and corresponding current addresses for all system servers which may legitimately have access to the computer or computers 54. These addresses are accessed by the source address filter which determines whether or not an incoming data packet with the proper destination address originates from a source with a legitimate source address entered in the source address table 74. If the source address is determined to be legitimate, the data packet is passed to a port address filter 76. Data packets with an illegitimate source address are directed to the security analysis section 68. Alternatively, source address screening can be done at the gateway router or bridge 58 first prior to port filter 76.

A port protection table 78 includes the current port assignments for the computer or computers 54, and these port assignments are accessed by the port designator filter 76 which then determines if an incoming data packet contains legitimate port designation. If it does, it is passed to an actual address translator 80 which forwards the data packet to the specific computer or computers 54 which are to receive the packet. If an illegitimate port address is found by the port address filter 76, the data packet is transmitted to the security analysis section 68.

The management unit 70 is under the control of a security administrator 82. A network membership master file 84 stores a master list of legitimate server's designators along with respective authorized access lists and corresponding current cyber coordinates. The security administrator can update the master list by adding or removing authorized access for every protected computer. An access authorization unit 86 distributes the upgraded relevant portions of the master lists to the address books of the respective authorized servers.

A random character generator 88 generates random characters for use in forming current port designators, and provides these characters to a port designator forming block 90. This port designator forming block forms the next set of network current port designators in conjunction with the master list and these are incorporated for transmission by a port table block 92. Alternatively, port designators can be formed in the computer unit instead of the management unit.

Similarly, a random character generator 94 generates random characters for use in forming current server addresses, and provides these characters to a server address forming

block 96. This server address forming block forms the next set of current network server addresses, and an address table 98 assigns addresses to servers designated on the master list.

A coordinator/dispatcher block 100 coordinates scheduled move of network servers to their next current addresses, provides the next set of network addresses for appropriate servers and routers and coordinates unscheduled changes of addresses on command from the security analysis unit 68. The coordinator/dispatcher block 100 may be connected to an encode/decode block 102 which decodes received address book upgrades from input 104 and encodes new port and server destination addresses to be sent to authorized servers in the system over output 106. Where encoding of new cyber coordinates is used, each authorized computer in the network will have a similar encoding/decoding unit.

The security analysis unit 68 analyses received illegitimate data packets and detects attack attempts. If needed, the security analysis unit orders the coordinator/dispatcher block 100 to provide an unscheduled address change and diverts the attack data packets to an investigation unit 108. This investigation unit simulates the target server keeping a dialog alive with the attacker to permit security personnel to engage and follow the progress of the attacker while tracing the origin of the attack.

Providing security against intrusion for e-commerce systems presents a unique problem, for an important peculiarity of an e-commerce system is that its address must be publicly known. This aspect represents a contradiction to the requirement of the address being known to authorized parties only. However, the only information intended for the general public usually relates to a company catalog and similar material. The rest of the information on a merchant's network is usually considered private and thus should be protected. Using this distinction, a merchant's e-commerce site should be split into two parts: public and private. The public part is set up on a public "catalog" server with a fixed IP address and should contain only information intended for the general public. The rest of the corporate information should be placed in a separate network and protected as described in relation to Figures 1-7.

When a customer has completed shopping and made purchasing decisions concerning the terms and price of the sale, pertinent for the transaction, information is placed in a separate register. This register is periodically swept by a server handling financial transactions ("financial" server), which belongs to the protected corporate network. In fact,

the "catalog" server does not know the current address of the financial transactions server. Thus, even if an intruder penetrates the "catalog" server, the damage is limited to the contents of the catalog and the intruder cannot get an entry to the protected corporate network.

The financial server, having received pending transaction data, contacts the customer, offering a short-term temporary access for finalizing the transaction. In other words, the customer is allowed access just long enough to communicate pertinent financial data such as a credit card number and to receive a transaction confirmation at which point the session is terminated, the customer is diverted back to the catalog server and the financial server is moved to a new cyber address thus making obtained knowledge of its location during the transaction obsolete.

Dial-up communications systems, in respect to their infrastructure channels susceptibility to transmission intercept by unrelated parties, can be separated into two broad categories: easily interceptable, such as cellular and satellite telephone systems and relatively protected such as conventional land-line based telephone systems. Relatively protected systems such as conventional land-line based telephone systems can be protected in the following way. Phone numbers, assigned by a telephone company to a dial-up telephone-based private network serve as the members' computer addresses. As described previously, such a private network can be protected from unauthorized remote access by implementing periodic changes in the addresses, i.e. telephone numbers assigned to the members for transmission by the network along with other designators such as access codes and communicating the changed numbers to the appropriate parties.

For the conventional land-line dial-up telephone systems, while the "last mile" connection remains constant, the assigned telephone number is periodically changed, making the corresponding computer a moving target for a potential attacker. In this case the telephone company serves as the security system manager. It assigns the current variable telephone numbers to the members of a protected, private network, performs notification of all the appropriate parties, and changes the members' current numbers to a new set at an appropriate time. The telephone company switches naturally serve in the role of routers, and thus they can be programmed to perform surveillance of the system, to detect potential intrusion attacks and to issue appropriate alarms.

Periodically changing the current assigned numbers creates system entropy for a potential intruder, making unauthorized access difficult. Obviously, the implementation of this security system is dependent on availability of sufficient vacant numbers at a particular facility of the telephone company. Furthermore, for a variety of practical reasons it is advisable to keep a just vacated number unassigned for a certain period of time. All this may require additional number capacity at the telephone company facility in order to enable it to provide remote access security to a larger number of personal networks while preserving a comfortable level of system entropy.

If the mentioned additional capacity is not available, or a still higher level of entropy is desired, it could be artificially increased by adding an access code to the assigned number. This would amount to adding virtual capacity to the system, and would make a combination of the phone number and access code an equivalent of a computer's telephone address. In effect, this would make a dialed number larger than the conventional format. This method makes a virtual number capacity practically unlimited and, since the process is handled by computers without human involvement, it should not put any additional burden on a user. With or without a virtual number capacity, utilization of this method allows the intrusion attempts to be easily identified by their wrong number and/or code. At the same time, implementation of this system might require some changes in dialing protocols as well as additional capabilities of the telephone switching equipment.

Entropy density can be increased by limiting the number of allowable connection attempts. Similarly to the method described previously, telephone company switching equipment can be made to perform a role of an outside security barrier for the private network. In this case wrongly addressed connection attempts should be analyzed in order to detect possible "sweeping". If such an attempt is detected, tracing the origin of the attempt and notifying the appropriate phone company should not present a problem even with the existing technology.

The simplest form of private network protection under the proposed method and system is when at a predetermined time all the members of a particular network are switched to the new "telephone book" of the network. However, in some cases required level of security for some members of the same private network could substantially differ, or they may face different levels of security risk. In such cases frequency of the phone number

change could be set individually with appropriate notification of the other members of the network. This differentiation enables the telephone company to offer differentiated levels of security protection to its customers even within the same private network.

A telephone company can also offer its customers protected voice private networks which would provide a higher level of privacy protection than the presently used "unlisted numbers." In this configuration the customers' telephone sets are equipped with a computerized dialing device with remotely upgradeable memory which would allow each member of a protected voice network to contain the network "telephone book" and that book is periodically updated by the telephone company.

The telephone company would periodically change the assigned telephone numbers of a protected network to a new set of current numbers. These new numbers would be communicated to the members of a protected voice network through updating their computerized dialing devices.

As a derivative of the described system, an updateable electronic telephone directory system can be also implemented. In this case a customer's phone set would include a computerized dialing device with electronic memory containing a conventional telephone directory and a personal directory as well. This telephone directory can be periodically updated on-line by the telephone company.

Easily interceptable systems such as cellular and satellite telephone systems, in addition to the protection described above, can be protected from "cloning" when their signals can be intercepted and the "identity" of the phone can be cloned for gaining unauthorized access and use of the system by unauthorized parties.

Mobile telephone and mobile communications systems are protected in a manner similar to networks or land based telephone systems. In this instance, the novel and improved method of changing cyber coordinates is designed to reliably protect mobile phone systems from unauthorized use commonly known as cloning as well as to make intercept of wireless communications more difficult than it is at present. With this system the static wireless phone number or other similar identifier is not used for identification and authorization. Instead, a set of private identifiers is generated known only to the phone company and base stations controlling mobile phone calls and used to continually update the mobile phone and base station directories with current valid identifiers. This approach provides vastly superior

protection over current methods requiring that each call be intercepted in order to track and keep current with changing identifiers. Immediate detection of unauthorized attempts to use a cloned phone is realized and law enforcement may be notified in near real time for appropriate action.

Other electronic devices using wireless communications can be protected by the methods and systems described above.

Finally, computers often contain databases with a variety of information. That information in a database often has wide-ranging levels of sensitivity or commercial value. This creates a situation when large computers serve multiple users with vastly different levels of access. Furthermore, even within the same level of access, security considerations require compartmentalization of information when each user has to have access to only a small portion of the database.

The existing systems try to solve this situation by utilizing passwords and internal firewalls. As it was mentioned earlier, password-based systems and firewalls are not sufficient against computerized attacks. In practical terms it means that a legitimate user with a low level of access, utilizing hacking techniques from his station, potentially can break into even the most restricted areas of the database.

This problem can be solved by using the method of the present invention. A piece of information such as a file or a directory in a computer exists in cyber space. Accordingly, it has its cyber address, usually expressed as a directory and/or a file name which defines its position in a particular computer file system. This, in effect, represents the cyber coordinates of that piece of information within a computer.

As described earlier, information security can be provided if a system manager periodically changes the directories and/or file names in the system, i.e. the cyber addresses of the information, and notifies only appropriate parties of the current file names. This method would ensure that each user computer knows locations of only files to which it has legitimate access. Furthermore, a user would not even know of existence of the files to which he has no access.

To further strengthen the system and make it user-friendly, the user would have a personal directory similar to an address book, where only permanent directory and/or file names are accessible to him, while the variable side of the "address book" would be

accessible only to the system manager and upgraded periodically. In this arrangement variable directory and/or file names can contain any required level of entropy, further increasing resistance to attacks from within the system. Additionally, an internal "router" or "filter" can also perform information security monitoring functions, detect intrusion attempts and issue appropriate alarms in real time.

Obviously, in order to ensure information security in such arrangement any computer-wide search by keywords or subject should be disabled and substituted with a search within specific clients' "address books".

The systems and methods described above allow for creation of a feasible infrastructure protection system such as a national or international infrastructure protection system. When detected at specific points cyber attacks are referred to such a system for further analysis and a possible action by law enforcement authorities.

I claim:

1. A method for protecting a communications device which is connected to a communications system against an unauthorized intrusion which includes:

providing the communications device with at least one identifier,

providing the at least one identifier for use in accessing the communications device to entities authorized to access said communications device,

sensing the presence or absence of said identifier before granting access to said communications device,

providing access to said communications device when the use of said at least one correct identifier is sensed

denying access to said communications device and providing said communications device with at least one new identifier when the absence of the correct at least one identifier is sensed during an attempt to access said communications device, and providing said at least one new identifier to entities authorized to access said communications device.

2. The method of claim 1 which includes periodically changing the at least one identifier and providing the changed at least one identifier to the entities authorized to access said communications device.

3. The method of claim 1 which includes providing said communications device with a plurality of separate identifiers,

sensing the presence or absence of all of said plurality of identifiers before granting access to said communications device,

providing access to said communications device when the use of all of said identifiers is sensed, and

denying access to said communications device and providing said communications device with a new plurality of identifiers to replace the previous plurality of identifiers when the absence of any one of the correct identifiers is sensed.

4. The method of claim 3 which includes periodically changing said plurality of

separate identifiers and providing the changed identifiers to the entities authorized to access said communications device.

5. The method of claim 1 which includes permitting a predetermined number of attempts to access said communications device with a correct at least one identifier after the absence of the correct at least one identifier is sensed before providing said communications device with at least one new identifier,

and providing access to said communications device if the correct at least one identifier is sensed during the predetermined number of attempts to access.

6. The method of claim 2 wherein said communications system is a telephone system and said communications device is a telephone.

7. The method of claim 1 wherein said communications system is a computer network with said entities authorized to access said communications device being authorized computers having access to said computer network, said communications device including at least one host computer having access to said computer network.

8. The method of claim 7 which includes periodically changing the at least one identifier for the host computer and providing the changed at least one identifier to the authorized computers.

9. The method of claim 7 which includes providing the authorized computers with an unchangeable, accessible address for the host computer which is used by the authorized computer to activate and transmit the at least one identifier for the host computer when the authorized computer initiates access to the host computer.

10. The method of claim 8 which includes providing each authorized computer with an authorized computer identifier,

providing the host computer with a destination identifier,

causing each authorized computer to access said host computer with at least a host

computer destination identifier and the authorized computer identifier,

sensing the presence or absence of both said host computer destination identifier and an authorized computer identifier before granting access to said host computer,

providing access to said host computer when the use of both a correct host computer destination identifier and an authorized computer identifier is sensed, and

denying access to said host computer and providing said host computer with a new host computer destination identifier when the absence of either a correct host computer destination identifier or a correct authorized computer identifier is sensed.

11. The method of claim 10 which includes permitting a predetermined number of attempts to access said host computer with both a correct host computer destination identifier and an authorized computer identifier after the absence of a correct host computer destination identifier or an authorized computer identifier is sensed before providing said host computer with a new host computer destination identifier, and

providing access to said host computer if correct host computer destination and authorized computer identifier are sensed during the predetermined number of attempts to access the host computer.

12. The method of claim 11 which includes storing said host computer destination identifier as an inaccessible identifier in said authorized computers, and providing said authorized computers with an unchangeable, accessible host computer address, which will activate and transmit the host computer destination identifier when an authorized computer initiates access to the host computer.

13. The method of claim 8 which includes providing said host computer with a host computer destination identifier and a host computer port identifier,

causing each authorized computer to access said host computer with at least the host computer destination identifier and the host computer port identifier,

sensing the presence or absence of both said host computer destination identifier and said host computer port identifier before granting access to said host computer,

providing access to said host computer when the use of both a correct host computer

destination identifier and a correct host computer port identifier are sensed, and

denying access to said host computer and providing said host computer with a new destination identifier and port identifier when the absence of either or both of a correct host computer destination or port identifier is sensed.

14. The method of claim 13 which includes permitting a predetermined number of attempts to access said host computer with both a correct host computer destination and port identifier when either or both an incorrect host computer destination or port identifier is sensed before providing said host computer with a new destination and port identifier, and

providing access to said host computer if both correct host computer destination and port identifiers are sensed during the predetermined number of attempts to access said host computer.

15. The method of claim 14 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computers and providing said authorized computers with an unchangeable, accessible host computer address which will activate and transmit the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

16. An intrusion protection method for protecting a host computer connected to a computer communications system which includes one or more authorized computers having access to said computer communications system which are authorized to access said host computer which includes:

providing each authorized computer with an authorized computer identifying address,

providing said host computer with a host computer destination identifier and a host computer port identifier,

providing said host computer destination identifier and said host computer port identifier to said authorized computers,

causing each authorized computer to access said host computer with the host computer destination and port identifiers and said authorized computer identifying address,

sensing the presence or absence of said host computer destination and port identifiers

and said authorized computer identifying address before granting access to said host computer,

providing access to said host computer when the use of correct computer destination and port identifiers and a correct authorized computer identifying address is sensed, and

denying immediate access to said host computer when the absence of any one or more of the correct host computer destination and port identifiers or the authorized computer identifying address is sensed.

17. The method of claim 16 which includes periodically changing the host computer destination and port identifiers and providing these changes to the authorized computers.

18. The method of claim 17 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and transmit the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

19. The method of claim 16 which includes changing the host computer destination and port identifiers when access is denied to said host computer after at least one access attempt has been made and providing these changed identifiers to the authorized computers.

20. The method of claim 16 which includes permitting a predetermined number of attempts to access said host computer with correct host computer destination and port identifiers and a correct authorized computer identifying address after the absence of at least a correct one of said identifiers and authorized computer identifying address is sensed by the host computer and

providing access to said host computer if correct host computer destination and port identifiers and a correct authorized computer identifying address are sensed during the predetermined number of attempts to access said host computer.

21. The method of claim 19 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and cause transmission of the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

22. The method of claim 20 which includes changing the host computer destination and port identifiers when access is denied to said host computer after at least one access attempt has been made and providing these changed identifiers to the authorized computers.

23. The method of claim 22 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and cause transmission of the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

24. A method of communication with a remote entity over a communication system which includes

providing the remote entity with at least one remote entity cyber coordinate identifier,

providing the remote entity cyber coordinate identifier to one or more base entities authorized to communicate with said remote entity,

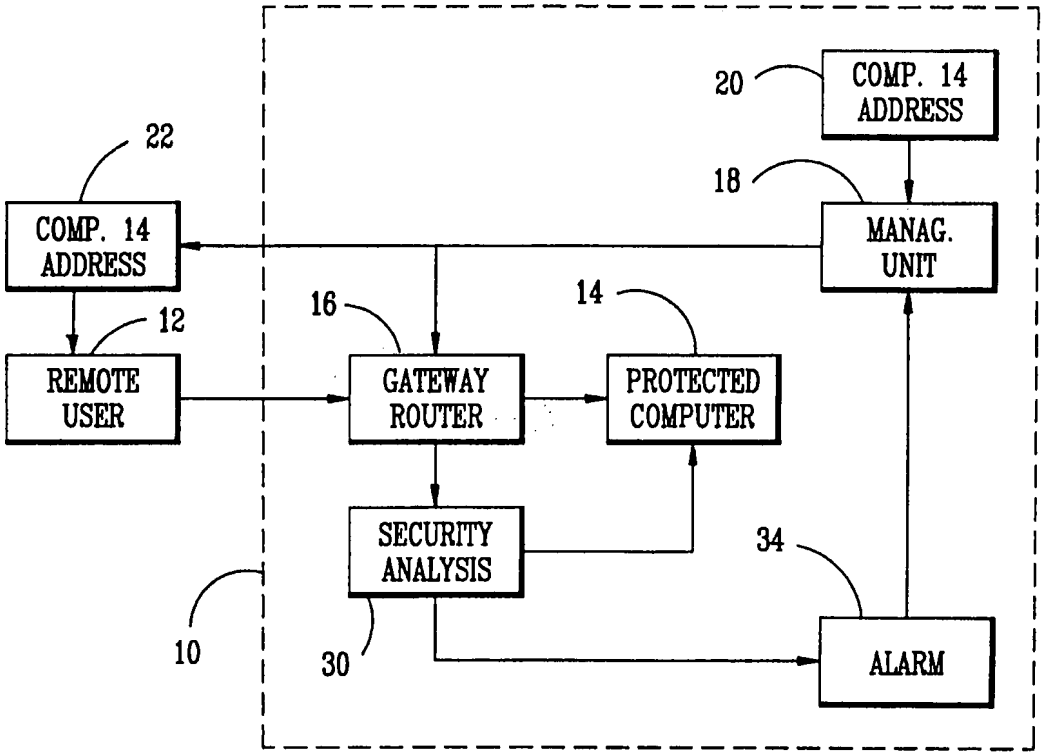
periodically changing the remote entity cyber coordinate identifier to a new remote entity cyber coordinate identifier and

providing the new remote entity cyber coordinate identifier to said one or more base entities.

25. The method of claim 24 which includes changing the remote entity cyber coordinate identifier to a new cyber coordinate identifier in response to an attempt to communicate with said remote entity with an incorrect remote entity cyber coordinate identifier and

providing the new remote entity cyber coordinate identifier to said one or more base entities.

FIG. 1



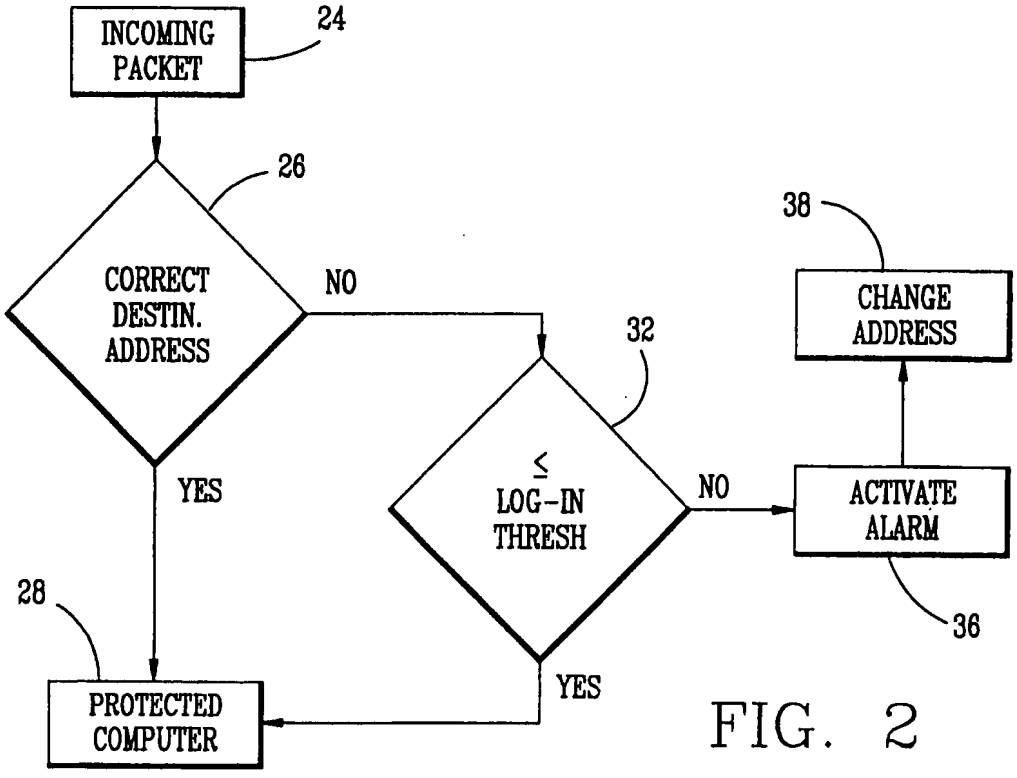


FIG. 2

Petitioner Apple Inc. - Exhibit 1026, p. 316

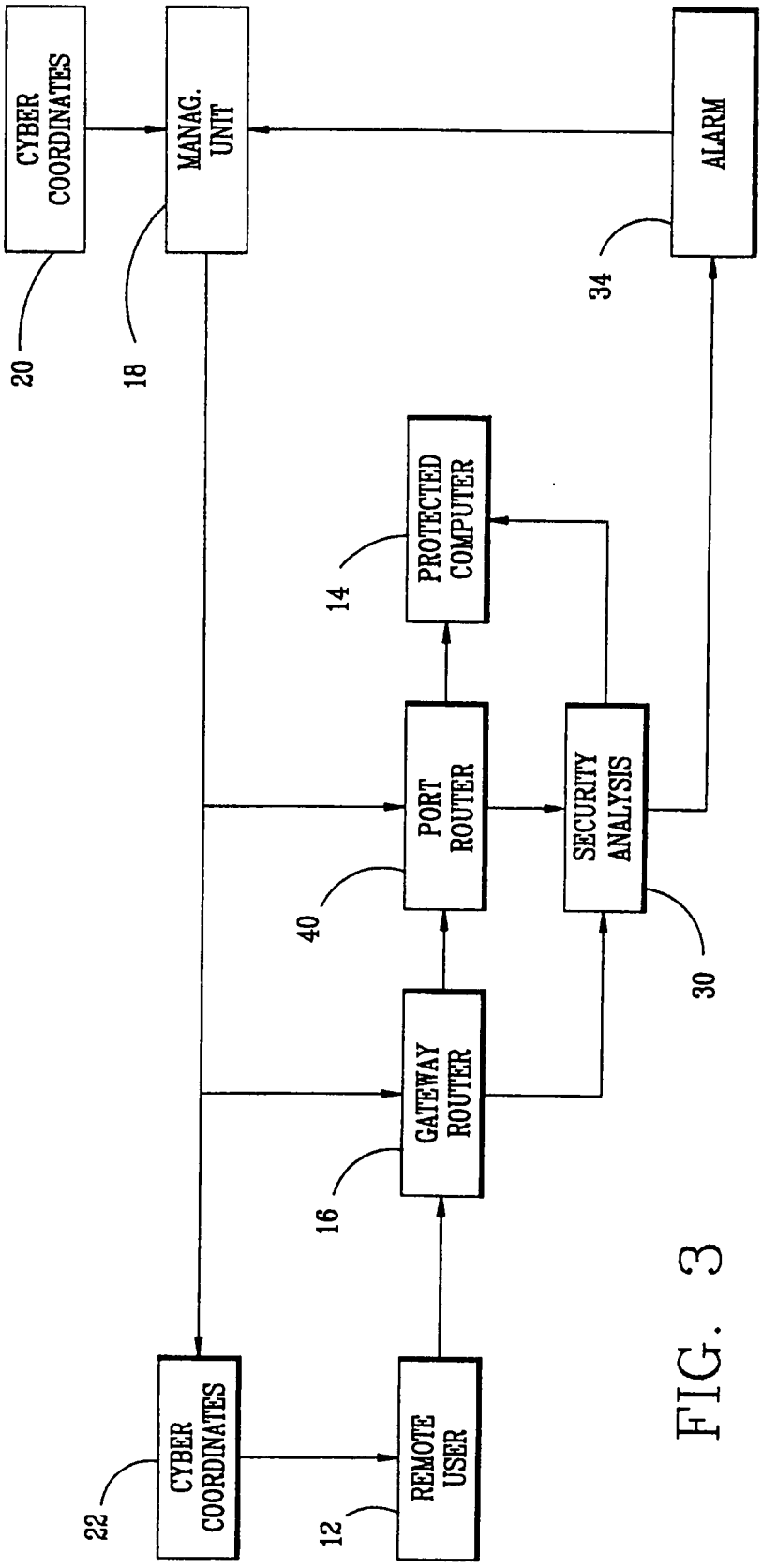


FIG. 3

Petitioner Apple Inc. - Exhibit 1026, p. 317

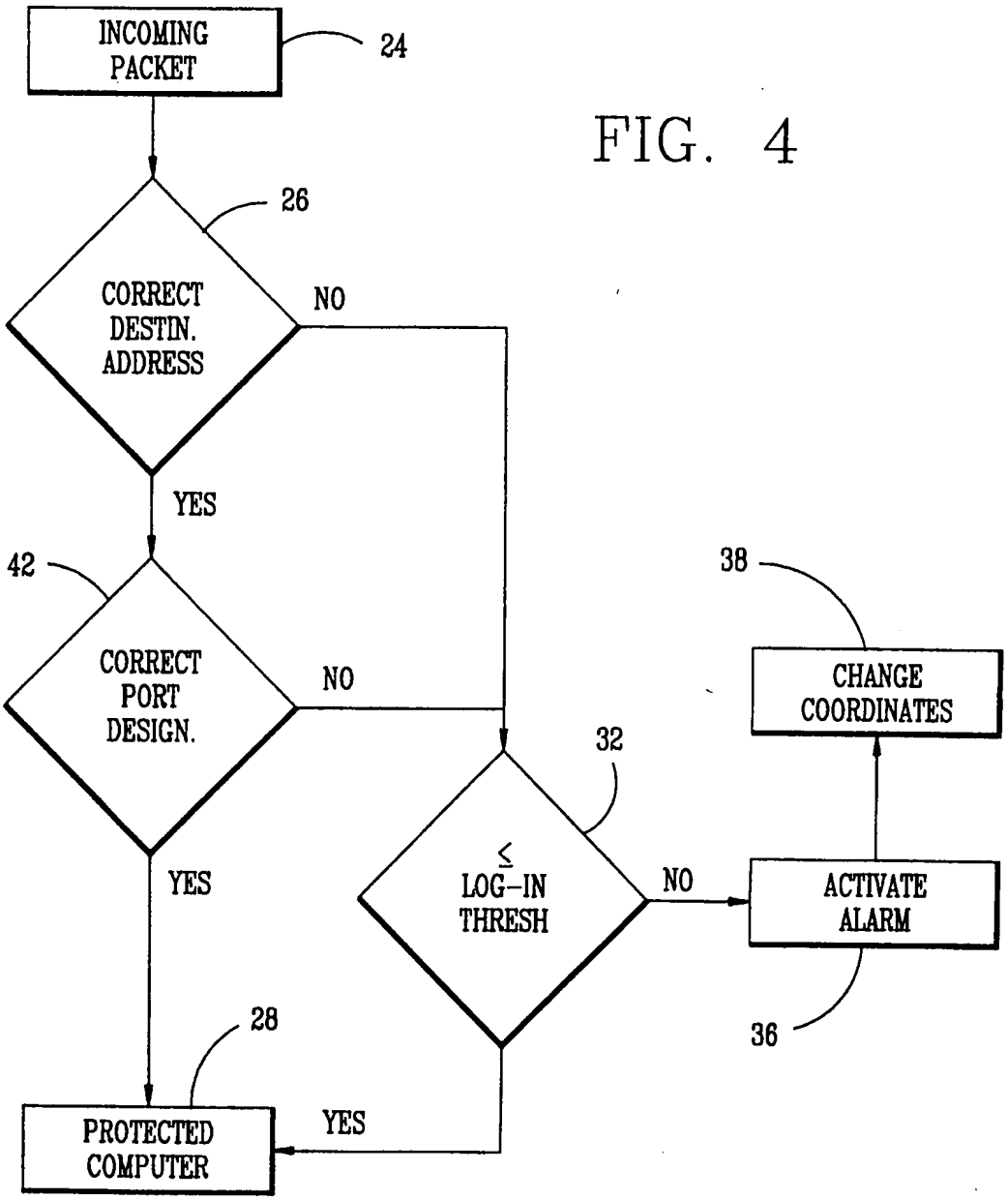


FIG. 4

Petitioner Apple Inc. - Exhibit 1026, p. 318

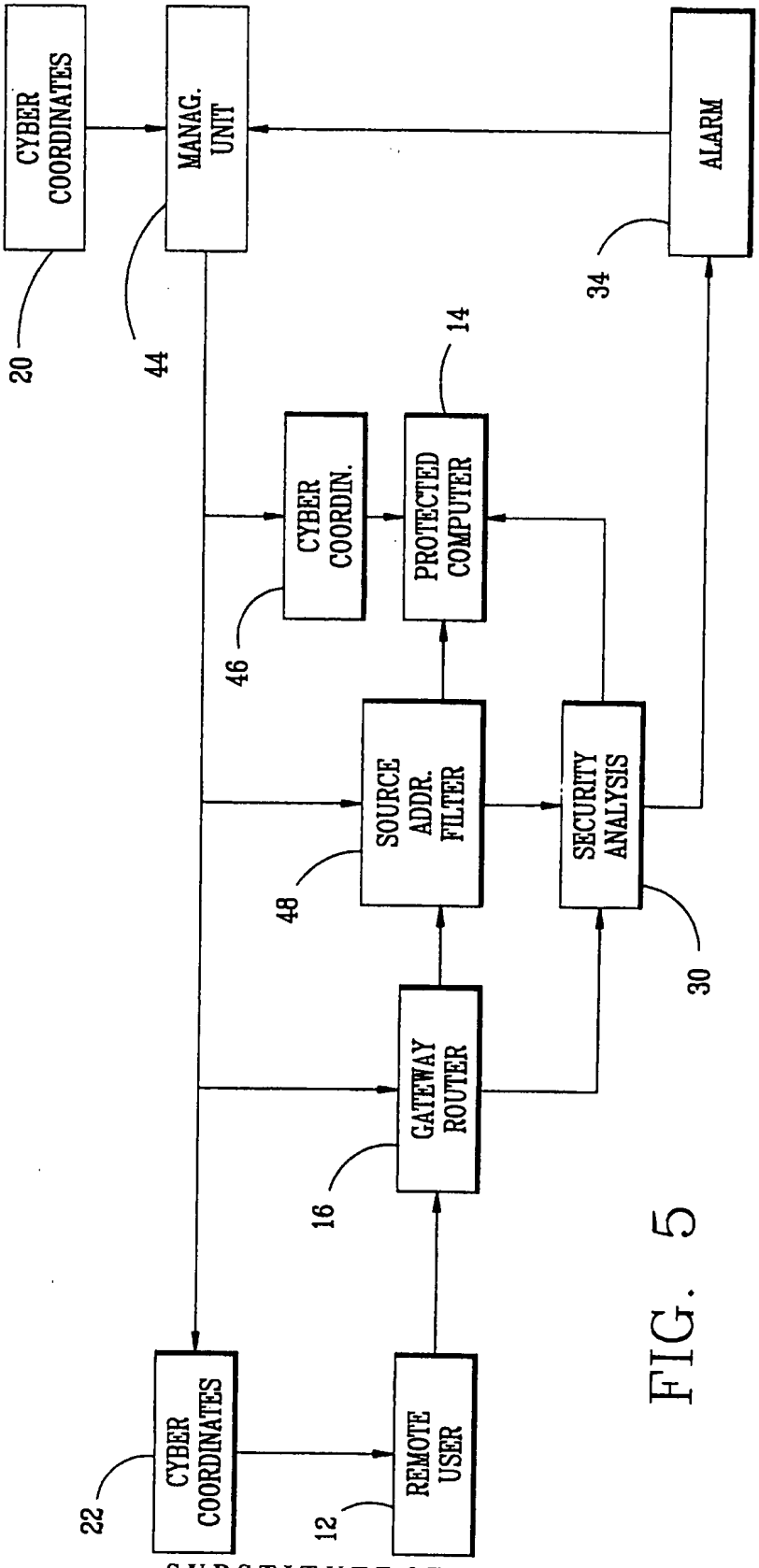


FIG. 5

Petitioner Apple Inc. - Exhibit 1026, p. 319

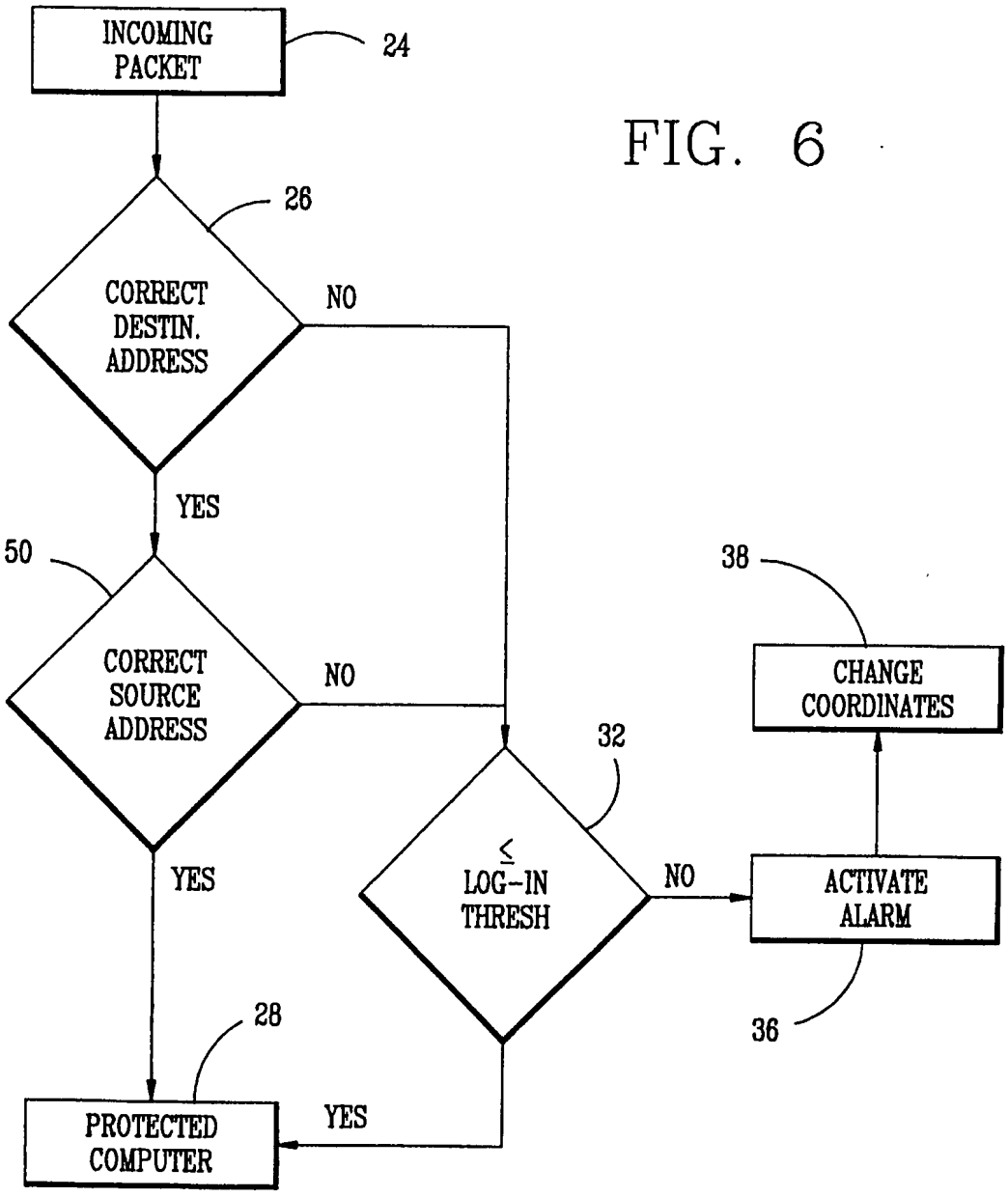
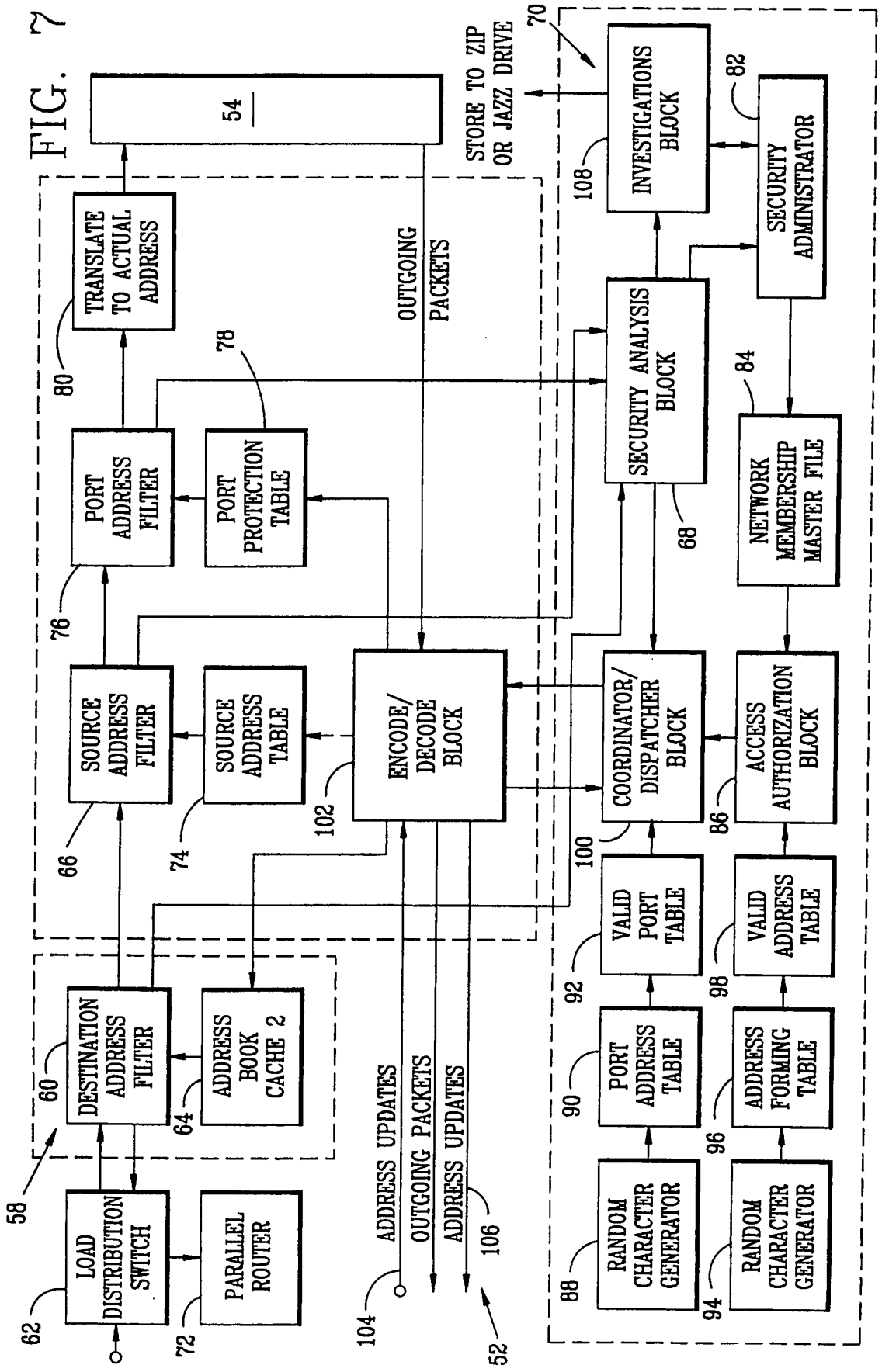


FIG. 6

Petitioner Apple Inc. - Exhibit 1026, p. 320

FIG. 7



Petitioner Apple Inc. - Exhibit 1026, p. 321

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08219

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 11/00
US CL : 713/201
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/201,200,202; 340/825.31,825.34; 380/255;

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS US PATENT FILE; WEST; JPAB; EPAB; DWPI; TDBD;

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,805,801 A (HOLLOWAY ET AL) 08 SEPTEMBER 1998, Entire document.	1-25
Y	US 5,796,942 A (ESBENSEN) 18 AUGUST 1998, Entire document.	1-25
Y,P	US 5,905,859 A (HOLLOWAY ET AL) 18 MAY 1999, Entire document.	1-25
Y	US 5,892,903 A (KLAUS) 06 APRIL 1999, Entire document.	1-25
A	US 5,537,099 A (LIANG) 16 JULY 1996, Entire document.	1-25
A	US 5,278,901 A (SHIEH ET AL) 11 JANUARY 1994, Entire document.	1-25

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
20 JULY 2000	22 AUG 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer NADEEM IQBAL Telephone No. (703) 308-5228

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08219

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,991,881 A (CONKLIN ET AL) 23 NOVEMBER 1999, Entire document.	1-25

Form PCT/ISA/210 (continuation of second sheet) (July 1998)*

B14

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 11/04, H04L 12/22

A1

(11) International Publication Number: **WO 98/27783**

(43) International Publication Date: 25 June 1998 (25.06.98)

(21) International Application Number: PCT/IB97/01563

(22) International Filing Date: 12 December 1997 (12.12.97)

(30) Priority Data:
08/769,649 19 December 1996 (19.12.96) US

(71) Applicant *(for all designated States except US)*: NORTHERN TELECOM LIMITED [CA/CA]; World Trade Center of Montreal, 8th floor, 380 St. Antoine Street West, Montreal, Quebec H2Y 3Y4 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: TELLO, Antonio, G. [US/US]; 114 Fountain Hills Drive, Garland, TX 75044 (US). HUI, Margaret [US/US]; 9920 Forest Lane #208, Dallas, TX 75243 (US). HOLMES, Kim [US/US]; 5409 Scenic Drive, Rowlett, TX 75088 (US).

(74) Agents: MCCOMBS, David et al.; Haynes and Boone, L.L.P., Suite 3100, 901 Main Street, Dallas, TX 75202-3789 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: VIRTUAL PRIVATE NETWORK SERVICE PROVIDER FOR ASYNCHRONOUS TRANSFER MODE NETWORK

(57) Abstract

A virtual private network service provider is used to transfer data over a data network to a final destination, with third-party billing. The method comprises the steps of: prompting the user at a data terminal to select a destination, password, and call type; sending a set-up message to the data network; selecting a virtual private network provider through the data network; the virtual private network provider giving an encryption key to the user, and then prompting the user for a password and a user identification; encrypting the password, and sending the user identification and the encrypted password to the virtual private network provider; the virtual private network provider decrypting the encrypted password, and verifying the password; the virtual private network provider providing an authorization code; and the data terminal transferring the data through the data network to the final destination, using the authorization code.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

VIRTUAL PRIVATE NETWORK SERVICE PROVIDER FOR ASYNCHRONOUS TRANSFER MODE NETWORK

Technical Field

The invention relates generally to asynchronous transfer mode ("ATM") networks and virtual private networks ("VPN"), such as those offered by MCI and Sprint, and, more particularly, to a method of using a VPN to transfer data over a data network, with third-party billing.

Background of the Invention

Telephone service providers offer third-party billing. For example, local and long distance telephone companies offer calling cards for third party billing.

VPNs exist to provide the sense of a private network among a company's locations. The lines/trunks of a VPN are actually shared among several companies, to reduce costs, yet to each company the VPN appears to be that company's own private network. However, a user at a remote data terminal, such as a portable computer in a hotel room, can not immediately charge his company for the access time to a data net, such as the Internet. Instead, his access time is charged to his hotel room, and so he must pay the inflated rates that hotels charge for phone service.

What is needed is a VPN service provider that offers remote access for users belonging to a VPN, user authorizations to prevent delinquent access into the VPN, and convenient third-party billing.

Summary of the Invention

The present invention, accordingly, provides a system and method for using a VPN service provider to transfer data over a data network to a final destination, with third-party billing. The method comprises the steps of: prompting the user at a data terminal to select a destination, password, and call type; selecting a VPN through the data network; giving an encryption key to the user, and then prompting the user for a password and a user identification; verifying the password, and providing an authorization code to

CONFIRMATION COPY

Petitioner Apple Inc. - Exhibit 1026, p. 326

the user; and allowing the user to transfer the data through the data network to the final destination, using the authorization code.

In another feature of the invention, the method further comprises negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

In another feature of the invention, the method further comprises encrypting the user's password, and sending the user identification and the encrypted password to the VPN service provider.

In another feature of the invention, the method further comprises a step of sending a set-up message to the data network.

In another feature of the invention, the method further comprises a step of the VPN service provider decrypting the encrypted password.

A technical advantage achieved with the invention is that it shifts or defers costs from an end user to a bulk purchaser of data network services. Another technical advantage achieved with the invention is that it permits end users mobility while attaining a virtual appearance on a corporate intranet.

Brief Description of the Drawings

Fig. 1 is a system block diagram of a VPN service provider of the present invention.

Fig. 2 is a flow chart depicting the method of the present invention, as implemented by application software on a user terminal.

Fig. 3 is the initial screen display of the user interface of the application software.

Figs. 4A and 4B are call flow diagrams, illustrating the preferred sequence of steps of the method of the present invention.

Figs. 5A, 5B, 5C, 5D, 5E, and 5F comprise a flow chart depicting the method of the present invention, as implemented by switching control point software.

Petitioner Apple Inc. - Exhibit 1026, p. 327

Description of the Preferred Embodiment

In Fig. 1, the VPN service provider system of the present invention is designated generally by a reference numeral 10. The VPN service provider system 10 includes a VPN 12. The VPN 12 may be a corporate, government, association, or other organization's telephone/data line `network. The VPN service provider system 10 also includes access lines 13 from the VPN 12 to a data network 14, such as the Internet, or an ATM network. The VPN service provider system 10 also includes access lines 16 from the data network 14 to a long distance phone company 18, such as AT&T, MCI, or Sprint. The VPN service provider system 10 also includes access lines 20 from the data network 14 to a called party 22, such as, for example, American Express reservations service. The VPN service provider system 10 also includes access lines 24 from the data network 14 to a remote user terminal 26, such as a portable computer in a hotel room. The user terminal 26 includes user application software 28, which provides the interface for the user to enter the number to be called, the user identification number, and the user's authorization code. The VPN service provider system 10 also includes VPN service provider software 30, located in a switching control point (SCP) device 32, which, in the preferred embodiment may be physically located anywhere. The SCP 32 connects to the data network 14 via access lines 36. One possible physical location for the SCP 32 is on the premises of a local phone company central switch building 34. However, even when located within the building 34, the SCP 32 connects to the local phone company switches via the data network 14. The local phone company switches connect to the data network 14 via access lines 38.

In an alternate embodiment, the VPN service provider software 30 and the SCP device 32 may be located on the premises of an independent provider of local phone service, or on the premises of an independent VPN service provider.

Petitioner Apple Inc. - Exhibit 1026, p. 328

Referring now to Fig. 2, the application software 28 begins the data transfer process in step 50. In step 52, the user is presented with a screen display.

Referring now to Fig. 3, a screen display 100 displays the following information requests: whether the call is a direct call 102 or a VPN call 104, the number the user desires to call 106, the VPN user ID 108, and the user password 110. The user is also presented with the option to make the call 112, or to quit 114.

Referring back to Fig. 2, in step 54 the user terminal sends to the SCP 32 the information captured through the graphical user interface ("GUI") in step 52 within a user network interface ("UNI") setup message. In step 56 the user terminal 26 waits for a connect message from the SCP 32. In step 58 the user terminal 26 determines if a connection was made. If no connection was made, then in step 60 the user application software 28 displays an error message to the user, and returns to step 50 to begin again the data transfer process.

If a connection was made, then in step 62 the user terminal 26 sends the VPN user ID to the SCP 32. In step 64 the user terminal 26 waits for an encryption key from the SCP 32. In step 66, having received the encryption key from the SCP 32, the user application software 28 encrypts the user's password, and sends it to the SCP 32. In step 68 the user terminal 26 waits for authentication of the user. In step 70 the user application software 28 determines if the SCP 32 authorizes the user to make the call.

If the user is not authorized, then in step 72 the user terminal 26 displays an error message, terminates the connection, blanks the screen display 100, and returns to step 50 to begin again the data transfer process. If the user is authorized, then in step 74 the VPN service provider software 30 sets up the billing, and authorizes it. In step 76 the user terminal 26 sends a "release", meaning to terminate or disconnect the connection, to the SCP 32. In step 78 the user terminal 26 sends a setup message to the number listed by

Petitioner Apple Inc. - Exhibit 1026, p. 329

the user as the "number to call", that is, to the final destination. In step 80 the user terminal 26 waits for a connection. In step 82 the user terminal 26 determines if a connection was made.

If a connection to the final destination was not made, then the user application software 28 returns to step 72, in which step the user terminal 26 displays an error message, terminates the connection, blanks the screen display 100, and returns to step 50 to begin again the data transfer process. If a connection to the final destination was made, then in step 84 the user terminal 26 exchanges user data, services, and/or value added or user specific applications with the computer at the address, that is, the telephone number, of the final destination. In step 86 the user selects the option presented to him to release, or terminate, the call. In step 88 the user terminal 26 sends a release message to the final destination. In step 90 the data network 14 sends billing information to the SCP 32. In step 92 the application software 28 ends the data transfer process.

Fig. 4A and Fig. 4B are call flow diagrams, showing the sequence of messages in the method of the preferred embodiment. These diagrams present the same method as the flow chart of Fig. 2. The horizontal arrows represent the messages sent and received. The vertical lines represent the various devices involved in sending and receiving the messages. For example, the top left arrow in Fig. 4A represents a message sent from the user terminal 26, labeled "Macintosh" in Fig.4A, to an interface with a public network. The user terminal 26 can be any brand of a work station computer, a desktop computer, a laptop computer, or even a notebook computer. The interface could be any interface, but in the example of Fig. 4A and Fig. 4B, the interface is imagined to be at a hotel, where a business traveler is using the method of the present invention. Thus, the interface is labeled "Hotel ATM Interface", which is not shown in Fig. 1. The vertical line labeled "Public ATM Network" is the same as the data network 14 in Fig. 1. The vertical line labeled "Moe's VPN Service" represents the VPN service provider software 30

Petitioner Apple Inc. - Exhibit 1026, p. 330

within the SCP 32. The vertical line labeled "Travel ATM Interface" is not shown in Fig. 1, but is located between the called party 22 and the data network 14. The vertical line labeled "Travel Service" is one example of the called party 22 shown in Fig. 1. In the example of Fig. 4A and Fig. 4B, the business traveler is imagined to be using the method of the present invention to contact a travel service to make reservations for his next airline flight. In Figs. 4A and 4B the designation "Ack" represents "acknowledge", and the designation "Cmp" represents "complete".

Referring now to Fig. 5, the VPN service provider software 30 begins the data transfer process in step 300 by waiting for an event. The event it waits for is a setup message on a signaling port of the SCP 32, to be received from the user terminal 26. In step 302, having monitored the signaling ports, and the SCP 32 having received a setup message, the VPN service provider software 30 assigns a call condense block ("CCB") to the setup message, based on a call reference number. The CCB is a software data structure for tracking resources associated with the call. The call reference number is a number, internal to the SCP, for tracking calls. In step 304 the VPN service provider software 30 compiles the connect message. In step 306 the VPN service provider software 30 sends a connect message to the calling address, that is, the hotel room from which the user is calling. In step 308 the VPN service provider software 30 condenses, that is, it remains in a wait state for that call.

Referring now to Fig. 5B, in step 310 the VPN service provider software 30 waits for an event by monitoring the signaling ports of the SCP 32. After the SCP 32 receives a connect acknowledge message from the user terminal 26, then in step 312 the VPN service provider software 30 accesses the CCB, based on the call reference number. In step 314 the VPN service provider software 30 condenses.

Referring now to Fig. 5C, in step 316 the VPN service provider software 30 waits for dialog on a data port of the SCP 32. After the SCP 32 receives a

Petitioner Apple Inc. - Exhibit 1026, p. 331

VPN ID on a data port, the VPN service provider software 30 verifies the VPN ID in step 318. In step 320 the VPN service provider software 30 determines if the VPN ID is valid. If the VPN ID is not valid, then in step 322 the SCP 32 sends a reject message over an assigned switch virtual circuit ("SVC"). The SVC is a channel over the data network 14. In step 324 the VPN service provider software 30 waits for dialog. In step 326, because the VPN ID is valid, the VPN service provider software 30 assigns an encryption key to the user terminal 26, in step 328 sends the encryption key over the assigned SVC to the user terminal 26, and in step 330 waits for dialog.

Referring now to Fig. 5D, in step 332 the VPN service provider software 30 waits for dialog. When the SCP 32 receives the encrypted password from the user terminal 26 at a data port, then in step 334 the VPN service provider software 30 verifies the password, and determines in step 336 if the password is valid. If the password is not valid, then in step 338 the SCP 32 sends a reject message over the assigned SVC to the user terminal, and in step 340 waits for dialog. If the password is valid, then in step 342 the VPN service provider software 30 assigns an authorization token to the user terminal 26, in step 344 sends the token over an assigned SVC to the user terminal 26, and in step 346 waits for dialog.

Referring now to Fig. 5E, in step 348 the VPN service provider software 30 waits for an event. When the VPN service provider software 30 senses that the SCP 32 has received on a signaling port a release message from the user terminal 26, then in step 350 the VPN service provider software 30 accesses the CCB, based on the call reference number of the user terminal 26, in step 352 compiles a release complete message, in step 354 sends a release complete message to the user terminal 26, and in step 356 condenses.

Referring now to Fig. 5F, in step 358 the VPN service provider software 30 waits for an event. When the VPN service provider software 30 senses that the SCP 32 has received on a signaling port a third-party billing setup message from the user terminal 26, then in step 360 the VPN service provider

Petitioner Apple Inc. - Exhibit 1026, p. 332

software 30 verifies the token just received from the user terminal 26, to determine, in step 362, if it is the same token that the VPN service provider software 30 sent to the user terminal 26 in step 344. If the token is not valid, then in step 364 the SCP 32 sends a release message to the terminal 26, and in step 366 condenses. If the token is valid, then in step 368 the SCP 32 sends a modified third-party billing setup message to the data network 14, and in step 370 condenses.

Although an illustrative embodiment of the invention has been shown and described, other modifications, changes, and substitutions are intended in the foregoing disclosure. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.

Petitioner Apple Inc. - Exhibit 1026, p. 333

WHAT IS CLAIMED IS:

1. A computerized method of a virtual private network service provider with third party billing, using a virtual private network to transfer data over a data network to a final destination, the method comprising the steps of:

a. prompting the user at a data terminal to select a destination, password, and call type;

b. selecting a virtual private network through the data network;

c. giving an encryption key to the user, and then prompting the user for a password and a user identification;

d. verifying the password, and providing an authorization code to the user; and

e. allowing the user to transfer the data through the data network to the final destination, using the authorization code.

2. The method of claim 1, wherein step (d) further comprises negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

3. The method of claim 2, wherein step (c) further comprises encrypting the user's password, and sending the user identification and the encrypted password to the virtual private network service provider.

4. The method of claim 3, further comprising, after step (a), the step of sending a set-up message to the data network.

5. The method of claim 4, further comprising, after step (c), the step of the virtual private network service provider decrypting the encrypted password.

6. An apparatus for providing a datalink connection from a user terminal to a data network and to a virtual private network, with third party billing, comprising:

a. an interface between the user terminal and the data network;

Petitioner Apple Inc. - Exhibit 1026, p. 334

b. a switching control point device connected to the data network, the switching control point device connected to a computer; and

c. a computer-readable medium encoded with a method of using the virtual private network and the data network, with third party billing, the computer-readable medium accessible by the computer.

7. The apparatus of claim 6, wherein the method comprises negotiating for more bandwidth for the user, and including within an authorization code a grant of additional bandwidth.

8. The apparatus of claim 7, wherein the method further comprises encrypting a user's password, and temporarily storing the user identification and the encrypted password.

9. The apparatus of claim 8, wherein the method further comprises sending a set-up message to the data network.

10. The apparatus of claim 9, wherein the method further comprises decrypting the encrypted password.

11. A computer-readable medium encoded with a method of using a virtual private network, with third party billing, the method comprising the steps of:

a. prompting the user at a data terminal to select a destination, password, and call type;

b. selecting a virtual private network through the data network;

c. giving an encryption key to the user, and then prompting the user for a password and a user identification;

d. verifying the password, and providing an authorization code to the user; and

e. allowing the user to transfer the data through the data network to the final destination, using the authorization code.

Petitioner Apple Inc. - Exhibit 1026, p. 335

12. The computer-readable medium of claim 11 wherein step (d) further comprises negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

13. The computer-readable medium of claim 12 wherein step (c) further comprises encrypting the user's password, and sending the user identification and the encrypted password to the virtual private network service provider.

14. The computer-readable medium of claim 13 further comprising, after step (a), the step of sending a set-up message to the data network.

15. The computer-readable medium of claim 14 further comprising, after step (c), the step of the virtual private network service provider decrypting the encrypted password.

16. An apparatus for providing a datalink connection from a user terminal to a data network and to a virtual private network, with third party billing, comprising:

a. means for prompting a user at the data terminal to select a destination, password, and call type;

b. means for selecting the virtual private network through the data network;

c. means for giving an encryption key to the user, and then prompting the user for a password and a user identification;

d. means for verifying the password, and providing an authorization code to the user; and

e. means for allowing the user to transfer data through the data network to a final destination, using the authorization code.

17. The apparatus of claim 16, further comprising means for negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

Petitioner Apple Inc. - Exhibit 1026, p. 336

18. The apparatus of claim 17, further comprising means for encrypting the user's password, and sending the user identification and the encrypted password to the virtual private network service provider.

19. The apparatus of claim 18, further comprising means for sending a set-up message to the data network.

20. The apparatus of claim 19, further comprising means for decrypting the encrypted password.

Petitioner Apple Inc. - Exhibit 1026, p. 337

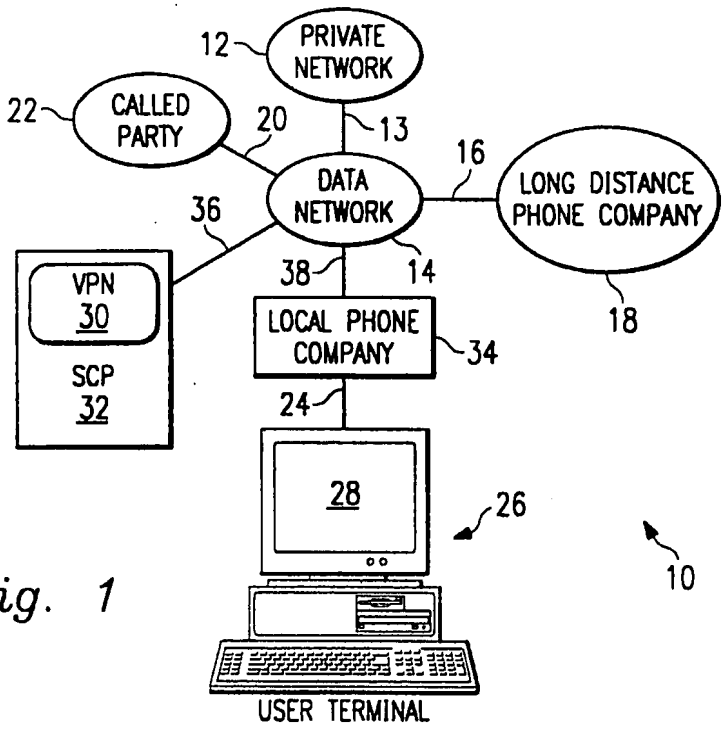

12
PRIVATE NETWORK
22
CALLED PARTY
20
13
16
DATA NETWORK
LONG DISTANCE PHONE COMPANY
36
38
14
18
VPN
30
SCP
32
LOCAL PHONE COMPANY
34
24
28
26
10
USER TERMINAL

Fig. 1

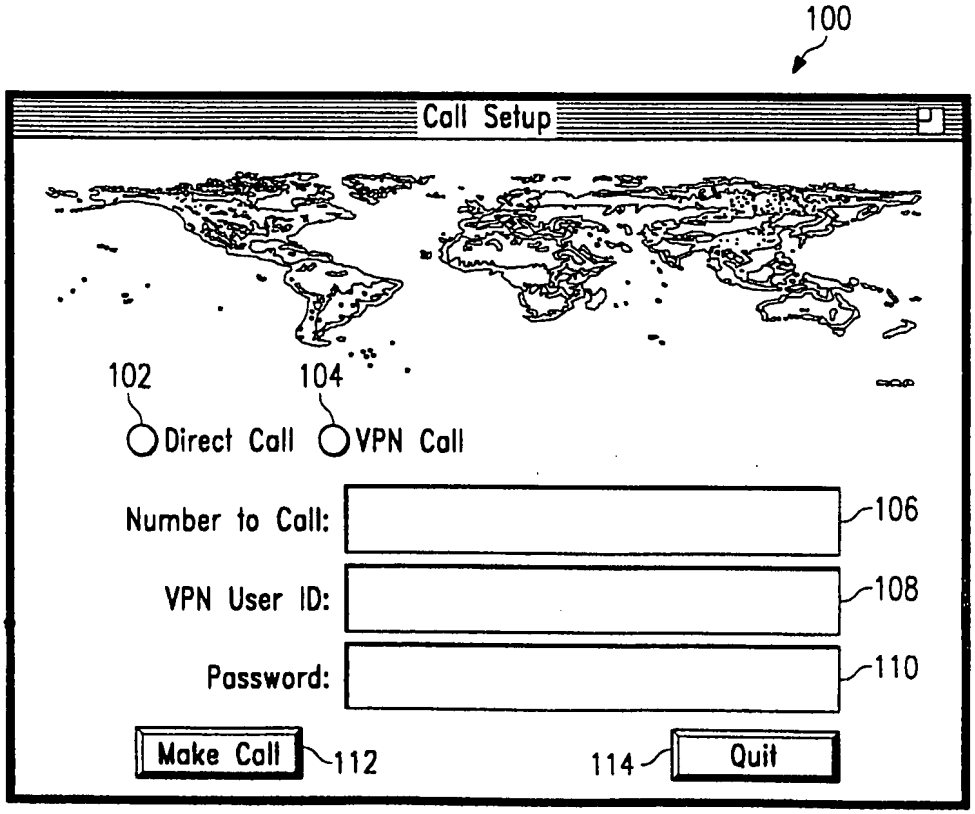

100
Call Setup
102
104
Direct Call
VPN Call
Number to Call:
106
VPN User ID:
108
Password:
110
Make Call
112
114
Quit

Fig. 3

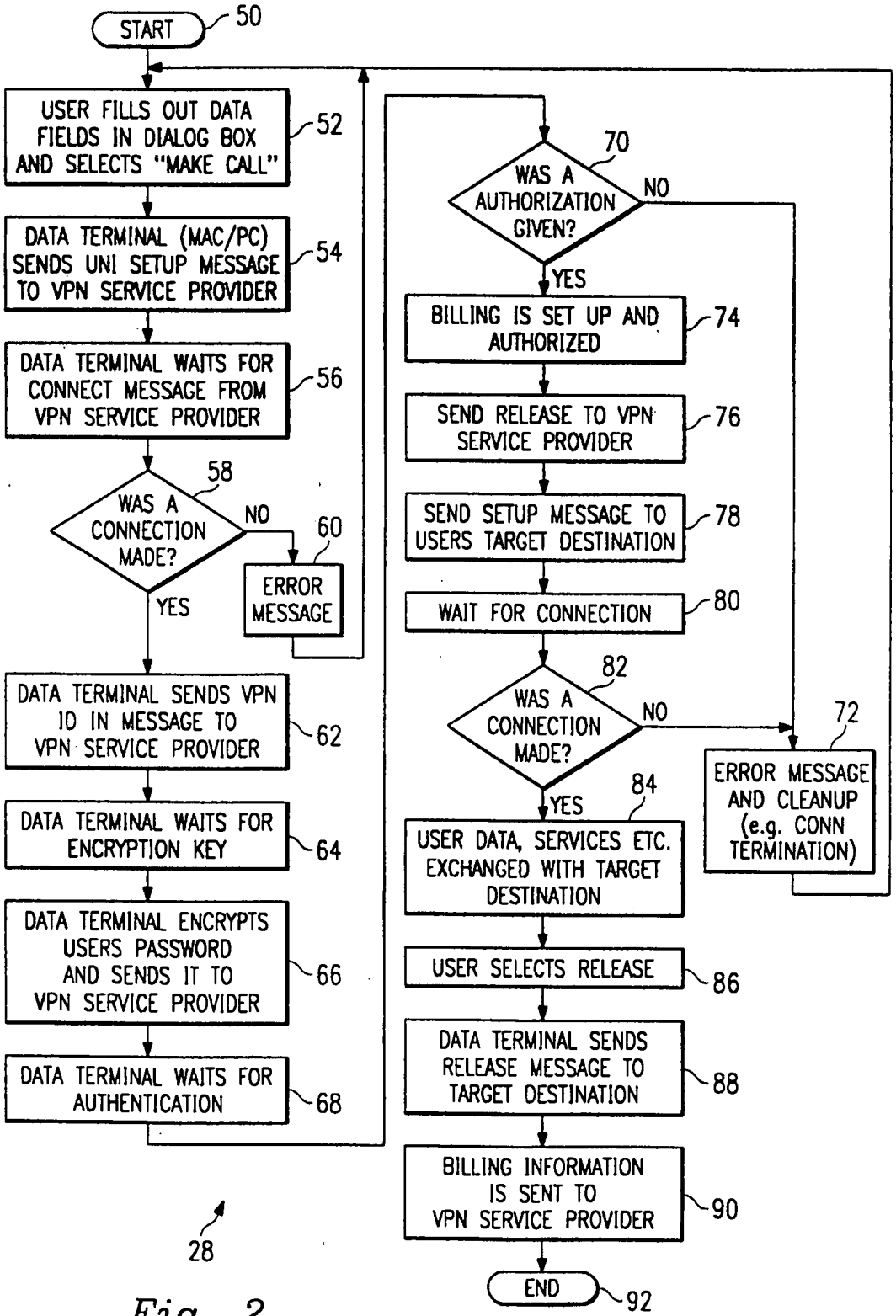

START
50
USER FILLS OUT DATA FIELDS IN DIALOG BOX AND SELECTS "MAKE CALL"
52
DATA TERMINAL (MAC/PC) SENDS UNI SETUP MESSAGE TO VPN SERVICE PROVIDER
54
DATA TERMINAL WAITS FOR CONNECT MESSAGE FROM VPN SERVICE PROVIDER
56
WAS A CONNECTION MADE?
58
NO
60
ERROR MESSAGE
YES
DATA TERMINAL SENDS VPN ID IN MESSAGE TO VPN SERVICE PROVIDER
62
DATA TERMINAL WAITS FOR ENCRYPTION KEY
64
DATA TERMINAL ENCRYPTS USERS PASSWORD AND SENDS IT TO VPN SERVICE PROVIDER
66
DATA TERMINAL WAITS FOR AUTHENTICATION
68
28
WAS A AUTHORIZATION GIVEN?
70
NO
YES
BILLING IS SET UP AND AUTHORIZED
74
SEND RELEASE TO VPN SERVICE PROVIDER
76
SEND SETUP MESSAGE TO USERS TARGET DESTINATION
78
WAIT FOR CONNECTION
80
WAS A CONNECTION MADE?
82
NO
72
ERROR MESSAGE AND CLEANUP (e.g. CONN TERMINATION)
YES
84
USER DATA, SERVICES ETC. EXCHANGED WITH TARGET DESTINATION
USER SELECTS RELEASE
86
DATA TERMINAL SENDS RELEASE MESSAGE TO TARGET DESTINATION
88
BILLING INFORMATION IS SENT TO VPN SERVICE PROVIDER
90
END
92

Fig. 2

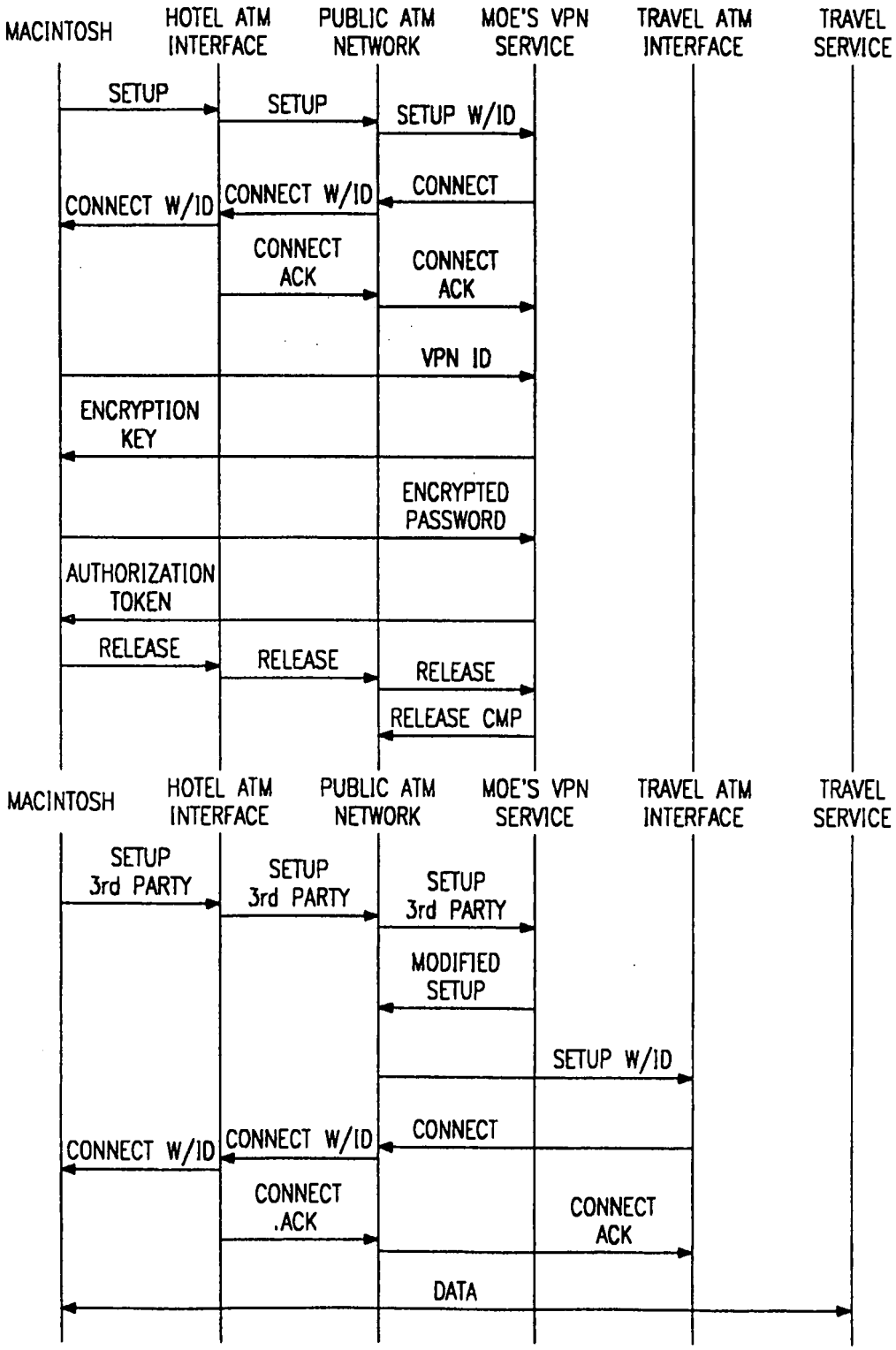

MACINTOSH
HOTEL ATM INTERFACE
PUBLIC ATM NETWORK
MOE'S VPN SERVICE
TRAVEL ATM INTERFACE
TRAVEL SERVICE
SETUP
SETUP
SETUP W/ID
CONNECT W/ID
CONNECT W/ID
CONNECT
CONNECT ACK
CONNECT ACK
VPN ID
ENCRYPTION KEY
ENCRYPTED PASSWORD
AUTHORIZATION TOKEN
RELEASE
RELEASE
RELEASE
RELEASE CMP
MACINTOSH
HOTEL ATM INTERFACE
PUBLIC ATM NETWORK
MOE'S VPN SERVICE
TRAVEL ATM INTERFACE
TRAVEL SERVICE
SETUP 3rd PARTY
SETUP 3rd PARTY
SETUP 3rd PARTY
MODIFIED SETUP
SETUP W/ID
CONNECT W/ID
CONNECT W/ID
CONNECT
CONNECT .ACK
CONNECT ACK
DATA

Fig. 4A

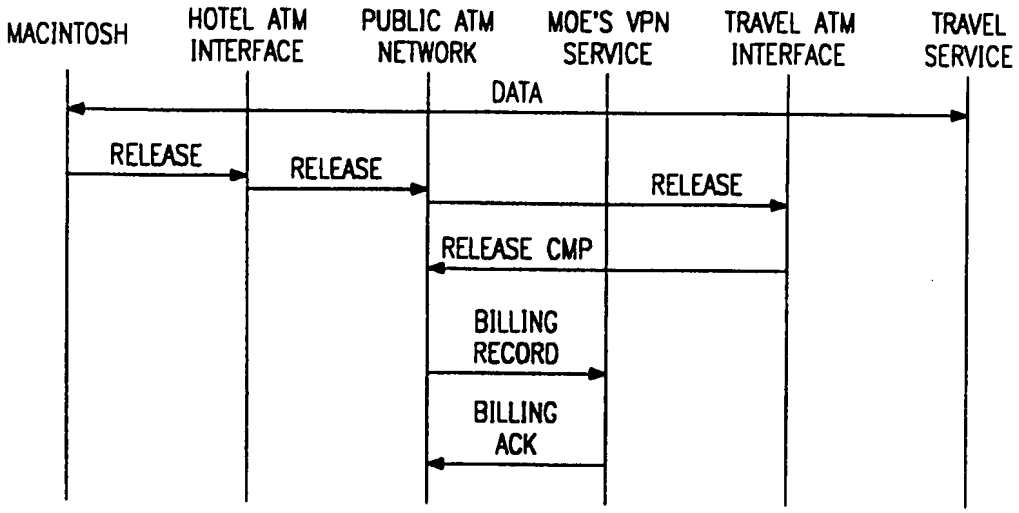


Fig. 4B

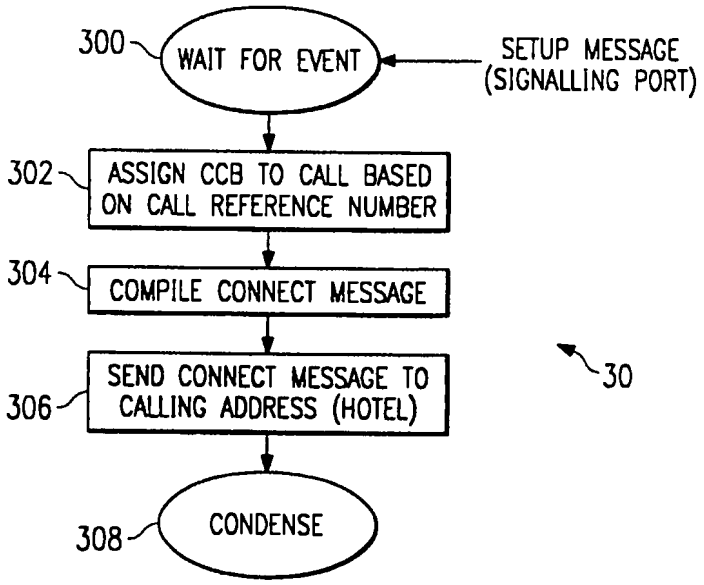


Fig. 5A

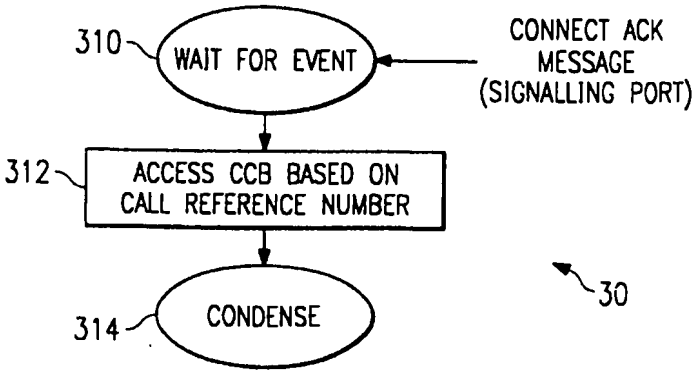


Fig. 5B

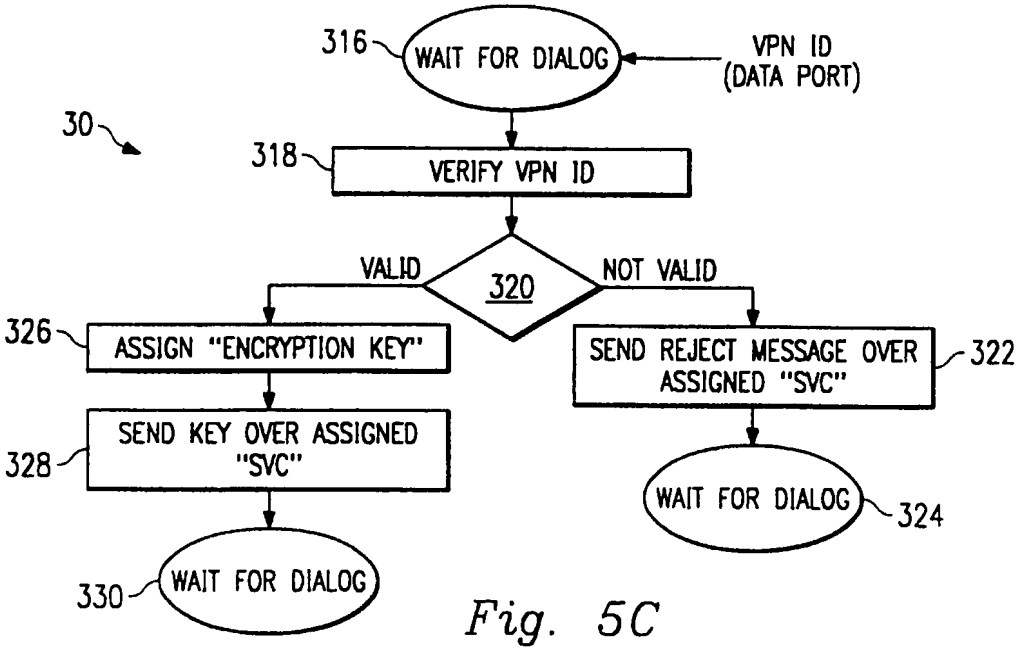

316
WAIT FOR DIALOG
VPN ID
(DATA PORT)
30
318
VERIFY VPN ID
VALID
320
NOT VALID
326
ASSIGN "ENCRYPTION KEY"
SEND REJECT MESSAGE OVER
ASSIGNED "SVC"
322
328
SEND KEY OVER ASSIGNED
"SVC"
WAIT FOR DIALOG
324
330
WAIT FOR DIALOG

Fig. 5C

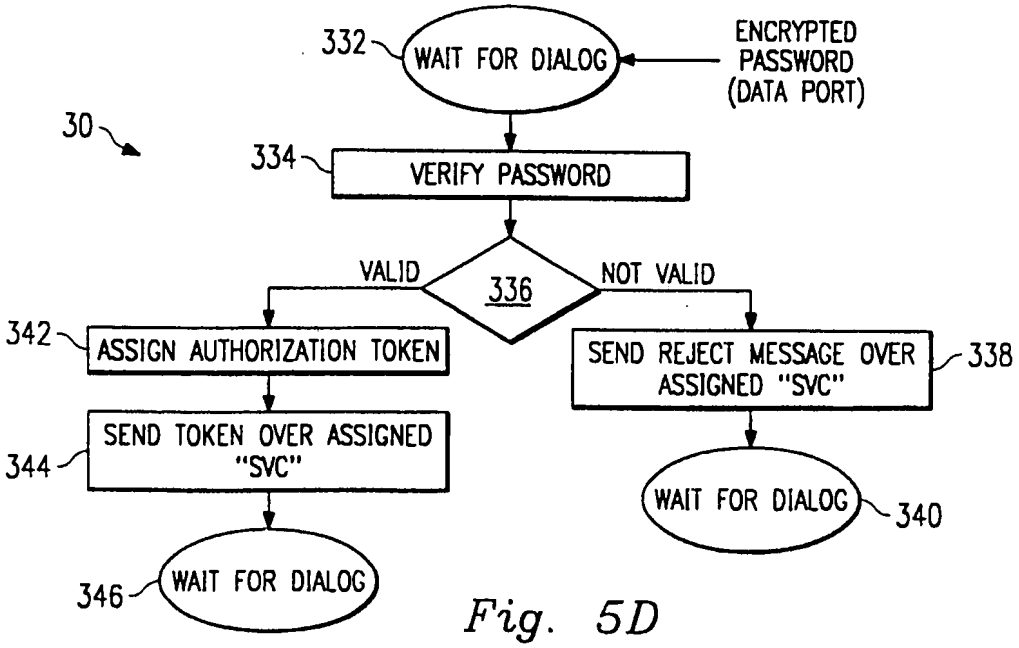

332
WAIT FOR DIALOG
ENCRYPTED
PASSWORD
(DATA PORT)
30
334
VERIFY PASSWORD
VALID
336
NOT VALID
342
ASSIGN AUTHORIZATION TOKEN
SEND REJECT MESSAGE OVER
ASSIGNED "SVC"
338
344
SEND TOKEN OVER ASSIGNED
"SVC"
WAIT FOR DIALOG
340
346
WAIT FOR DIALOG

Fig. 5D

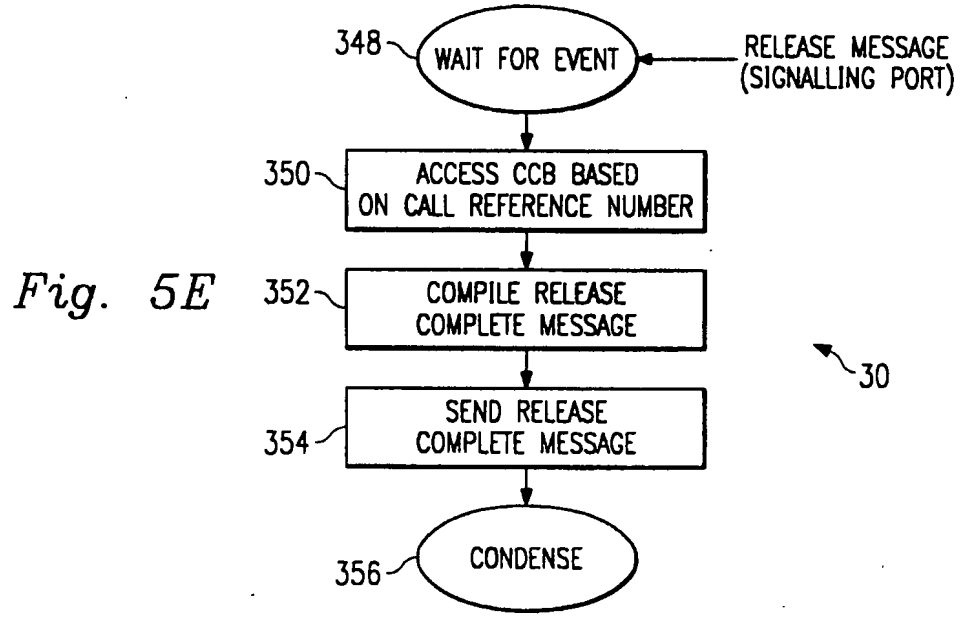

348
WAIT FOR EVENT
RELEASE MESSAGE (SIGNALLING PORT)
350
ACCESS CCB BASED ON CALL REFERENCE NUMBER
352
COMPILE RELEASE COMPLETE MESSAGE
30
354
SEND RELEASE COMPLETE MESSAGE
356
CONDENSE

Fig. 5E

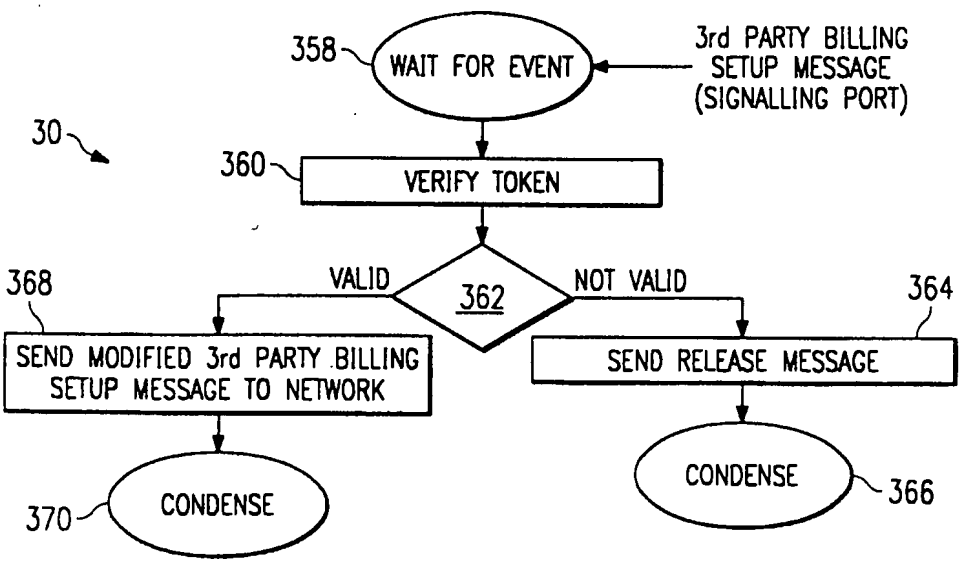

358
WAIT FOR EVENT
3rd PARTY BILLING SETUP MESSAGE (SIGNALLING PORT)
30
360
VERIFY TOKEN
368
VALID
362
NOT VALID
364
SEND MODIFIED 3rd PARTY BILLING SETUP MESSAGE TO NETWORK
SEND RELEASE MESSAGE
CONDENSE
366
370
CONDENSE

Fig. 5F

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/IB 97/01563

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q11/04 H04L12/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MUN CHOON CHAN ET AL: "AN ARCHITECTURE FOR BROADBAND VIRTUAL NETWORKS UNDER CUSTOMER CONTROL" NOMS '96 IEEE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM , vol. 1, 15 April 1996, KYOTO, JP, pages 135-144, XP000641086 see abstract ---	1-20
A	BIC V: "VOICE PERIPHERALS IN THE INTELLIGENT NETWORK" TELECOMMUNICATIONS, vol. 28, no. 6, June 1994, page 29/30, 32, 34 XP000600293 see the whole document ---	1-20

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(a) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
19 March 1998	02/04/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Staessen, B

Form PCT/ISA/210 (second sheet) (July 1992)

Petitioner Apple Inc. - Exhibit 1026, p. 344

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/IB 97/01563

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 729 256 A (NEDERLAND PTT) 28 August 1996 see abstract figures of pages 136 and 140	1-20
A	CROCETTI P ET AL: "ATM VIRTUAL PRIVATE NETWORKS: ALTERNATIVES AND PERFORMANCES COMPARISONS" SUPERCOMM/ICC '94, 1 May 1994, NEW ORLEANS, US, pages 608-612, XP000438985 see abstract	1-20

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

Petitioner Apple Inc. - Exhibit 1026, p. 345

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/IB 97/01563

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0729256 A	28-08-96	NL 9500339 A	01-10-96

Form PCT/ISA/210 (patent family annex) (July 1992)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/679,416	02/27/2007	Victor Larson	077580-0015 (VBNK-1CP2DVC

CONFIRMATION NO. 3528

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA02109-1775

Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Publication No. US-2008-0005792-A1
Publication Date: 01/03/2008

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Pre-Grant Publication Division, 703-605-4283

PTO/SB/08a (11-08)
Approved for use through 12/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11679416
Filing Date	2007-02-27
First Named Inventor	Larson, et al.
Art Unit	
Examiner Name	
Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5384848		1995-01-00	Kikuchi	
	2	6223287		2001-04-00	Douglas, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/THK/	Date (YYYY-MM-DD)	2008-12-16
Name/Print	Toby H. Kusmer	Registration Number	26,418

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	4461180
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Erin Shea
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0015 (VBNK-1CP2DVC
Receipt Date:	16-DEC-2008
Filing Date:	27-FEB-2007
Time Stamp:	10:05:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	77580_015_US_IDS_Form__SB_08a.pdf	608044 062dd8c55fe8b4eb341402e0997b9e7e297490e5	no	4

Warnings:	
Information:	

Total Files Size (in bytes):	608044

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (11-08)
Approved for use through 12/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11679416
Filing Date	2007-02-27
First Named Inventor	Larson, et al.
Art Unit	
Examiner Name	
Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5303302		1994-04-12	Burrows	
	2	5629984		1997-05-13	McManis	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ARR/	Date (YYYY-MM-DD)	2009-01-22
Name/Print	Atabak R. Royaee	Registration Number	59037

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	4657554
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royaee/Erin Shea
Filer Authorized By:	Atabak R Royaee
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)
Receipt Date:	22-JAN-2009
Filing Date:	27-FEB-2007
Time Stamp:	15:01:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	77580_015_US_IDS_Form__SB_08a.pdf	607958 ab62da557108fd0b709c7a807b833946524 69d64	no	4

Warnings:	
Information:	

Total Files Size (in bytes):	607958

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/08a (11-08)
Approved for use through 12/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11679416
Filing Date	2007-02-27
First Named Inventor	Larson, et al.
Art Unit	
Examiner Name	
Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5771239		1998-06-23	Moroney, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

	1	FASBENDER, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ARR/	Date (YYYY-MM-DD)	2009-02-24
Name/Print	Atabak R. Royaee	Registration Number	59037

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	4847992
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royaee/Erin Shea
Filer Authorized By:	Atabak R Royaee
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)
Receipt Date:	24-FEB-2009
Filing Date:	27-FEB-2007
Time Stamp:	15:23:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	77580_015_US_IDS_Form__SB_08a.pdf	608127 3ccff882a98ab32668b882b575e57a9685b2c6a4	no	4

Warnings:	
Information:	

2	NPL Documents	VRNK_NPLREFERENCE.PDF	731920 7e1f64823a0ad0d6d42fb2b62ae80e8c05c3f713	no	5

Warnings:	
Information:	
Total Files Size (in bytes):	1340047

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

MAY 0 4 2009
PATENT & TRADEMARK OFFICE

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	11/679,416
Filing Date	February 27, 2007
First Named Inventor	Victor Larson
Art Unit	2157
Examiner Name	Not yet assigned
Docket Number	77580-015 (VRNK-1CP2DVCN)

Sheet 1 of 17

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1000	5,311,593	05/10/1994	Carmi	
	A1001	5,511,122	04/23/1996	Atkinson	
	A1003	5,805,803	09/08/1998	Birrell et al.	
	A1004	5,822,434	10/13/1998	Caronni et al.	
	A1005	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A1006	60/134,547	05/17/1999	Victor Sheymov	
	A1007	60/151,563	08/31/1999	Bryan Whittles	
	A1008	5,950,195	09/07/1999	Stockwell et al.	
	A1009	6,119,171	09/12/2000	Alkhatib	
	A1010	6,937,597	08/30/2005	Rosenberg et al.	
	A1011	7,072,964	07/04/2006	Whittle et al.	
	A1012	09/399,753	09/22/1998	Graig Miller et al.	
	A1013	6,079,020	06/20/2000	Liu	
	A1014	6,173,399	01/09/2001	Gilbrech	
	A1015	6,226,748	05/01/2001	Bots et al.	
	A1016	6,226,751	05/01/2001	Arrow et al.	
	A1017	6,701,437	03/02/2004	Hoke et al.	
	A1018	6,055,574	04/25/2000	Smorodinsky et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	B1000	WO 001/17775	03-30-2000	Science Applications International Corporation		Yes	No
	B1001	WO 00/70458	11-23-2000	Comsec Corporation			
	B1002	WO 01/016766	03-08-2001	Science Applications International Corporation			

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 366

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	2	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C998	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation,	
	C999	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1000	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1001	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) (RFC1101, DNS SRV)	
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1003	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	C1004	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	C1005	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	C1006	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	C1007	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	C1008	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	C1009	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	C1010	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	C1011	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	C1012	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 367

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	3	Of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1013	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1015	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	C1016	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista	
	C1017	Automative Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	C1018	Automative Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1020	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997).(Data Sheet, Aventail)	
	C1021	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	
	C1022	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail)	
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1024	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	C1025	Goldschlag, et al. "*Privacy on the Internet,*" Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 368

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	4	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1026	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	C1027	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	C1028	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	C1029	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server NewOpportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM).(Routing, Microsoft Prior Art VPN Technology)	
	C1030	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	C1031	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	C1032	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1034	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	C1035	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	C1036	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Defintion, ANX)	
	C1037	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	C1038	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 369

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	5	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1039	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	C1040	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1042	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1044	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	C1045	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	C1046	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (available at hap //www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue).(NT Beta, Microsoft Prior Art VPN Technology)	
	C1047	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	
	C1048	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	C1049	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	C1050	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 370

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	6	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1051	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	C1052	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET)	
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1055	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1058	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1060	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10) 9 **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1062	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 371

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	7	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1067	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	C1068	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1070	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, <draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	C1071	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs)	
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1073	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	C1074	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	C1075	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	C1076	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	
	C1077	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	C1078	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 372

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	8	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1079	Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	C1080	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	C1081	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1082	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	C1083	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	C1084	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	C1085	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	C1086	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	C1087	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	C1088	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	C1089	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	C1090	Assured Digital Products. (Assured Digital) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1091	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	C1092	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	C1093	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	C1094	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	C1095	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	C1096	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 373

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	9	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1097	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	C1098	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	C1099	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	C1100	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	C1101	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	C1102	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	C1103	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	C1104	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	C1105	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	C1106	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	C1107	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1108	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1109	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	C1110	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	
	C1111	Dan Sterne *et.al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	C1112	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 374

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	10	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1113	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	C1114	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	C1115	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	C1116	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	C1117	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide – Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-insuit.)	
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide – Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1119	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	C1123	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	C1124	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	C1125	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 375

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	11	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1126	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	C1127	Microsoft Corp., DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	C1128	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	C1129	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	C1130	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	C1131	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	C1132	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	C1133	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	
	C1134	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at*http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	C1135	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B:Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	C1136	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999)(Mastering Windows NT Server)	
	C1137	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	C1138	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	C1139	Kenneth Gregg, *et al.*, *Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	C1140	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 376

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	12	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1141	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1142	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/ deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1143	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	C1144	Microsoft Corp., Chapter 1 – Introduction to Windows NT Routing with Routing and Remote Access Service, *Available at* http://www.microsoft.com/technet/archive/winntas/proddocs/ rras40/rrasch01.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	C1145	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 – Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1146	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1147	F-Secure, *F-Secure NameSurfer* (May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	C1148	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)	
	C1149	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	C1150	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
EXAMINER		DATE CONSIDERED	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 377

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	13	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1151	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	C1152	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	C1153	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	C1154	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	C1155	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1156	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	C1157	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	C1158	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	C1159	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	C1160	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	C1161	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	C1162	F-Secure, F-Secure VPN+ for Windows NT 4.0 (1998) (from FSECURE 00000009) (FSecure VPN+)	
	C1163	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1164	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1165	IRE, Inc., *SafeNet / Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 378

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	14	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1166	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	C1167	IRE, Inc., About SafeNet / VPN Policy Manager (1999) (About Safenet VPN Policy Manager)	
	C1168	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1169	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* (July 22, 1996) (Gauntlet Functional Summary)	
	C1170	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	C1171	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	C1172	Todd W. Matehrs and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame* (Macmillan Technial Publishing 1999) (Windows NT Mathers)	
	C1173	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	C1174	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	C1175	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN) Overview)	
	C1176	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	C1177	WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1178	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1179	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1180	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 379

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	15	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1181	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	C1182	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1183	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	C1184	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0* (September 21, 1998)	
	C1185	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	C1186	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	C1187	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	C1188	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	C1189	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	C1190	*Virtual Private Network Demonstration* (March 21, 1998)	
	C1191	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	C1192	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	C1193	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	C1194	Information Assurance, *Science Fair Agenda* (2000)	
EXAMINER		DATE CONSIDERED	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 380

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	16	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1195	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	C1196	*IFE 3.1 Technology Dependencies* (2000)	
	C1197	*IFE 3.1 Topology* (February 9, 2000)	
	C1198	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* (January 10-11, 2000)	
	C1199	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	C1200	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	
	C1201	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1202	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	C1203	Network Associates Products – *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	C1204	Microsoft Corporation, Microsoft Proxy Server 2.0 (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	C1205	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	C1206	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	C1207	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	C1208	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 381

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	17	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1209	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	C1210	David G. Schaer, *MCSE Test Success: Proxy Server 2* (1998) (Schaer, Microsoft Prior Art VPN Technology)	
	C1211	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	C1212	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1213	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1214	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	C1215	*AutoSOCKS v2.1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	C1216	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html	
	C1217	FirstVPN Enterprise Networks, Overview	
	C1218	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	C1219	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	C1220	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	C1221	Virtual Private Networks – Assured Digital Incorporated – ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	C1222	Accessware – The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	C1223	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	C1224	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/socks wp.html	
	C1225	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	C1226	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

BST99 1618785-1.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 382

OIPE
MAY 0 4 2009
PATENT & TRADEMARK OFFICE

5-5-09

IDS

COPY

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	11/679,416
Filing Date	February 27, 2007
First Named Inventor	Victor Larson
Art Unit	2157
Examiner Name	Not yet assigned
Docket Number	77580-015 (VRNK-1CP2DVCN)

Sheet	1	of	17

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1000		5,311,593	05/10/1994	Carmi	
	A1001		5,511,122	04/23/1996	Atkinson	
	A1003		5,805,803	09/08/1998	Birrell et al.	
	A1004		5,822,434	10/13/1998	Caronni et al.	
	A1005		5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A1006		60/134,547	05/17/1999	Victor Sheymov	
	A1007		60/151,563	08/31/1999	Bryan Whittles	
	A1008		5,950,195	09/07/1999	Stockwell et al.	
	A1009		6,119,171	09/12/2000	Alkhatib	
	A1010		6,937,597	08/30/2005	Rosenberg et al.	
	A1011		7,072,964	07/04/2006	Whittle et al.	
	A1012		09/399,753	09/22/1998	Graig Miller et al.	
	A1013		6,079,020	06/20/2000	Liu	
	A1014		6,173,399	01/09/2001	Gilbrech	
	A1015		6,226,748	05/01/2001	Bots et al.	
	A1016		6,226,751	05/01/2001	Arrow et al.	
	A1017		6,701,437	03/02/2004	Hoke et al.	
	A1018		6,055,574	04/25/2000	Smorodinsky et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
	B1000	WO 001/17775	03-30-2000	Science Applications International Corporation		Yes	No
	B1001	WO 00/70458	11-23-2000	Comsec Corporation			
	B1002	WO 01/016766	03-08-2001	Science Applications International Corporation			

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 383

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	2	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C998	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation,	
	C999	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1000	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1001	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) (RFC1101, DNS SRV)	
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1003	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	C1004	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	C1005	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	C1006	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	C1007	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	C1008	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	C1009	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	C1010	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	C1011	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	C1012	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 384

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	3	Of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1013	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1015	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	C1016	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista	
	C1017	Automative Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	C1018	Automative Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1020	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997).(Data Sheet, Aventail)	
	C1021	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	
	C1022	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail)	
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1024	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	C1025	Goldschlag, et al. *"Privacy on the Internet,"* Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 385

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	4	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1026	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	C1027	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	C1028	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	C1029	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server NewOpportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM).(Routing, Microsoft Prior Art VPN Technology)	
	C1030	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	C1031	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	C1032	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1034	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	C1035	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	C1036	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Defintion, ANX)	
	C1037	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	C1038	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 386

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	5	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1039	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	C1040	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1042	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1044	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	C1045	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	C1046	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (available at hap //www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue).(NT Beta, Microsoft Prior Art VPN Technology)	
	C1047	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	
	C1048	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	C1049	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	C1050	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 387

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	6	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1051	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	C1052	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET)	
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1055	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1058	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1060	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10) 9 **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1062	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 388

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	7	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1067	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	C1068	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1070	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, <draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	C1071	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs)	
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1073	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	C1074	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	C1075	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	C1076	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	
	C1077	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	C1078	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 389

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	8	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1079	Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	C1080	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	C1081	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1082	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	C1083	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	C1084	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	C1085	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	C1086	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	C1087	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	C1088	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	C1089	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	C1090	Assured Digital Products. (Assured Digital) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1091	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	C1092	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	C1093	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	C1094	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	C1095	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	C1096	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 390

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	9	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1097	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	C1098	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	C1099	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	C1100	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	C1101	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	C1102	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	C1103	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	C1104	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	C1105	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	C1106	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	C1107	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1108	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1109	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	C1110	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	
	C1111	Dan Sterne *et.al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	C1112	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 391

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	10	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1113	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	C1114	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	C1115	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	C1116	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	C1117	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide – Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-insuit.)	
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide – Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1119	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	C1123	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	C1124	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	C1125	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 392

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	11	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1126	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	C1127	Microsoft Corp., DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	C1128	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	C1129	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	C1130	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	C1131	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	C1132	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	C1133	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	
	C1134	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at*http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	C1135	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B:Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	C1136	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999)(Mastering Windows NT Server)	
	C1137	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	C1138	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	C1139	Kenneth Gregg, *et al.*, *Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	C1140	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 393

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	12	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1141	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1142	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/ deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1143	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	C1144	Microsoft Corp., Chapter 1 – Introduction to Windows NT Routing with Routing and Remote Access Service, *Available at* http://www.microsoft.com/technet/archive/winntas/proddocs/ rras40/rrasch01.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	C1145	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 – Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1146	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1147	F-Secure, *F-Secure NameSurfer* (May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	C1148	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)	
	C1149	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	C1150	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 394

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	13	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1151	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	C1152	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	C1153	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	C1154	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	C1155	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1156	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	C1157	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	C1158	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	C1159	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	C1160	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	C1161	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	C1162	F-Secure, F-Secure VPN+ for Windows NT 4.0 (1998) (from FSECURE 00000009) (FSecure VPN+)	
	C1163	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1164	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1165	IRE, Inc., *SafeNet / Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 395

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	14	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1166	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	C1167	IRE, Inc., About SafeNet / VPN Policy Manager (1999) (About Safenet VPN Policy Manager)	
	C1168	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1169	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* (July 22, 1996) (Gauntlet Functional Summary)	
	C1170	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	C1171	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	C1172	Todd W. Matehrs and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame* (Macmillan Technial Publishing 1999) (Windows NT Mathers)	
	C1173	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	C1174	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	C1175	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN) Overview)	
	C1176	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	C1177	WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1178	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1179	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1180	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 396

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	15	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1181	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	C1182	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1183	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	C1184	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0* (September 21, 1998)	
	C1185	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	C1186	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	C1187	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	C1188	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	C1189	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	C1190	*Virtual Private Network Demonstration* (March 21, 1998)	
	C1191	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	C1192	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	C1193	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	C1194	Information Assurance, *Science Fair Agenda* (2000)	
EXAMINER		DATE CONSIDERED	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 397

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	16	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1195	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	C1196	*IFE 3.1 Technology Dependencies* (2000)	
	C1197	*IFE 3.1 Topology* (February 9, 2000)	
	C1198	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* (January 10-11, 2000)	
	C1199	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	C1200	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	
	C1201	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1202	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	C1203	Network Associates Products – *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	C1204	Microsoft Corporation, Microsoft Proxy Server 2.0 (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	C1205	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	C1206	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	C1207	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	C1208	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 398

Best Available Copy

Substitute for form 1449/PTO SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known	
				Application Number	11/679,416
				Filing Date	February 27, 2007
				First Named Inventor	Victor Larson
				Art Unit	2157
				Examiner Name	Not yet assigned
Sheet	17	of	17	Docket Number	77580-015 (VRNK-1CP2DVCN)

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1209	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	C1210	David G. Schaer, *MCSE Test Success: Proxy Server 2* (1998) (Schaer, Microsoft Prior Art VPN Technology)	
	C1211	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	C1212	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1213	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1214	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	C1215	*AutoSOCKS v2.1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	C1216	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html	
	C1217	FirstVPN Enterprise Networks, Overview	
	C1218	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	C1219	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	C1220	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	C1221	Virtual Private Networks – Assured Digital Incorporated – ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	C1222	Accessware – The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	C1223	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	C1224	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/socks wp.html	
	C1225	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	C1226	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.
BST99 1618785-1.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 399

OIPE
MAY 0 4 2009
PATENT & TRADEMARK OFFICE

5-5-09

COPY

IDS

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	11/679,416
Filing Date	February 27, 2007
First Named Inventor	Victor Larson
Art Unit	2157
Examiner Name	Not yet assigned
Docket Number	77580-015 (VRNK-1CP2DVCN)

Sheet	1	of	17

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1000	5,311,593	05/10/1994	Carmi	
	A1001	5,511,122	04/23/1996	Atkinson	
	A1003	5,805,803	09/08/1998	Birrell et al.	
	A1004	5,822,434	10/13/1998	Caronni et al.	
	A1005	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A1006	60/134,547	05/17/1999	Victor Sheymov	
	A1007	60/151,563	08/31/1999	Bryan Whittles	
	A1008	5,950,195	09/07/1999	Stockwell et al.	
	A1009	6,119,171	09/12/2000	Alkhatib	
	A1010	6,937,597	08/30/2005	Rosenberg et al.	
	A1011	7,072,964	07/04/2006	Whittle et al.	
	A1012	09/399,753	09/22/1998	Graig Miller et al.	
	A1013	6,079,020	06/20/2000	Liu	
	A1014	6,173,399	01/09/2001	Gilbrech	
	A1015	6,226,748	05/01/2001	Bots et al.	
	A1016	6,226,751	05/01/2001	Arrow et al.	
	A1017	6,701,437	03/02/2004	Hoke et al.	
	A1018	6,055,574	04/25/2000	Smorodinsky et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	B1000	WO 001/17775	03-30-2000	Science Applications International Corporation			
	B1001	WO 00/70458	11-23-2000	Comsec Corporation			
	B1002	WO 01/016766	03-08-2001	Science Applications International Corporation			

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 400

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	2	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C998	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation,	
	C999	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1000	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1001	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) (RFC1101, DNS SRV)	
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1003	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	C1004	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	C1005	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	C1006	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	C1007	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	C1008	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	C1009	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	C1010	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	C1011	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	C1012	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 401

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	3	Of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1013	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1015	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	C1016	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista	
	C1017	Automative Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	C1018	Automative Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1020	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997).(Data Sheet, Aventail)	
	C1021	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	
	C1022	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail)	
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1024	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	C1025	Goldschlag, et al. "*Privacy on the Internet,*" Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 402

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	4	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1026	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	C1027	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	C1028	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	C1029	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server NewOpportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM).(Routing, Microsoft Prior Art VPN Technology)	
	C1030	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	C1031	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	C1032	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1034	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	C1035	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	C1036	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Defintion, ANX)	
	C1037	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	C1038	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 403

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	5	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1039	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	C1040	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1042	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1044	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	C1045	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	C1046	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (available at hap //www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue).(NT Beta, Microsoft Prior Art VPN Technology)	
	C1047	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	
	C1048	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	C1049	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	C1050	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 404

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	6	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1051	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	C1052	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET)	
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1055	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1058	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1060	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10) 9 **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1062	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 405

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	7	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1067	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	C1068	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1070	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, <draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	C1071	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs)	
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1073	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	C1074	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	C1075	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	C1076	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	
	C1077	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	C1078	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 406

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	8	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1079	Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	C1080	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	C1081	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1082	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	C1083	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	C1084	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	C1085	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	C1086	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	C1087	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	C1088	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	C1089	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	C1090	Assured Digital Products. (Assured Digital) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1091	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	C1092	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	C1093	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	C1094	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	C1095	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	C1096	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 407

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	9	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1097	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	C1098	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	C1099	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	C1100	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	C1101	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	C1102	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	C1103	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	C1104	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	C1105	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	C1106	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	C1107	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1108	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1109	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	C1110	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	
	C1111	Dan Sterne *et.al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	C1112	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 408

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	10	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1113	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	C1114	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	C1115	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	C1116	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	C1117	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide – Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-insuit.)	
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide – Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1119	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	C1123	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	C1124	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	C1125	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 409

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	11	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1126	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	C1127	Microsoft Corp., DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	C1128	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	C1129	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	C1130	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	C1131	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	C1132	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	C1133	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	
	C1134	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at*http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	C1135	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B:Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	C1136	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999)(Mastering Windows NT Server)	
	C1137	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	C1138	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	C1139	Kenneth Gregg, *et al.*, *Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	C1140	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 410

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	12	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1141	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1142	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/ deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1143	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	C1144	Microsoft Corp., Chapter 1 – Introduction to Windows NT Routing with Routing and Remote Access Service, *Available at* http://www.microsoft.com/technet/archive/winntas/proddocs/ rras40/rrasch01.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	C1145	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 – Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1146	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1147	F-Secure, *F-Secure NameSurfer* (May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	C1148	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)	
	C1149	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	C1150	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
EXAMINER			DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 411

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	13	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1151	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	C1152	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	C1153	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	C1154	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	C1155	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1156	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	C1157	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	C1158	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	C1159	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	C1160	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	C1161	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	C1162	F-Secure, F-Secure VPN+ for Windows NT 4.0 (1998) (from FSECURE 00000009) (FSecure VPN+)	
	C1163	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1164	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1165	IRE, Inc., *SafeNet / Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 412

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	14	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1166	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	C1167	IRE, Inc., About SafeNet / VPN Policy Manager (1999) (About Safenet VPN Policy Manager)	
	C1168	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1169	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* (July 22, 1996) (Gauntlet Functional Summary)	
	C1170	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	C1171	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	C1172	Todd W. Matehrs and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame* (Macmillan Technial Publishing 1999) (Windows NT Mathers)	
	C1173	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	C1174	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	C1175	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN) Overview)	
	C1176	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	C1177	WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1178	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1179	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1180	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
EXAMINER		DATE CONSIDERED	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 413

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	15	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1181	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	C1182	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1183	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	C1184	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0* (September 21, 1998)	
	C1185	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	C1186	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	C1187	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	C1188	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	C1189	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	C1190	*Virtual Private Network Demonstration* (March 21, 1998)	
	C1191	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	C1192	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	C1193	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	C1194	Information Assurance, *Science Fair Agenda* (2000)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 414

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	16	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1195	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	C1196	*IFE 3.1 Technology Dependencies* (2000)	
	C1197	*IFE 3.1 Topology* (February 9, 2000)	
	C1198	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* (January 10-11, 2000)	
	C1199	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	C1200	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	
	C1201	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1202	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	C1203	Network Associates Products – *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	C1204	Microsoft Corporation, Microsoft Proxy Server 2.0 (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	C1205	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	C1206	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	C1207	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	C1208	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 415

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	17	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1209	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	C1210	David G. Schaer, *MCSE Test Success: Proxy Server 2* (1998) (Schaer, Microsoft Prior Art VPN Technology)	
	C1211	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	C1212	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1213	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1214	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	C1215	*AutoSOCKS v2.1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	C1216	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html	
	C1217	FirstVPN Enterprise Networks, Overview	
	C1218	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	C1219	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	C1220	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	C1221	Virtual Private Networks – Assured Digital Incorporated – ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	C1222	Accessware – The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	C1223	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	C1224	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/socks wp.html	
	C1225	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	C1226	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.
BST99 1618785-1.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 416

OIPE MAY 0 4 2009 PATENT & TRADEMARK OFFICE

COPY 5-5-09

IDS

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	11/679,416
Filing Date	February 27, 2007
First Named Inventor	Victor Larson
Art Unit	2157
Examiner Name	Not yet assigned
Docket Number	77580-015 (VRNK-1CP2DVCN)

Sheet 1 of 17

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1000	5,311,593	05/10/1994	Carmi	
	A1001	5,511,122	04/23/1996	Atkinson	
	A1003	5,805,803	09/08/1998	Birrell et al.	
	A1004	5,822,434	10/13/1998	Caronni et al.	
	A1005	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A1006	60/134,547	05/17/1999	Victor Sheymov	
	A1007	60/151,563	08/31/1999	Bryan Whittles	
	A1008	5,950,195	09/07/1999	Stockwell et al.	
	A1009	6,119,171	09/12/2000	Alkhatib	
	A1010	6,937,597	08/30/2005	Rosenberg et al.	
	A1011	7,072,964	07/04/2006	Whittle et al.	
	A1012	09/399,753	09/22/1998	Graig Miller et al.	
	A1013	6,079,020	06/20/2000	Liu	
	A1014	6,173,399	01/09/2001	Gilbrech	
	A1015	6,226,748	05/01/2001	Bots et al.	
	A1016	6,226,751	05/01/2001	Arrow et al.	
	A1017	6,701,437	03/02/2004	Hoke et al.	
	A1018	6,055,574	04/25/2000	Smorodinsky et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	B1000	WO 001/17775	03-30-2000	Science Applications International Corporation			
	B1001	WO 00/70458	11-23-2000	Comsec Corporation			
	B1002	WO 01/016766	03-08-2001	Science Applications International Corporation			

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 417

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	2	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C998	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation,	
	C999	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1000	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1001	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) (RFC1101, DNS SRV)	
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1003	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	C1004	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	C1005	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	C1006	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	C1007	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	C1008	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	C1009	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	C1010	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	C1011	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	C1012	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 418

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	3	Of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1013	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1015	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	C1016	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista	
	C1017	Automative Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	C1018	Automative Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1020	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997).(Data Sheet, Aventail)	
	C1021	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	
	C1022	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail)	
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1024	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	C1025	Goldschlag, et al. "*Privacy on the Internet,*" Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 419

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	4	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1026	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	C1027	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	C1028	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	C1029	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server NewOpportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM).(Routing, Microsoft Prior Art VPN Technology)	
	C1030	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	C1031	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	C1032	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1034	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	C1035	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	C1036	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Defintion, ANX)	
	C1037	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	C1038	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 420

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	5	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1039	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	C1040	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1042	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1044	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	C1045	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	C1046	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (available at hap //www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue).(NT Beta, Microsoft Prior Art VPN Technology)	
	C1047	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	
	C1048	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	C1049	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	C1050	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 421

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	6	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1051	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	C1052	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET)	
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1055	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1058	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1060	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10) 9 **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1062	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 422

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	7	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1067	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	C1068	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1070	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, <draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	C1071	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs)	
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1073	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	C1074	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	C1075	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	C1076	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	
	C1077	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	C1078	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	
EXAMINER		DATE CONSIDERED	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 423

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	8	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1079	Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	C1080	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	C1081	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1082	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	C1083	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	C1084	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	C1085	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	C1086	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	C1087	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	C1088	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	C1089	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	C1090	Assured Digital Products. (Assured Digital) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1091	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	C1092	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	C1093	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	C1094	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	C1095	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	C1096	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 424

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	9	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1097	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	C1098	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	C1099	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	C1100	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	C1101	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	C1102	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	C1103	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	C1104	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	C1105	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	C1106	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	C1107	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1108	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1109	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	C1110	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	
	C1111	Dan Sterne *et.al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	C1112	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 425

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	10	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1113	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	C1114	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	C1115	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	C1116	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	C1117	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide – Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-insuit.)	
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide – Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1119	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	C1123	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	C1124	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	C1125	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 426

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	11	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1126	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	C1127	Microsoft Corp., DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	C1128	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	C1129	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	C1130	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	C1131	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	C1132	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	C1133	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	
	C1134	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at*http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	C1135	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B:Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	C1136	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999)(Mastering Windows NT Server)	
	C1137	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	C1138	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	C1139	Kenneth Gregg, *et al.*, *Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	C1140	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 427

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	12	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1141	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1142	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/ deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1143	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	C1144	Microsoft Corp., Chapter 1 – Introduction to Windows NT Routing with Routing and Remote Access Service, *Available at* http://www.microsoft.com/technet/archive/winntas/proddocs/ rras40/rrasch01.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	C1145	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 – Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1146	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1147	F-Secure, *F-Secure NameSurfer* (May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	C1148	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)	
	C1149	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	C1150	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 428

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	13	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1151	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	C1152	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	C1153	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	C1154	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	C1155	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1156	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	C1157	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	C1158	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	C1159	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	C1160	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	C1161	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	C1162	F-Secure, F-Secure VPN+ for Windows NT 4.0 (1998) (from FSECURE 00000009) (FSecure VPN+)	
	C1163	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1164	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1165	IRE, Inc., *SafeNet / Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 429

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	14	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1166	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	C1167	IRE, Inc., About SafeNet / VPN Policy Manager (1999) (About Safenet VPN Policy Manager)	
	C1168	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1169	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* (July 22, 1996) (Gauntlet Functional Summary)	
	C1170	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	C1171	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	C1172	Todd W. Matehrs and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame* (Macmillan Technial Publishing 1999) (Windows NT Mathers)	
	C1173	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	C1174	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	C1175	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN) Overview)	
	C1176	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	C1177	WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1178	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1179	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1180	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 430

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	15	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1181	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	C1182	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1183	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	C1184	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0* (September 21, 1998)	
	C1185	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	C1186	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	C1187	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	C1188	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	C1189	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	C1190	*Virtual Private Network Demonstration* (March 21, 1998)	
	C1191	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	C1192	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	C1193	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	C1194	Information Assurance, *Science Fair Agenda* (2000)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 431

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	16	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1195	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	C1196	*IFE 3.1 Technology Dependencies* (2000)	
	C1197	*IFE 3.1 Topology* (February 9, 2000)	
	C1198	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* (January 10-11, 2000)	
	C1199	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	C1200	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	
	C1201	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1202	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	C1203	Network Associates Products – *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	C1204	Microsoft Corporation, Microsoft Proxy Server 2.0 (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	C1205	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	C1206	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	C1207	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	C1208	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 432

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	17	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1209	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	C1210	David G. Schaer, *MCSE Test Success: Proxy Server 2* (1998) (Schaer, Microsoft Prior Art VPN Technology)	
	C1211	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	C1212	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1213	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1214	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	C1215	*AutoSOCKS v2.1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	C1216	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html	
	C1217	FirstVPN Enterprise Networks, Overview	
	C1218	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	C1219	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	C1220	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	C1221	Virtual Private Networks – Assured Digital Incorporated – ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	C1222	Accessware – The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	C1223	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	C1224	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/socks wp.html	
	C1225	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	C1226	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.
BST99 1618785-1.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 433

OIPE MAY 04 2009 PATENT & TRADEMARK OFFICE

COPY

5-5-09

IDS

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	11/679,416
Filing Date	February 27, 2007
First Named Inventor	Victor Larson
Art Unit	2157
Examiner Name	Not yet assigned
Docket Number	77580-015 (VRNK-1CP2DVCN)

Sheet 1 of 17

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1000	5,311,593	05/10/1994	Carmi	
	A1001	5,511,122	04/23/1996	Atkinson	
	A1003	5,805,803	09/08/1998	Birrell et al.	
	A1004	5,822,434	10/13/1998	Caronni et al.	
	A1005	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A1006	60/134,547	05/17/1999	Victor Sheymov	
	A1007	60/151,563	08/31/1999	Bryan Whittles	
	A1008	5,950,195	09/07/1999	Stockwell et al.	
	A1009	6,119,171	09/12/2000	Alkhatib	
	A1010	6,937,597	08/30/2005	Rosenberg et al.	
	A1011	7,072,964	07/04/2006	Whittle et al.	
	A1012	09/399,753	09/22/1998	Graig Miller et al.	
	A1013	6,079,020	06/20/2000	Liu	
	A1014	6,173,399	01/09/2001	Gilbrech	
	A1015	6,226,748	05/01/2001	Bots et al.	
	A1016	6,226,751	05/01/2001	Arrow et al.	
	A1017	6,701,437	03/02/2004	Hoke et al.	
	A1018	6,055,574	04/25/2000	Smorodinsky et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	B1000	WO 001/17775	03-30-2000	Science Applications International Corporation			
	B1001	WO 00/70458	11-23-2000	Comsec Corporation			
	B1002	WO 01/016766	03-08-2001	Science Applications International Corporation			

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	2	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C998	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation,	
	C999	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1000	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1001	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) (RFC1101, DNS SRV)	
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1003	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	C1004	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	C1005	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	C1006	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	C1007	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	C1008	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	C1009	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	C1010	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	C1011	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	C1012	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 435

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	3	Of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1013	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1015	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	C1016	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista	
	C1017	Automative Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	C1018	Automative Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1020	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997).(Data Sheet, Aventail)	
	C1021	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	
	C1022	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail)	
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1024	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	C1025	Goldschlag, et al. "*Privacy on the Internet,*" Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 436

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	4	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1026	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	C1027	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	C1028	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	C1029	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server NewOpportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM).(Routing, Microsoft Prior Art VPN Technology)	
	C1030	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	C1031	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	C1032	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1034	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	C1035	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	C1036	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Defintion, ANX)	
	C1037	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	C1038	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 437

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	5	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1039	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	C1040	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1042	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1044	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	C1045	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	C1046	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (available at hap //www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue).(NT Beta, Microsoft Prior Art VPN Technology)	
	C1047	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	
	C1048	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	C1049	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	C1050	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 438

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	6	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1051	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	C1052	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET)	
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1055	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1058	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1060	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10) 9 **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1062	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 439

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	7	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1067	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	C1068	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1070	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, <draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	C1071	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs)	
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1073	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	C1074	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	C1075	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	C1076	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	
	C1077	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	C1078	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 440

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	8	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1079	Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	C1080	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	C1081	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1082	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	C1083	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	C1084	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	C1085	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	C1086	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	C1087	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	C1088	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	C1089	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	C1090	Assured Digital Products. (Assured Digital) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1091	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	C1092	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	C1093	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	C1094	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	C1095	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	C1096	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 441

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	9	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1097	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	C1098	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	C1099	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	C1100	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	C1101	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	C1102	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	C1103	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	C1104	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	C1105	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	C1106	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	C1107	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1108	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1109	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	C1110	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	
	C1111	Dan Sterne *et.al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	C1112	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 442

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	10	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1113	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	C1114	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	C1115	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	C1116	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	C1117	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide – Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-insuit.)	
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide – Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1119	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	C1123	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	C1124	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	C1125	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 443

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	11	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1126	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	C1127	Microsoft Corp., DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	C1128	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	C1129	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	C1130	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	C1131	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	C1132	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	C1133	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	
	C1134	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at*http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	C1135	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B:Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	C1136	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999)(Mastering Windows NT Server)	
	C1137	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	C1138	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	C1139	Kenneth Gregg, *et al.*, *Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	C1140	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 444

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	12	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1141	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1142	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/ deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1143	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	C1144	Microsoft Corp., Chapter 1 – Introduction to Windows NT Routing with Routing and Remote Access Service, *Available at* http://www.microsoft.com/technet/archive/winntas/proddocs/ rras40/rrasch01.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	C1145	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 – Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1146	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1147	F-Secure, *F-Secure NameSurfer* (May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	C1148	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)	
	C1149	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	C1150	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
EXAMINER			DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 445

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	13	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1151	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	C1152	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	C1153	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	C1154	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	C1155	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1156	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	C1157	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	C1158	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	C1159	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	C1160	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	C1161	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	C1162	F-Secure, F-Secure VPN+ for Windows NT 4.0 (1998) (from FSECURE 00000009) (FSecure VPN+)	
	C1163	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1164	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1165	IRE, Inc., *SafeNet / Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 446

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	14	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1166	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	C1167	IRE, Inc., About SafeNet / VPN Policy Manager (1999) (About Safenet VPN Policy Manager)	
	C1168	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1169	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* (July 22, 1996) (Gauntlet Functional Summary)	
	C1170	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	C1171	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	C1172	Todd W. Matehrs and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame* (Macmillan Technial Publishing 1999) (Windows NT Mathers)	
	C1173	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	C1174	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	C1175	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN) Overview)	
	C1176	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	C1177	WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1178	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1179	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1180	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 447

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	15	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1181	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	C1182	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1183	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	C1184	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0* (September 21, 1998)	
	C1185	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	C1186	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	C1187	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	C1188	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	C1189	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	C1190	*Virtual Private Network Demonstration* (March 21, 1998)	
	C1191	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	C1192	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	C1193	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	C1194	Information Assurance, *Science Fair Agenda* (2000)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 448

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	16	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1195	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	C1196	*IFE 3.1 Technology Dependencies* (2000)	
	C1197	*IFE 3.1 Topology* (February 9, 2000)	
	C1198	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* (January 10-11, 2000)	
	C1199	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	C1200	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	
	C1201	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1202	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	C1203	Network Associates Products – *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	C1204	Microsoft Corporation, Microsoft Proxy Server 2.0 (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	C1205	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	C1206	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	C1207	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	C1208	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 449

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	17	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1209	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	C1210	David G. Schaer, *MCSE Test Success: Proxy Server 2* (1998) (Schaer, Microsoft Prior Art VPN Technology)	
	C1211	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	C1212	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1213	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1214	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	C1215	*AutoSOCKS v2.1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	C1216	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html	
	C1217	FirstVPN Enterprise Networks, Overview	
	C1218	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	C1219	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	C1220	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	C1221	Virtual Private Networks – Assured Digital Incorporated – ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	C1222	Accessware – The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	C1223	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	C1224	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/socks wp.html	
	C1225	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	C1226	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.
BST99 1618785-1.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 450

OIPE
MAY 01 2009
PATENT & TRADEMARK OFFICE

COPY 5-5-09

IDS

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	11/679,416
Filing Date	February 27, 2007
First Named Inventor	Victor Larson
Art Unit	2157
Examiner Name	Not yet assigned
Docket Number	77580-015 (VRNK-1CP2DVCN)

Sheet 1 of 17

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1000	5,311,593	05/10/1994	Carmi	
	A1001	5,511,122	04/23/1996	Atkinson	
	A1003	5,805,803	09/08/1998	Birrell et al.	
	A1004	5,822,434	10/13/1998	Caronni et al.	
	A1005	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A1006	60/134,547	05/17/1999	Victor Sheymov	
	A1007	60/151,563	08/31/1999	Bryan Whittles	
	A1008	5,950,195	09/07/1999	Stockwell et al.	
	A1009	6,119,171	09/12/2000	Alkhatib	
	A1010	6,937,597	08/30/2005	Rosenberg et al.	
	A1011	7,072,964	07/04/2006	Whittle et al.	
	A1012	09/399,753	09/22/1998	Graig Miller et al.	
	A1013	6,079,020	06/20/2000	Liu	
	A1014	6,173,399	01/09/2001	Gilbrech	
	A1015	6,226,748	05/01/2001	Bots et al.	
	A1016	6,226,751	05/01/2001	Arrow et al.	
	A1017	6,701,437	03/02/2004	Hoke et al.	
	A1018	6,055,574	04/25/2000	Smorodinsky et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	B1000	WO 001/17775	03-30-2000	Science Applications International Corporation			
	B1001	WO 00/70458	11-23-2000	Comsec Corporation			
	B1002	WO 01/016766	03-08-2001	Science Applications International Corporation			

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	2	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C998	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation,	
	C999	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1000	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1001	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) (RFC1101, DNS SRV)	
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1003	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	C1004	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	C1005	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	C1006	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	C1007	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	C1008	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	C1009	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	C1010	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	C1011	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	C1012	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 452

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	3	Of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1013	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1015	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	C1016	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista	
	C1017	Automative Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	C1018	Automative Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1020	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997).(Data Sheet, Aventail)	
	C1021	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	
	C1022	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail)	
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1024	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	C1025	Goldschlag, et al. "*Privacy on the Internet,*" Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 453

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	4	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1026	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	C1027	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	C1028	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	C1029	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server NewOpportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM).(Routing, Microsoft Prior Art VPN Technology)	
	C1030	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	C1031	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	C1032	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1034	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	C1035	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	C1036	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Defintion, ANX)	
	C1037	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	C1038	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 454

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	5	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1039	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	C1040	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1042	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1044	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	C1045	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	C1046	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (available at hap //www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue).(NT Beta, Microsoft Prior Art VPN Technology)	
	C1047	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	
	C1048	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	C1049	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	C1050	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 455

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	6	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1051	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	C1052	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET)	
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1055	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1058	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1060	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10) 9 **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1062	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 456

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	7	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1067	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	C1068	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1070	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, <draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	C1071	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs)	
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1073	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	
	C1074	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	C1075	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	C1076	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	
	C1077	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	C1078	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	
EXAMINER		DATE CONSIDERED	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 457

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	8	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1079	Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	C1080	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	C1081	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1082	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	C1083	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	C1084	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	C1085	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	C1086	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	C1087	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	C1088	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	C1089	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	C1090	Assured Digital Products. (Assured Digital) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1091	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	C1092	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	C1093	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	C1094	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	C1095	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	C1096	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 458

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	9	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1097	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	C1098	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	C1099	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	C1100	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	C1101	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	C1102	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	C1103	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	C1104	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	C1105	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	C1106	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	C1107	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1108	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1109	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	C1110	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	
	C1111	Dan Sterne *et.al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	C1112	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 459

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	10	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1113	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	C1114	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	C1115	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	C1116	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	C1117	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide – Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-insuit.)	
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide – Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1119	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	
	C1123	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	C1124	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	C1125	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 460

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	11	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1126	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	C1127	Microsoft Corp., DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	C1128	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	C1129	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	C1130	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	C1131	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	C1132	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	C1133	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	
	C1134	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at*http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	C1135	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B:Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	C1136	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999)(Mastering Windows NT Server)	
	C1137	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	
	C1138	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	C1139	Kenneth Gregg, *et al.*, *Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	C1140	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 461

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	12	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1141	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1142	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/ deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1143	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	C1144	Microsoft Corp., Chapter 1 – Introduction to Windows NT Routing with Routing and Remote Access Service, *Available at* http://www.microsoft.com/technet/archive/winntas/proddocs/ rras40/rrasch01.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	C1145	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 – Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1146	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1147	F-Secure, *F-Secure NameSurfer* (May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	C1148	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)	
	C1149	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	C1150	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 462

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	13	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1151	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	C1152	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	C1153	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	C1154	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	C1155	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1156	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	C1157	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	C1158	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	C1159	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	C1160	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	C1161	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	C1162	F-Secure, F-Secure VPN+ for Windows NT 4.0 (1998) (from FSECURE 00000009) (FSecure VPN+)	
	C1163	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1164	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1165	IRE, Inc., *SafeNet / Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 463

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	14	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1166	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	C1167	IRE, Inc., About SafeNet / VPN Policy Manager (1999) (About Safenet VPN Policy Manager)	
	C1168	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1169	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* (July 22, 1996) (Gauntlet Functional Summary)	
	C1170	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	C1171	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	C1172	Todd W. Matehrs and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame* (Macmillan Technial Publishing 1999) (Windows NT Mathers)	
	C1173	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	C1174	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	C1175	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN) Overview)	
	C1176	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	C1177	WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1178	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1179	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1180	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 464

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	15	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1181	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	C1182	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1183	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	C1184	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0* (September 21, 1998)	
	C1185	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	
	C1186	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint*	
	C1187	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	C1188	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	C1189	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	C1190	*Virtual Private Network Demonstration* (March 21, 1998)	
	C1191	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	C1192	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	C1193	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	C1194	Information Assurance, *Science Fair Agenda* (2000)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 465

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	16	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1195	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	C1196	*IFE 3.1 Technology Dependencies* (2000)	
	C1197	*IFE 3.1 Topology* (February 9, 2000)	
	C1198	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* (January 10-11, 2000)	
	C1199	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	C1200	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	
	C1201	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000) **[Due to difficulty locating this reference, a copy has not been provided]**	
	C1202	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	C1203	Network Associates Products – *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	C1204	Microsoft Corporation, Microsoft Proxy Server 2.0 (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	C1205	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	C1206	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	
	C1207	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	C1208	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 466

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2157**
				Examiner Name	**Not yet assigned**
Sheet	17	of	17	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1209	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	C1210	David G. Schaer, *MCSE Test Success: Proxy Server 2* (1998) (Schaer, Microsoft Prior Art VPN Technology)	
	C1211	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	C1212	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1213	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1214	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	C1215	*AutoSOCKS v2.1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	C1216	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html	
	C1217	FirstVPN Enterprise Networks, Overview	
	C1218	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	C1219	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	C1220	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	C1221	Virtual Private Networks – Assured Digital Incorporated – ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	C1222	Accessware – The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	C1223	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	C1224	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/socks wp.html	
	C1225	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	
	C1226	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.
BST99 1618785-1.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 467

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 17/00 — A2

(11) International Publication Number: WO 00/17775

(43) International Publication Date: 30 March 2000 (30.03.00)

(21) International Application Number: PCT/US99/21934

(22) International Filing Date: 22 September 1999 (22.09.99)

(30) Priority Data:

60/101,431	22 September 1998 (22.09.98)	US
09/399,753	21 September 1999 (21.09.99)	US

(71) Applicant *(for all designated States except US)*: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION [US/US]; 10260 Campus Point Drive, San Diego, CA 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: MILLER, Craig [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). MANGIS, Jeffrey, K. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). LESTER, Harold, D. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). NICHOLAS, John, M. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). WALLO, Andrew [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). KRESS, Thomas, P. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). CHEAL, Linda, J. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). WEATHERBEE, James, E., Jr. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US). DAVIES, Linda, M. [US/US]; Science Applications International Corporation, 10260 Campus Point Drive, San Diego, CA 92121 (US).

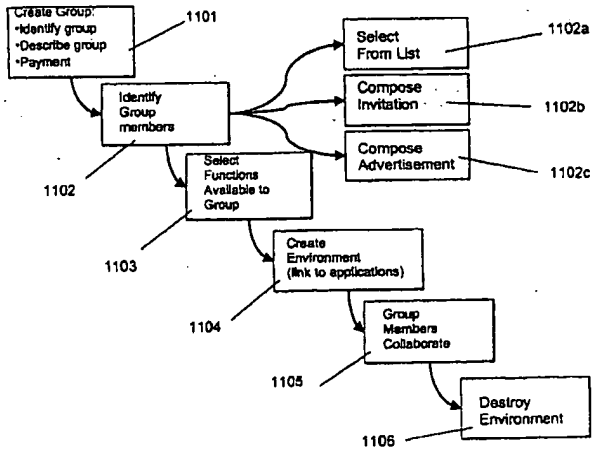
(74) Agents: WRIGHT, Bradley et al.; Banner & Witcoff, Ltd., Eleventh floor, 1001 G Street, N.W., Washington, DC 20001–4597 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

Without international search report and to be republished upon receipt of that report.

(54) Title: USER–DEFINED DYNAMIC COLLABORATIVE ENVIRONMENTS



(57) Abstract

A collaborative system and method allows members of a group to collaborate on a project such as a bid or proposal. According to a first embodiment, a complex instrument trading engine (CITE) facilitates negotiation between two or more parties. A set of tools and techniques are provided in order to facilitate negotiation and execution of complex instruments such as contracts between corporations and governments. According to a second embodiment, referred to as a dynamic collaborative environment, a user can define a group and a virtual private network environment including user–selected tools that facilitate communication, research, analysis, and electronic transactions within the group. The environment can be destroyed easily when it is no longer needed. Multiple environments can co–exist on the same physical network of computers.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

USER-DEFINED DYNAMIC COLLABORATIVE ENVIRONMENTS

This application is related in subject matter to and claims priority from provisional U.S. application serial number 60/101,431, filed on September 22, 1998. The contents of that application are bodily incorporated herein.

BACKGROUND OF THE INVENTION

1. Technical Field

This invention relates generally to computer systems and networks. More particularly, the invention relates to systems and methods for providing user-defined collaborative environments for transacting business or electronic commerce.

2. Related Information

Following hurricane Andrew, many insurance companies sought to limit their risk by withdrawing coverage from coastal areas. While this made good sense for the specific companies, it was not acceptable from a societal perspective. The cities, towns, homes and businesses built near the coasts could not afford to go without insurance, nor could the financial institutions that loaned money on these properties afford the risk. The problem facing the insurance companies was not the absolute magnitude of the risk, but the concentration of the risks in one area, leading to the possibility of very large losses resulting from a single event.

One law firm had conceived the idea of providing a mechanism for insurance companies to exchange risk. Companies with a high exposure in one area (e.g. Florida windstorms) could reduce their risk by ceding part of this to another company with non-coincident risk (e.g. California earthquakes) and assume part of the second company's risk in return. A company (CATEX) was formed to conduct such trading, but the trading rules had yet to be defined and the trading infrastructure had not yet been developed. CATEX postulated that the key barrier to insurance risk trading was determining the relative risk of different perils in different regions. One approach suggested by CATEX was to try to estimate these relative risks (termed relativities) for a broad set of perils and regions, to provide an initial basis for trading.

It was recognized, for various reasons, that this could not be done feasibly because: general estimates of risk, rather than the risk for specific locations, buildings, ships, etc. would be inadequate for commerce; there were many risks to evaluate given all of the permutations of location, perils, and structure; and companies would not be willing to trade risk based strictly on a third-party's analysis

Petitioner Apple Inc. - Exhibit 1026, p. 470

An analysis of the problem, however, indicated that estimating the relativities was not essential to facilitate trading, or, in a broader sense, that trading was the only way to address the problem of insuring concentrated risk. The key difficulty was determining how to create greater efficiency in the reinsurance market, whether by introducing new instruments (like swaps), bringing new capital to the market, connecting more buyers to more traders, or reducing the cost of placing reinsurance. It was determined that the above concept could be implemented in an electronic trading system that could play an important role in promoting these factors, and could, in fact, transform the reinsurance market, which is not very automated. A system that allowed trading was developed and implemented. A more detailed description of this system, as enhanced in accordance with various inventive principles herein (referred to as "first-generation" complex instrument trading technology), are provided below. More generally, as electronic commerce (and business-to-business commerce, in particular) has grown, various companies have developed software tools and services to facilitate transactions on the Internet and over private networks. E-Bay, for example, hosts a well-known web site that operates a transaction model (a so-called "concurrent auction") that permits buyers to submit bids on items offered by individuals. Lotus Notes provides a network-oriented system that allows users within a company to collaborate on projects. Oracle Corporation hosts various transaction engines for clients that pay to host such services on a web site. DIGEX Corporation similarly hosts web-based application programs including various transaction engines. Other companies sell so-called "shrink wrap" software that allows individuals to set up web sites that provide catalog ordering facilities and the like.

Some Internet service providers, such as America Online, host "chat rooms" that permit members to hold private discussions with other members who enter various rooms associated with predetermined topics. A company known as blueonline.com hosts a web site that facilitates collaboration on construction projects. Various virtual private networks have been created to facilitate communication among computer users across the Internet and other networks, but these networks provided very limited functionality (e.g., e-mail services); are not user-defined (they must be created and installed by system administrators); and they cannot be easily destroyed when they are no longer needed.

Petitioner Apple Inc. - Exhibit 1026, p. 471

The aforementioned products and services are generally not well suited to facilitating complex electronic transactions. As one example, most conventional services are predefined (not user-defined) and are centrally administered. Thus, for example, a group of companies desiring to collaborate on a project must fit their collaboration into one of the environment models provided by an existing service provider (or, alternatively, build a custom system at great expense).

Suppose, for example, that a group of high school students needs to collaborate on a research paper that requires soliciting volunteers for a survey on drug use, conducting the survey, brainstorming on the survey results, posing follow-up questions to survey participants anonymously, publishing a report summarizing the results, and advertising the report for sale to newspapers and radio stations. This project requires elements of communication among persons inside a defined group (those writing the paper) and outside the group (e.g., survey participants); conducting research (conducting the survey, compiling the results, comparing the results with other surveys published by news sources; and brainstorming on the meaning of the results); and conducting a commercial transaction (e.g., publishing the survey in electronic form and making it available at a price to those who might be interested in the results). No existing software product or service is available to meet the specific needs of this research team. Creating a user-defined environment including tools and communication facilities to perform such a task would be prohibitively expensive. Even if such a tailor-made environment could be created, it would be difficult to disassemble the environment (computers, networks, and software) after the project was completed.

In short, there is a need to provide a user-defined collaborative environment that is tailored to the needs of particular groups that conduct communication, research, electronic transactions, and deal-making.

SUMMARY OF THE INVENTION

A first embodiment of the invention, referred to as a complex instrument trading engine (CITE), facilitates negotiation between two or more parties. In this embodiment, a set of negotiation tools and techniques such as anonymous email, secure communication, document retention, and bid and proposal listing services are provided in order to facilitate the negotiation and execution of complex instruments such as contracts between corporations, governments, and individuals.

Petitioner Apple Inc. - Exhibit 1026, p. 472

A second embodiment of the invention, referred to as a dynamic collaborative environment (DCE), allows members of a group to define a dynamic virtual private network (DVPN) environment including user-selected tools that facilitate communication, research, analysis, and electronic transactions both within the group and outside the group. The environment can be destroyed easily when it is no longer needed. Multiple environments can co-exist on the same physical network of computers.

Although the two embodiments are described separately for ease of comprehension, it should be understood that the two embodiments share many features and, in fact, the second embodiment could include some or all of the features of the first embodiment in a generalized collaborative system. Consequently, references to a specific embodiment in the following description should not be deemed to limit the scope of features or tools included in each embodiment. Moreover, references to specific applications, such as the reinsurance industry, should not be deemed to limit the application of the invention to any particular field.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1A shows a four-step model of deal making including meeting, analysis, negotiation, and closing the deal.

FIG. 1B shows contract formation among a group of parties to a contract.

FIG. 2 shows a listing display system showing all offers for contracts and responses thereto.

FIG. 3 shows details of a listing that has been selected by a user.

FIG. 4 shows one possible implementation of a reply card definition screen.

FIG. 5 shows one possible implementation of a document management screen.

FIG. 6 shows one possible implementation of a screen indicating persons having access to a shared folder.

FIG. 7 shows a list of consummated deals in the system.

FIG. 8A shows detailed information regarding a completed trade.

FIG. 8B shows a deal summary including structured and unstructured information concerning the deal.

FIG. 9 shows a "flip widget" in a first state.

FIG. 10 shows a "flip widget" in a second state.

Petitioner Apple Inc. - Exhibit 1026, p. 473

FIG. 9A shows a more detailed example of a "flip widget" in a first state.

FIG. 10A shows a more detailed example of a "flip widget" in a second state.

FIG. 11 shows method steps that can be carried out to define, create, and destroy an environment according to a second embodiment of the invention.

FIG. 12 shows one possible system architecture in which various principles of the invention can be implemented.

FIGS. 13A through 13C show one possible user interface for creating a group and identifying group members.

FIG. 14A shows one possible user interface for selecting group members from one or more lists.

FIG. 14B shows one possible user interface for selecting group members by composing invitations.

FIG. 14C shows one possible user interface for selecting group members by composing an advertisement.

FIG. 15 shows a banner advertisement 1501 displayed on a web site, wherein the banner advertisement solicits participation in a group.

FIG. 16 shows one possible user interface for selecting communication tools to be made available to group members.

FIG. 17 shows one possible user interface for selecting research tools to be made available to group members.

FIG. 18 shows one possible user interface for selecting transaction engines to be made available to group members.

FIG. 19 shows one possible user interface for selecting participation engines to be made available to group members.

FIG. 20A shows an authentication screen for group members to gain access to a newly created environment.

FIG. 20B shows a web page generated for a specific user-defined environment, including tools available to group members having access to the environment.

FIG. 21 shows one possible method of generating environments in accordance with various aspects of the present invention.

FIG. 22 shows one possible data storage arrangement for storing and manipulating brain writing cards.

Petitioner Apple Inc. - Exhibit 1026, p. 474

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

A. COMPLEX INSTRUMENT TRADING ENGINE EMBODIMENT

A first embodiment of the present invention provides a second-generation version of a complex instrument trading system. The second-generation system includes specialized tools that were not included in the first version of the prior art CATEX insurance trading system described above. These tools represent a substantial improvement over the first generation and incorporate new concepts of communications in a trading environment, and other capabilities that did not exist in the first generation technology. In addition, it is believed that many of these tools are also applicable to software systems other than the Complex Instrument Trading Engine or Negotiating System (CITE) described herein. Thus, the inventive principles are not limited to trading systems for complex instruments, nor even to trading systems in general.

Primarily, the tools described herein ameliorate certain difficulties associated with trading of complex instruments. Complex instruments are instruments where there is more than one dimension for negotiation. As compared to such instruments as securities, complex instrument transactions take longer to research and consummate and require more extensive documentation. For example, stock trading employs a simple instrument (a share) and negotiation focuses on one dimension (price) while insurance contracts have many dimensions (term, price, coverage, definitions of perils, etc.). The stock market is relatively simple to automate -- as soon as bid and asked prices match, the deal is concluded in an instant according to the rules of the exchange. Automation of complex trading is much more difficult, since the parties must negotiate and reach agreement on multiple dimensions and document that agreement using an instrument specific to the precise agreement. Automation of complex instrument trading is more difficult in every way than trading simple instruments.

The trading model behind the Complex Instrument Trading Engine or Negotiating System is built around a simple, four-step model of deal making. Referring to FIG. 1A, the steps are as follows:

1. Meeting: Potential buyers connect with potential sellers with reciprocal interests. This connection does not mean that a deal will necessarily be concluded but simply that the two parties have some basis for continuing discussion. In simple

Petitioner Apple Inc. - Exhibit 1026, p. 475

instrument trading, it is typically only necessary to advertise quantity and price offered or sought. Offers for complex instruments must include substantially more detail and (frequently) extensive attachments or exhibits.

2. Research/Analysis: Each company considers its own position and/or offer and the counter party's position. Using information and analytic tools from various sources, including internal resources and resources provided by or through the trading system, each party does research and refines its position. The multiple dimensions of complex instruments increases the analytical complexity and limits the value of a simple market price. As indicated by the arrows in FIG. 1, this step is usually performed iteratively with the negotiation.

3. Negotiation: Parties to the negotiation speak directly and exchange whatever information is necessary to advance the deal. As indicated by the arrows in FIG. 1A, this step is usually performed iteratively with the research step.

4. Close: the companies negotiate and sign an instrument that documents the deal. This can be a complete and detailed contract, or it may be a simple memorandum. In simple instrument trading, the actual trade agreement is often standardized by the exchange. In complex instrument trading, the agreement must be more specific to the deal, though it is possible to use such tools and fill-in-the blank forms.

Within a system using these complex instrument tools, trading parties can place offers to buy, sell, or trade in a public area, and examine such offers ("listings") posted by others. Using advanced communications tools the parties can conduct initial discussions to determine if a placement is possible. Using tools described herein, the initial contact can be done anonymously.

If a deal seems possible, the system preferably provides access to the extensive information necessary to assess the possible deal. This can include static information (e.g. reports or data) maintained within the system, links to information providers outside the system, online analytical tools, and links to providers of analytical services.

For complex instruments, the process of negotiating a deal is contemplated to be an iterative one, with successive stages of analysis and discussion. The need for extensive communication is one of the critical distinctions between trading of simple instruments (e.g. retail sale) and complex instruments. Complex instrument

Petitioner Apple Inc. - Exhibit 1026, p. 476

trading requires dialog and more -- exchange of documents (often voluminous), consultation with counsel and intermediaries, conferencing, and working together on the final agreement. For electronic commerce to have an impact in complex instrument trading, it must support and facilitate this communication, and not force traders to fall back on methods and technology outside the electronic trading environment.

The final step is closing the deal. The companies can negotiate a contract online. Tools provide sample, fill-in the blank contracts and memoranda of understanding as a starting point. Negotiators can begin with these, or they can use one of their own. Collaborative software makes it possible to display text simultaneously on each negotiator's screen and to work on the language together. When the contract is final, the system allows for secure, online signature, though companies not comfortable with electronic signature for very large deals may print a hard copy and sign it conventionally.

By creating electronic exchanges for complex instrument trading, the CITE tools can have a fundamental and positive impact on many areas of commerce:

1. An electronic exchange makes it possible to put an offer in front of more people more quickly than could be informed through direct contact, even allowing for active intermediaries or brokers.

2. Traders can advertise and conclude deals without the need for an intermediary when they have adequate support or internal resources.

3. Through better communications, wider exposure for offers, and the first steps towards standard contract language, electronic trading of complex instruments can substantially reduces transaction costs.

4. With lower transaction costs, it is possible to conclude deals that were not possible with higher overhead.

5. Through the immediate posting of the results of trades, pricing is moved towards a market basis, reducing research and analysis costs enormously. This speeds placement.

6. Smaller exposure means lower risk, and market pricing is an adequate surrogate for analytically derived pricing in some circumstances. Together these factors make it possible for traders to participate in markets or market segments in which they would not normally do business.

Petitioner Apple Inc. - Exhibit 1026, p. 477

7. By making it possible for all companies, large and small, to talk directly to each other, electronic trading of complex instruments can lead to the democratization of the marketplace increasing competition.

Overall, electronic trading of complex instruments has the potential to improve the efficiency of markets enormously, and to establish markets in areas of commerce that are currently done through intermediaries or on a one-on-one basis. The trading tools described herein are designed to facilitate electronic trading of complex instruments. The first-generation complex instrument trading tools broke new ground in the extension of electronic commerce into new and more complicated markets. The table below summarizes the areas of new and improved technology, organized into the four steps of the general complex instrument trading model.

Phase	First Generation Complex Instrument Trading Technology (PRIOR ART)	Advanced Complex Instrument Trading Technology
Meet	• Operates on private network only • Post a listing to board by filling out a form • Display listing summary in a table • Search listings by key word • Post response to listing on board • Establish communications with lister by following up on contact information in listings using unconnected communications tools	• Operates on private network or over the Internet • Post listing to a board by filling out a form • Listings and responses can have attachments and documents • Display listing summary in a table, with sorting by title, date, market type, buy/sell, or listing number. • Search listings by keyword • Register keywords with an electronic "agent" that monitors listings and sends notice of relevant new listings by Email • Post response to listing on board • Send private response (anonymously or with name attached). • Response can be through a "reply card" designed by the trader posting a listing, to structure responses • Direct connection between listings and communications tool

Petitioner Apple Inc. - Exhibit 1026, p. 478

Analysis	• Internet access to research resources, on line and third-party analysis	• Internet access to research resources, on line and third-party analysis • Research resources searchable using the same search engine and display as used for listings. • Online dialogs / user groups
Negotiation	• Requires private network • Directory of contact information for all traders • Connection between directory and Email client. • Directory not linked to other components of the system • Anonymous mail application providing for communications between two individuals • Anonymous mail delivered to mail client • No attachments for anonymous mail • No system for central repository of documents	• Works on Internet or private network • Directory of contact information for all traders. • Direct connection between directory and Email client • Direct connection between directory and online conferencing software • Directory linked to listings and document management tool • Anonymous mail application providing for communications between individuals or groups of people working together • Anonymous mail does not require separate Email client software • Anonymous mail supports attachments • Internet-based system for distributions and sharing of documents. • Password and secure has protection for documents.
Closure	• Requires private network • Online signature of uploaded document	• Internet or private network • Online signature of uploaded document • Registration / closure of deal through a fill-in form • Provision for digital signature and archiving of all documents associated with a deal

Referring to FIG. 1B, one aspect of the system within the framework of the

Petitioner Apple Inc. - Exhibit 1026, p. 479

negotiation/analysis loop shown in FIG. 1, is the ability to define one or more contracts, for example, in the parlance of the reinsurance trade, "slip sheets." Various members of a group of authorities modify the contract causing it gradually to take a final form that is either rejected as untenable or accepted as a finalized deal. The system exposes various aspects of the contract and attendant documents to the appropriate participants in the transaction, also providing each with a level of authority to add, delete, or modify documents as well as the evolving contract or contracts (assuming there may be various contract templates being discussed). These filters (filter 1 through filter 4, for example), as shown in FIG. 1B, determine the authority of the party (Party 1-Party 4) to modify or see the data object, whether it is a document or a slip sheet. The system combines this system of filters with signature technology for closing the deal; that is, implementing signatures so that an enforceable contract is generated.

A deal is like any other data object and once it is defined and entered, it cannot be modified. Elements of the deal can be "signed" such as documents attached to a contract (for example, Contract 1 has documents D1 and D2 attached to (combined with) it. Together these elements, the contract and the attachments, define the deal. Also, the entire deal 245 can be signed using a signature device ("widget") S8. Other documents may relate to a deal but not be attached. These can be viewed using a document manager described further below.

Listing System

Referring to FIG. 2, a listing screen displays all offers for contracts, for example offer 314, as well as responses to them, for example, response 313. The parameters of the offers and responses to them are shown in columns, the heading of each of which may be selected to sort the listings by that heading, for example heading 315 if clicked would sort by the unique index number for the listing. Notice that the responses (for example, response 313) are shown indented to indicate a series of elements of a dialogue-thread. As indicated, the responses have a "daughter" relationship to the parent listings. That is, listing 314 is a parent and reply 313 is a daughter. The daughters remain in their hierarchical position beneath the parent despite sorting by the column headings. This makes the tabular sort scheme compatible with a threaded display, which is useful to show dialogues.

Referring now also to FIG. 3, when a user invokes a display of the details of

Petitioner Apple Inc. - Exhibit 1026, p. 480

a listing by clicking on an index hyperlink 312 to show the details of the listing, a user interface element displays the lister's defined parameters of the listing. As shown, various parameters are displayed, many of which are hyperlinked. For example, attachments 304 may be selected to display the corresponding attachments. A detailed description 301 may be provided as well as specific instructions for responding 302. A reply button 303 permits the user to reply. Activating the reply button 303 will either invoke a standard public reply screen which creates a new listing similar to the parent listing or a special reply defined by a reply card which is further described below.

A reply to a listing can take the form of a public reply that invokes a screen substantially the same as FIG. 3 but with blank spots for entry of reply information. A more useful kind of response element is a reply card that can be defined by the lister. This is because in negotiations on complex transactions such as reinsurance contracts and, for example, pollution emission allowances, the parties with whom a lister would be willing to trade are limited in terms of certain criteria. These criteria will vary from one type of transaction to another.

In an active trading system, the number of listings can quickly grow to a large number and quickly exceed the number which can conveniently be displayed in a single table. Several capabilities are built into the system to address this problem. First, by default, listings are presented in order from newest to oldest. Second, the sort capabilities previously described allow users to modify the standard order. Third, the total market may be divided into subcategories. In the area of insurance catastrophe risk, these could include categories for different lines of insurance (e.g. marine, aviation, commercial buildings). Fourth, users may enter search criteria to identify a subset of listings of particular interest.

Searching listings: A user may enter a keyword such as "hurricane" to identify all listings that contain that word in the title, description, and (optionally) attachments. To improve the reliability of the search, users are provided access to a standard lexicon when composing a listing. In the first embodiment, this capability is invoked by pressing the right mouse button while the cursor is any field of the listing. A list of common terms is displayed. The user can select the term of interest, which is then placed into the text of the listing at the insertion point marked by the cursor. For example, a listing for insurance risk would typically include a

Petitioner Apple Inc. - Exhibit 1026, p. 481

field for geographic scope (i.e. the location of the properties to be insured). When in this field, the lexicon displayed would include terms such as "California" and "Coastal Florida". Choosing a term from the lexicon insures uniformity of terminology across listings and between the search engine and the listings. "California" will be used rather than a mix of "Ca", "CA", "Calif", etc. The search is further improved by symantic indexing. Essentially, this means that synonymous terms are grouped, so that searches for one will find the other. A person who searches for "California" will get listings for "Los Angeles" that do not include the word "California".

The search engine can include an agent capability. This agent capability offers the user the option of saving a search, after the user reviews the results and deems them acceptable. This search is retained in a library of searches along with the email address of the owner of the agent. The search is retained in the library until is it either deleted by the user when it is no longer needed or automatically deleted in a cleanup of searches older than a certain date. Whenever a new listing is placed on the system, all of the saved searches are executed. If the new listing meets any of the search criteria, a message is sent to the owner of that criterion via email or instant messaging.

A model was developed to allow a lister to define a set of criteria and request a set of information from any respondents in the form of an anonymous reply "card." The card defines a set of requested information which may be packaged as a document object and placed in the document manager system and connected with each listing. A user would download the reply card and fill the card out and send it back to the posting party.

A document object, called a reply card, is made available to a respondent through the document manager. The respondent is permitted to retain his anonymity as is the lister. Each may communicate with the other through an Amail system described in more detail below. The respondent supplies the requested information and sends the data to the lister. A system in the listing manager allows a lister to define a reply card having any particular fields and instructions required of a respondent. Some of the information required may be obtained automatically from a set of default data stored on the respondent's computer.

Referring to FIG. 4, a reply card definition screen is invoked to define the

Petitioner Apple Inc. - Exhibit 1026, p. 482

parameters of a new listing. The new listing is defined using a user-interface element looking much like FIG. 3. While the details are not critical, the definition of reply card involves, in essence, the definition of a user-interface control such as a dialog with radio buttons, text boxes, etc. These are definable for server-side implementation through HTML and are well known so the details are not discussed here. The lister defines a set of controls that allow the entry by a replying party of the information that the lister requires. The reply card is stored as any other information object and may be organized and accessed through the document manager described below. FIG. 4 shows a simple example of a format of a reply card.

A reply card is created by a user when posting a new listing. The lister specifies the information that must be included in a response, and the type of information object to display for the data element (e.g. a text box, check box, radio button). The system then creates an HTML page to collect the requested information. When a respondent clicks "Reply Card" on the listing screen, the page is displayed. All of the responses are automatically entered into a database created automatically when the reply card is composed. As each respondent fills out a reply card, a new record is added to the database of the system and the lister is permitted to view it through an appropriate filter as discussed above.

Signature System

As business is increasingly done in an electronic environment, electronic signature and approval is becoming more critical. The typical electronic signature model has focused on two aspects:

1. Electronic validation of the user -- specifically determining that the person viewing a document on line is the authorized signatory; and
2. Validating the document being signed by a means that either prevents modification of a document or will reveal whether changes have been made.

Methods for validation of identity range from simple personal identification numbers or passwords, to electronic signature pads, and more advanced methods of biogenic validation such as fingerprint or retinal patterns. Methods for document validation range from simple archiving of one or more copies in a read-only model or inaccessible location to methods based on mathematical algorithms that create a characteristic number or alphanumeric string for a document. These strings are

Petitioner Apple Inc. - Exhibit 1026, p. 483

termed "electronic signatures." Changes to the document change the electronic signatures. Because the signatures are much shorter than the documents, very many documents have precisely the same signature, but the algorithms to calculate the signature are very difficult to invert, so that it is effectively impossible to deduce a meaningful change to a document that will preserve a specific signature.

These two aspects of electronic signature are highly developed, but there has been little analysis or development of the general process by which documents can be signed.

The invention allows for secure and reliable routing of documents, for which signatures are required, to a specified list of signatories. Unlike prior art systems, such as ordering or accounts payable systems which have highly structured signature procedures tailored to a specific process, the present invention provides a flexible method and system that allows a signature-type of authority/requirement to be attached any kind of information object. The method is sufficiently abstract, flexible, and general that it can be applied in many contexts aside from the CITE embodiment described in the present specification.

One signature method/device employs the following steps:

1. Registration of signatories – This process provides a register of identifiers indicating entities with signatory authority and correlates these identifiers with the information objects for which the signatory authority is applicable. The same register may also be used to identify other types of authority in the system in which the signature device is implemented. For example, document read authority, modification authority, exclusive access to documents, etc. may also be provided in the same register. Signature registration may be provided automatically in certain systems where registration of, for example, read/write authority is provided since any entity with signatory authority would in almost all instances, also be provided with some other kind of authority, most notably, read authority. Thus, where the signatory system is embedded in certain kinds of systems, it may be that no particular additional method or device is required to implement signatory registration since an existing register may already exist or be required for other purposes.

Registration information includes the general categories of information listed below. Definitions of specific fields within these categories are a function of the specific implementation of the signature system or the parent system. The following

Petitioner Apple Inc. - Exhibit 1026, p. 484

are exemplary:

1. Identity – unique identifier of the entity, the organization(s) with which the entity is affiliated, other relevant information.

2. Contact information – information indicating how the entity can be reached, how documents and mail messages can be routed to the entity.

3. Security Information – a password for each class of signature as described further below.

2. Classes of signatures – The device/method provides a variety of classes of signature, each associated with a unique level of approval or level of commitment. For example, a class of signature-authority can be defined that represents individuals, for example, with authority to sign contracts only below a set amount, or for expenses relating only to one department of an organization, or within certain time constraints, etc. The signatory system maintains this taxonomy of possible signature types in a database with a unique identifier for each level of authority defined. The system allows the creation and deletion of classes. Each class is preferably permitted to be named and a descriptive definition attached to each class.

3. Defining a Set of Signatures – Using an appropriate user interface element, the user of the system selects an information object (for example, a document, file, or collection of such objects) requiring signature(s). The entity originating the signature process then identifies the entity or entities required to sign the object. The specification of the signers can proceed either by the selection of individuals from a list supported by the above defined entity register. Alternatively, in an environment where individuals are strongly bound to organizations, for example, it can proceed by selecting the list of organizations that will sign and, within each organization, the person who will sign. The list is built by a series of selections. After each selection from the list, the user indicates his/her desire to add the selected individual to a list of required signatories. The user interfaces provides for entries in which all the selected signatories are required or only one of the selected signatories are required.

For example, if more than one entity is selected from the list prior to the selection (e.g., clicking an "Add" button), the system may require a signature from any of the people selected, but not all of them. To require signature from every member of the group, the initiator may select one person, then "add", select the second, then "add", and so on. Thus, adding a group with one "add" command would

Petitioner Apple Inc. - Exhibit 1026, p. 485

provide an "any signature will suffice" list and adding members individually would require a signature from that individual or entity. Note that this technique may also be used to define combinations of required and "any of" groups.

For each signer or group of signers selected in a single "add" command, the initiator of the signing sequence must specify the class of signature associated with the person for the document being signed. This may be selected from a list of signature classes (see item 2). If the specific implementation of the signature process only supports one class of signature, the selection of class may be omitted.

4. Random or Serial Order of Signature – After or concurrent with the creation of a signature list, the initiator specifies whether signatures must be in order or if a specific order is not required. For purposes of defining the order of signature, individuals who are selected as a group are considered as occupying a single place in the sequence.

5. Document Authentication – Upon initiating a signature sequence, the information object is authenticated by means of a secure hash algorithm. The specific hashing algorithm is a matter of design choice or may made dependent on a user's choice. There are several possible hash algorithms available in the public domain. The electronic signature produced by the secure hash algorithm is archived with the information object in a secure repository. If the information object is, for example, a record in a database, the contents of the record are copied to a file in delimited format for archival purposes. If the object is a table, the table is exported prior to archive.

6. Document Routing – Upon initiation of a signature sequence, the initiator specifies how the signatories are to be informed. The options are:

- No notification from the signature system
- Email message
- Email message with attachment of the information object.
- Posting on a signature web site

The system accepts and implements the chosen method, which may be connected to the signature or a single choice applied to all signatories. Alternatively, the method of notification may be stored with the signature class definitions. In a signature process with no required order, e-mail notice may be sent simultaneously to all of the

Petitioner Apple Inc. - Exhibit 1026, p. 486

designated individuals at the time of initiation. If the process is serial, only the first person may be notified. The electronic signature of the information object may be included in an e-mail message.

7. Accessing the signature system – The signature system can be implemented for access via a web browser or database client-server software across the Internet, an intranet, a LAN, or a WAN. Access to the system will typically require a password, but this may not be necessary on a secure network. Upon access to the system a user will have the option to display a list of all of the information objects which he or she has signed or is being asked to sign. For each object, the display can include the following information:

- Object name
- Description of object (text, mime, size, date)
- List of scheduled signatories
- Date each person signed
- Class of signature for each person
- Electronic signature produced by the secure hash algorithm

If the object is available (viewable) on line, the display may also include a link to display or download the object.

8. Validation of the Object at Time of Signature – If the user downloads or views the object, the system will execute the secure hash algorithm to calculate the electronic signature. This will be displayed so that the potential signer can compare it to the signature calculated at the time the process was initiated. If the user has previously downloaded the object or received it as an attachment to an Email, the user may access the secure hash code through the signature system and apply it to the version on the user's disk.

9. Signing a Document – After the user has determined that an information object is authentic and that the contents merit signature, he or she can affix a signature by authenticating his or her identity. Various means of authentication may be used. The means of authentication may be at the discretion of the manager of the signature system. Such means may include personal identification numbers, passwords, authentication based on computer address or information stored on the signer's computer, third party validation using a public key or other security infrastructure,

Petitioner Apple Inc. - Exhibit 1026, p. 487

or biogenic (fingerprint-recognition, retina scan) methods.

After a document is signed, the date of signature is recorded in a database so that the display to other potential signers is updated. If the signature process is serial, the next person in the sequence is notified. E-mail notice can be sent to all signers when the last signature is collected.

10. Follow-up – At the time a signature process is initiated, the initiator can select a time (in hours, days, or a time or date-certain) for automated follow-up. If a document is not signed within the specified period after notice, a follow-up e-mail can be sent as a reminder. Additional reminders may be sent at the same interval if the object has not been signed. The reminders can be sent automatically by the system according to user-input specifications.

11. Cancellation – The initiator of a signature sequence can modify the sequence at any time, except that a signer can not be deleted from the list once they have signed an object.

12. Transfer of authority – The individual initiating a sequence can transfer the right to modify the list signature list to another individual in the system with appropriate validation of identity.

Document Manager

Successfully conducting commerce over an electronic network requires the exchange not only of messages, but of substantial blocks of information in the form of documents and data. Beyond simply transferring files from hand to hand, it is often necessary for multiple parties to work on a document simultaneously or serially, to track changes, and to maintain a record of versions. Two general architectures have emerged for document management, which can be termed a "mail model" and a "repository model." Under the mail model, documents are attached to messages and circulated person to person. Under the repository model, documents are placed in a central location. There are advantages and disadvantages to each. At a summary level:

	Mail Model	**Repository Model**

Petitioner Apple Inc. - Exhibit 1026, p. 488

Advantages	Precise routing on a document specific basis. Push in the recipient is informed of a new document. Coupling between document flow and a messaging. Dating is automatic.	Compact storage -- only one version of a file need to be stored. Natural group of files on the basis of subject or access group. Supports good configuration management and version control.
Disadvantages	Creates multiple versions of a document, confounding configuration management and version control. Does not easily couple to online collaboration. Many mail servers limit size of attachment. Relatively high effort to prepare messages.	Not push in the sense that users are automatically informed of new documents. Security model is more complicated than for email. Prior arrangement is necessary to access a repository.

A browser-based document management model and tool combines the best features of repository model and the mail model, for document dissemination and sharing across the Internet or an intranet.

General Architecture – The general architecture of the system combines two basic components: (1) a database of directories and documents and (2) a directory of users. The directory of documents lists documents (of any type) contained in the system, and folders that can contain documents or other folders. The directory of users contains a list of individuals and organizations that can access the system, with passwords and/or other information necessary to validate identity and to establish authority.

Representation of document – The term "document" is used here in the broadest sense of any file that can be stored magnetically or electronically. Preferably, each file is given a unique name consisting of a string of no more than 256 characters. Preferably, the character set is limited to those members of the ASCII character set

Petitioner Apple Inc. - Exhibit 1026, p. 489

which are displayable or printable. Thus, such codes as "escape" which have no visible representation, would be excluded. This is the file name that is displayed for purposes of identifying the document to the users. There is also an actual file name (which is not shown to users) to identify where copies of the file are stored in the central repository. Certain other information is kept in addition to the name of the file. This includes the following:

1. Data of creation
2. Date entered into repository
3. Person who entered the document into the repository
4. Description
5. Size of the document
6. Document type if known
7. Date of last update
8. Access password (optional) stored in encrypted form
9. File folder(s) where the document appears
10. Actual file name

In addition to the above information, data indicating whether the file is checked-out and to what entity, and the identities of entities that have checked the document out and returned it in the past are also stored. The term "checking out" is described further below. These functions related to file change control and configuration management, which are discussed later.

User database – A database contains information on all individuals who can currently access the system or who previously had access up to an administratively determined retention period. This database includes standard contact information including physical and electronic addresses. Security data such as passwords and/or encryption keys is also maintained. In a combined system such as the presently described system, the same database or registry of users can be employed for the document manager as for the signature system.

High level directories – The entire document management system can be divided into a number of high level directories that the user can display, one at a time. These include, at a minimum, a "Private" directory of files and folders visible only to the user, and a "Public" directory of files and folders visible to all users. Additional high-level directories can be created by the system administrator as needed. These

Petitioner Apple Inc. - Exhibit 1026, p. 490

could correspond to projects, business units, or any other logical basis. At any point in the use of the document management system, a user can see and select from the high level directories to which the user has access. The name of the currently open directory can be always displayed on the screen.

Displaying the contents of a high-level directory – When a user selects a high-level directory, the repository displays a series of file folders against the left margin of the active window. File folders whose contents are displayed are shown as open folders. File folders who contents are not displayed are shown as closed folders. A folder is opened or closed by clicking a single time. When a folder is opened, the contents are shown with an indent to indicate the parent/child relationship between the folder and its contents. Each folder can contain files, shown by an icon representing a printed page and other folders, represented by an image of a closed folder.

Information about a folder – Information about each folder is displayed on the same line, to the right of the folder icon. This information is as follows, from left to right:

1. Name of the folder
2. Number of files in the folder, or the word "empty"
3. Accessibility of the folder

Accessibility refers to user access rights to a folder which may private relative to the entity that created it, restricted (limited to a subset of people who can access the high level directory), or shared (available to everyone with access to the high-level directory). The level of access to a directory is indicated by the words "private", "restricted" or "shared."

If the directory is restricted, clicking on the word restricted displays a list of the entities that have access to the folder. This list is a series of hyperlinks. Clicking on the name of a person pulls up detailed contact information (discussed below). The objective is to facilitate communications between people with a shared interest in a file.

Information about a file – Information about a file is displayed to the right of the file icon. From left to right, the first item displayed is the name. This is followed by the word "details." Clicking on "details," causes the document management system to display complete information about the file (see Item 2, above), the person who placed the document in the file, (see Item 3, above), and the person who most recently modified the file.

Petitioner Apple Inc. - Exhibit 1026, p. 491

Information about people/entities, and the link to communications – Information about people/entities with access to the system is displayable at several points in the document manager system:

1. by accessing the directory of users
2. when creating a new folder with "restricted" access
3. when displaying detailed information about a file (see #7)
4. when displaying information about a restricted directory (see #6)

Whenever such information is displayed, contact information from the database is rendered along with the name. Depending on the implementation, this can include complete contact info (multiple addresses, telephone and fax numbers, and email addresses), or some of the contact information may be restricted, in which case it is not displayed.

Creating a new top level folder – A new folder is created within a high-level directory, for example by clicking a button labeled "new folder." This can bring up a dialog in which the user assigns a name to the new folder and selects the type of access (private, shared, or restricted) rights to be assigned. If the document is restricted, the user specifies the entities (organizations and/or people) that can access the folder. If the creator of the folder specifies that an organization has access to a folder, all individuals associated with that organization may be granted access. Folders to which a user does not have access may remain hidden or not displayed. Alternatively, these folders can be shown with some indication that they are not accessible, for example, by ghosting.

Functions related to a folder – Once a folder is defined, a user can execute the following options.

1. Create a subfolder, using the same process described in 9
2. Add a document to the folder, using the process described in 11
3. Delete the folder, if it is empty
4. Modify access to the folder using the same tools used to specify access initially

The functions can be invoked by, for example, clicking on the appropriate label to the right of the name of the folder icon.

Adding a file – Users add a document using a dialog box that prompts for the following information:

Petitioner Apple Inc. - Exhibit 1026, p. 492

1. Location of file - may be entered by user, or selected through a standard file browse dialog
2. Name to be used for the file in the repository
3. Version number or name (optional)
4. Password or encryption key (optional)
5. Description (optional)
6. Access rules (read only or read-write)

After entering the above information, the user either aborts or initiates upload. The information listed above is recorded along with the name of the person entering the document, and date and time.

File options – The following functions may be provided, preferably for every file in the system:

1. Delete (with confirmation)
2. Archive. The file is removed from main repository, but a copy is retained outside the repository. It may be restored though manual intervention.
3. View or download: a copy of the file is brought to the user's computer. This file can be modified there for the individual user's use. A modified version can be uploaded as a new file or different version of a current one, but a file in the repository can only be replaced if the user has it checked out.
4. Check out / check in (see below)
5. Forward (see below)
6. Change Password. The old password must be entered followed by a new password and confirmation.
7. Move: copy or more a document from one folder to another.

The functions may be invoked, for example by clicking on a label corresponding to the function, which can be displayed to the right of the name of the file. Not all options are shown to all users. If an entity does not have write-access to a file, the entity may not delete it, archive it, check it in or out, or change the password.

Check in / Check Out – All entities with write access to a file may check it out. By checking the file out, the entity reserves the exclusive write to save changes to a file. A person may not replace a file that is checked out. To check out a file, the user selects this option from the list of functions associated with the file. The user can

Petitioner Apple Inc. - Exhibit 1026, p. 493

then enter an expected return date and a reason that the file is checked out or the changes to be made. This information is available to all others who can view the file. Each check in or check out is recorded in a permanent log. After a file is checked out, the "check out" button or link is changed to read "check in."

Each individual can check in only the files that he or she has checked out. This is done by clicking "check in." The user may then upload a new version of the file by specifying the location of the file on disk, or indicate that the version of the file currently in the repository is to be retained. After a file is checked in, the check button is changed back to "check out" and the file can be checked out by another user.

Forwarding – A file can be forwarded to any other user of the system. When the forward function is invoked, a list of users is displayed. The sender selects one or more users. Upon confirmation, a copy of the document is placed in folder labeled "in box" in each recipients private directory.

Referring to FIG. 5, a main screen for the document manager creates (using server-side scripting) a user-interface display with some of the features of a Windows Explorer® -type display. File and folder icons are shown along with an array features arranged next to each. The similarities with Windows Explorer® fairly well end there, however. Each of the properties shown next to each file/folder entry invokes a feature.

A parameter object W "Details" invokes a detailed display of the corresponding document object. The details can include contact information about the creator of poster of the document or other data as desired. This data can be hyperlinked and a return button can be provided to return the display back to the screen shown in FIG. 5. Clicking the "details" button to the right of any document brings up the display which can include the name, contact information, and other details about the person who loaded the document into the system, similar information about a person who has the document checked out, and, optionally, a description of the document and information on its change history.

A parameter object X "Forward" simply sends the document to a selected user. A selection screen can be invoked to allow selection of the recipient of the document from the user registry. Of course, since most correspondence can be handled on the server side, the user is, in reality, simply notified of the transfer and

Petitioner Apple Inc. - Exhibit 1026, p. 494

the recipient's action to view the document simply invokes a server side feature to display the document. The document is not actually transferred bodily to the recipient since the recipient, as a registrant logged in the user registry, can access it through the server by requesting to do so.

A parameter object U "Check-in" checks in a document that has been checked out. Other users may view the document, but not modify it when it is checked out. This button is not accessible to users that have not checked the document out and may be displayed ghosted or not displayed at all. A similar button can be displayed if a document that is not checked out may be checked out by the user authorized to see the document manager displayed shown in FIG. 5.

A parameter object T "Download" actually transfers a copy of the document to the client computer. Another object S "Delete" allows the document to be deleted. A new document can be added by clicking "New Document" Q. These are fairly conventional notions, except for their placement on the screen and the fact that each is filtered depending on the user's rights.

Note that when a folder is created, access to the folder can be restricted to the creator, shared with everyone (in which case the folder is created in the public directory), or shared with a select group of other users. The other users can be selected by company or organization (providing access to all individuals in the organization) or by individual within an organization. These are all selectable through a linked selection control where if one selects a company in one selection control, it shows employees in the linked selection control.

A parameter object P "Shared" displays a hyperlinked page that shows all users with access rights to the document. This page allows a user that places a document in the document manager or a user that has pertinent modify rights, to alter the parties that have access to the document. Also, it allows a user with read-only rights to see the list of users that can access that document. The names of the sharing parties are hyperlinked to invoke the user's email client to allow fast sending of email (which again may be performed server-side without actual transfer) or conventionally or selectively. If a folder is shared, the word "Shared" appears to the right of the folder. Clicking on "Shared" brings up the list of person who can access the folder, as shown in FIG. 6. Each name is a hyperlink to detailed contact information.

FIG. 7 shows a list of all deals that were completed through the system. The

Petitioner Apple Inc. - Exhibit 1026, p. 495

trade number (left column of the grid) is a hyper link to detailed information.

FIG. 8A shows detailed information about a completed trade. It shows the party to the trade, the price or rate, and a description of what was traded. The particular nomenclature is specific to a market. For insurance, for example, price is termed rate, and the summary of a deal is the slip sheet. A complete contract can be attached. Included documents can be downloaded to view on line. The intended signatories to a deal are shown (there can be more than two).

If a signatory has actually signed the document electronically, the date and time are shown. No date and time are shown for parties that have not yet signed. The amount of information displayed on the screen is dependent on the identity of the person viewing the screen. The viewer can be blocked from viewing any information about a deal, or certain fields, such as the contract details or the name of signatories.

Note that the detail screen of FIG. 8A would also show attached exhibits. The FIG. 8A display is the basic device for signing deals. A similar device would be used for signing documents.

Referring to FIG. 8B, all of the information necessary to document a deal is pulled together through the screen below. The deal summary includes highly structured information on parties, dates, terms, etc., as well as unstructured information in the form of attachments. The bottom part of the page allows the person registering the deal to designate the intended signatories. When the signers affix their electronic signature, they are doing so to all of the documents in the deal, including the attachments. These are archived and protected from tampering using secure hash technology. In this way it is possible to create a reliable, on line electronic signature to a complex deal, without risk of repudiation.

Note that any number of exhibits can be added to the UI device of FIG. 8B since the list scrolls from the bottom each time a second exhibit is added. The user interface has self-explanatory elements for defining information about the deal.

Anonymous Mail

For purposes of the following description, a "subscriber" is a person or entity that subscribes to an anonymous mail system to be described below. Certain types of negotiations and communications require anonymous initial contact, followed by some period of anonymous discourse, leading to eventual disclosure of the parties'

Petitioner Apple Inc. - Exhibit 1026, p. 496

identities. In the course of a typical sale or business deal, the initiating party begins either by contacting one or more targeted potential trading partners or advertising to a community of potential partners. While the identity of the initial offeror is usually clear in any direct contact, it need not be so in advertising. In certain cases it could be problematic for the initiating party to reveal his or her identity:

A party to a deal can have difficulty controlling the method of contact once the party's identity is known. If a company is known to be in the market for office space, for example, the party may be subjected to badgering by real estate firms outside the established bidding process. Executives of the company may be contacted directly in an effort to influence the decision.

Disclosure of intent may adversely affect the market. If a large company begins to acquire land in an area, the price can rise very quickly. Simple exploration of an option can make the option more costly or even impossible.

Disclosure of intent may adversely impact the reputation or standing of a company. An insurance company that determines that it is over exposed to a certain peril (e.g. hurricane losses in the Southeastern U.S.) would reveal that situation to their competitors and investors by a large public solicitation.

While anonymity can be crucial for the initiator of a deal, it can be equally important for the respondent for the same reasons. The need for controlled anonymity has been addressed by several methods that were initially developed for paper communications and have been extended to analogues in telephonic and computer communications.

- Numbered mail boxes, including government and private
- Communications through a mediator
- Anonymous voice mail drops
- The use of pseudonyms in computer e-mail and dialogs.

These methods have several serious shortcomings:

- The method may only allow anonymity from one side.
- There is no inherent mechanism to validate the credentials and intent on an anonymous party
- Use of a pseudonym may invalidate its future use by associating the name with a specific party

Petitioner Apple Inc. - Exhibit 1026, p. 497

- Manually mediated communications are slow
- The creation and deletion of pseudonyms may not be completely within the control of the party, imposing an overhead cost (in cash or labor) and/or delay in creating a new name
- In most systems, a person with multiple pseudonymous mailboxes or e-mail addresses will receive communications in several different places (mailboxes or accounts), thus requiring multiple logons/passwords.
- Routing of messages received anonymously requires manual forwarding to all relevant parties by the individual with access to the anonymous mail box or email account.
- There is no mechanism to reveal actual identities in a secure and mutually acceptable way.

The present invention addresses these deficiencies by providing two-way anonymous communications, a central point of collection for messages sent to multiple pseudonymous addresses, connection of multiple parties to a single anonymous account, and a mechanism to reveal identities to all parties to a deal simultaneously, by mutual consent. In summary, the anonymous mail system is a server side system that allows clients to create anonymous handles on the fly. It also allows them to share anonymous handles among multiple recipients so that the group of recipients appears as a single recipient to the sender using the anonymous handle. It is like a transparent mailing group. When mail is sent to an anonymous handle, it is sent to all members of the group.

Multiple Systems – In contrast to the first-generation anonymous mail system, the present system allows for multiple anonymous mail (Amail) systems. Each Amail system operates in association with a conventional e-mail server, and uses the e-mail server for communications with non-subscribers, subscribers to Amail systems other than the local one, and for forwarding messages to the subscribers Email client software.

Registration – Subscribers to an anonymous mail system (Amail) each complete a registration that provides:

- Contact information (name, address, telephone number, fax, etc.)
- Information to determine whether they the party is qualified to

Petitioner Apple Inc. - Exhibit 1026, p. 498

participate in the communications exchange. For example, if the system were to be used between and among real-estate agents, registrants to the system might be required to supply a real estate license number.

- Association with an organization (if appropriate)
- Additional information on the individual or organization that may be of use to others in the Amail system to determine the suitability of the party as a partner in negotiations.

The additional information can include such factors as credit ratings, assets, or the region in which the company does business. The specific information required depends on the application. Insurance, real estate, energy marketing, etc. would all have different data of interest.

Validation – Depending on the business model and role of the organization operating the Amail exchange, the organization can either accept the information provided by the subscriber, or verify the information and provide verification as part of the service. Upon acceptance of a subscription applications and validation of the background information if necessary, the use is assigned an Amail user ID and password.

In the first version of the Amail system, logon was automatic from the general application (CATEX); there was no separate user ID and password. In alternative versions, the Amail system can provide its own user ID and password, with the ability to bypass logon when it accessed from other applications with acceptable user validation. All of the actual contact information and validation information are maintained in a database. Validation information was not provided in the first version of CATEX.

Assignment of an Email address – Each subscriber must provide an Internet accessible Email address or be assigned an e-mail address in the Amail system. The first version of the Amail required that the user have an Email address on the system. The new version works directly with e-mail systems other than the Amail.

Logon – Subscribers access the Amail system by connecting an Amail web page provided either over the Internet or on an Intranet. The subscriber enters a user name and password. The first version of Amail was not browser-based and worked only over a LAN or WAN, not over the Internet or an intranet.

Petitioner Apple Inc. - Exhibit 1026, p. 499

Available functions – After logon, the subscriber can access the following functions:

- Manage aliases
- Compose an anonymous message
- Read Amail messages. In the original CATEX system, the user could not access messages from within the Amail application.
- Log off

Managing Aliases – Aliases are directly under user control. After logon, a user can:

- Add a new aliases
- Delete an existing alias
- Create a free-form note associated with a new alias, or edit the note for an existing alias that will be accessible to recipients from the alias.
- Identify other subscribers to whom messages to alias should be forwarded
- Identify other subscribers with permission to generate messages from the alias

These last two features make it possible for a group of subscribers to share an alias, allowing them share communications and work together more effectively. The user will:

Compose an anonymous message – After logon, a user can create and send an anonymous message. After the option is selected, the system will display a message creation screen with the following features:

1. A list of aliases currently owned by the user (i.e. created by the user and not deleted), for the user to select the alias from which the message will originate.
2. A subject box for the mail.
3. A list of the e-mail and alias addresses to which messages can be sent for the user to select one or more. The original version could only send to one alias. The user can also supply an Internet e-mail address off system.
4. A list of the e-mail and alias addresses to which copies of the messages can be sent for the user to select one or more. The user may also supply an Internet e-mail address off system. The original version did not include a "CC" feature.
5. A space where the message can be typed, allowing for users to paste text copies form another system using the Windows-based clipboard utility.

Petitioner Apple Inc. - Exhibit 1026, p. 500

6. A check box to select whether the sender is willing to reveal his identify to the recipient on mutual consent.

7. A check box to select whether the copies of the message should be sent to other subscribers who share the Alias. The original version allowed only one subscriber to access an alias.

Delivery of Messages – After an Amail message has been composed (see step 7), it is delivered as follows.

1. The body of the email message is modified by adding a header including routing information and an indication of whether the sender is willing to reveal identities if there is reciprocal concurrence. The message would appear as shown below. The items in italics are new since the original (prior art) version. The first generation of the anonymous mail system did not allow for communications between multiple Amail systems and, hence, did not list the Amail system name in the list of respondents. The first generation system also did not allow for multiple recipients.

Petitioner Apple Inc. - Exhibit 1026, p. 501

> *This message was sent anonymously from alias: Amail system name: alias*
> The message was sent to:
> Amail system name: *alias*
> Amail system name: alias (cc)
> Amail system name: alias
> The sender is willing to reveal identities.
> [Original body of the message]

2. If the message is sent to a specific, non-anonymous e-mail address, Amail composes and transmits a standard Email message. The sender is listed as "amail.admin.alias@xxxxx" where "xxxxx" is the address of the standard mail server supporting the mail system. Off-system access was not a feature of the first version.

3. If a message is sent to an alias on the local or any other related Amail system, and the owner of the alias has an off system email address, a message is sent as in step 1, above. In addition, however, the message is stored in an Amail message database for access through the Amail system interface. The original version did not have an Amail message database.

4. If a message has been sent to an alias for which there is no associated conventional mail account, the message is stored in the Amail message database. The Amail message database contains a repository for all messages, listing the subscriber(s) associated with the alias to which the message was addressed. The database contains the message (including sender, addressees, and ccs), date and time of transmission, and the alias of the subscriber to which the message was sent. The original version did not have an Amail message database.

5. If the option was checked to send copies to other that share the alias (see above), copies of the message are placed in the message database for the subscribers associated with each of the aliases.

Receipt of Messages – Messages sent from the Amail system can be received in a standard e-mail client by Amail subscribers and non-subscribers.

Amail subscribers can also receive messages through an Amail reader interface. All messages received are placed in the Amail message database (see above). Since an alias can be associated with more than one subscriber, the Amail message database can list more than one subscriber as an "owner" of the message even if it was sent to only one alias. When a user logs on and selects the option to

Petitioner Apple Inc. - Exhibit 1026, p. 502

read Amail messages (see above) the messages are rendered as an HTML page through a browser. Messages to all of the aliases associated with the user are displayed. Each message has a hotlink to respond to send a message back to the sending alias. Each message also has a link to display the background and validation information and note associated with the alias (see above). The original version did not provide an Amail viewer nor did it provide for display of validation information.

Responding from off System from Amail – Individuals from off system can respond to Amail messages using the standard reply feature of their mail server. Messages will be returned to the reply address (see above). Messages received by the conventional e-mail server supporting the Amail system will forward the message to the Amail message repository for the alias listed in the return address. Responding from a standard Email client was not provided in the original version.

Flip Widget

Increasingly, computer applications are delivered through browsers over the Internet or an intranet. There are many design considerations in building a system for browser delivery in contrast to delivery as conventional client server application. Two related considerations are the graphic richness of a browser screen and the time lag to render a new screen. Partly because good web pages contain complex graphics and partly because the Internet can be a relatively slow network, it is important to design a web application to make few unnecessary wholesale screen changes. It is more economical from the perspective of data transmission and, hence, from response time, to create a "flat" rather than "deep" hierarchy of screens, and change only the part of a screen that is minimally necessary.

For example, it is better in a data query to provide a single screen that allows a user to specify a state and city within the state than to provide a first screen for the state, followed by a second screen for the city. As the function of screens becomes more complex, however, it becomes an increasingly difficult challenge to fit all of the options onto the screen (particularly when a user selects a lower screen resolution) and while maintaining a clean appearance. The invention described here provides a tool that allows the Internet application developer to display an effectively unlimited number of options in a very small space using a very familiar and intuitive display feature.

Appearance – The "Flip Widget" tool renders a graphical object representing two

Petitioner Apple Inc. - Exhibit 1026, p. 503

rows of file folders, overlapping. The labels on the front row are visible, the labels on the second row are obscured by the front row of tabs, but the edges of the apparent back tabs are visible. The number of the apparent tabs displayed in each row is a function of the screen resolution and the length of the longest label entered by the user.

The Flip Tab – In one embodiment, the rightmost tab on the front row is labeled "FLIP". When a user actuates this tab, the response is as described below.

Database of labels and links – In creating the display, the application programmer enters a set of paired values. Each pair consists of (1) text of the label to be displayed and a tab, and (2) the name of an HTML link, either within or external to the page to be rendered when the tab is selected.

Action – Upon rendering a page containing the flip widget, the two-row tab display shows the first "n" options from the list of labels and links. The value of "n" represents the maximum number that can be displayed while allowing room for the flip tab. Upon clicking any of these tabs, the corresponding link is executed. Upon clicking the flip tab, the two-row tab display is changed to reflect the next "n" options from the list of labels and links, retaining the flip tab on the right. If there are fewer than n options remaining, the flip widget will either display the last n options, or whatever number remain supplement by as many options are needed from the start of the list. Clicking the flip tab when the list has been completed starts the cycle over again with the first option.

Referring to FIGS. 9 and 10, a flip widget in a first state is shown in FIG. 9. In the first state, any of the tabs A through E can be selected and the corresponding set of controls displayed. For example, in FIG. 9, tab B has been selected and the controls 430-432 are displayed. If the flip tab 410 is selected, a next row of tabs is brought forward so that the display appears as in FIG. 10 with tabs F through J showing. In FIG. 10, tab G has been selected and the corresponding controls 435-437 are displayed.

FIGs. 9A and 10A show a more detailed example of how a flip widget can be used to organize functions available to a user. For example, suppose that one application is a commodity futures trading system that permits a user to execute trades, review prices, and obtain other information relating to various metals such as gold, silver, and platinum. As shown in FIG. 9A, for example, controls or functions

Petitioner Apple Inc. - Exhibit 1026, p. 504

430, 431, and 432 (e.g., execute a trade, review current prices, and the like) are associated with a "gold" category and can be invoked easily when that category is at the forefront of the flip widget as shown. Clicking one of the other tabs (e.g., silver tab 400) would bring the functions associated with that category to the forefront while allowing the user to readily select other categories visible behind the front. Clicking "other markets" tab 410 would change the selection of front-row tabs to a different set of categories, as shown in FIG. 10A. The "other markets" tab 410 could be continually clicked to rotate through a plurality of groupings of markets, each having a set of functions or controls associated therewith.

A flip widget can be implemented in conjunction with the first or second embodiments of the present invention in order to permit many different functions to be displayed in a small screen space. The flip widget is a device to organize many different functions in a logical way, and can be used as a tool for building an interface to multiple applications. As one example, in a DCE (described in more detail below), there may exist n functions (e.g. bulletin boards, chat rooms, e-mail, a-mail, transaction engines, and the like) the specific availability of which can be defined by a user who creates the collaborative environment. This collection can change over time. Accordingly, the interface cannot be "hard coded" for a particular user.

One way to represent an indefinite (and potentially large) number of functions in a small space is with tabs resembling a file folder, with a graphic element representing hidden cards, implying that the user can reach the functionality on the cards by paging (i.e. flipping) to them. The flip widget makes it possible to provide a link to a list of applications maintained in a database rather than requiring that they be hard coded. Programming logic for storing folder labels in a database, linking those labels with associated functions and activating them using browser-type buttons, and for performing the display features described above, are conventional and no further elaboration is necessary. Although the "flip widget" provides one method of structuring a user interface to structure a user's view of application functions, other methods can of course be used.

B. DYNAMIC COLLABORATIVE ENVIRONMENT EMBODIMENT

In a second embodiment of the invention, a dynamic, user-defined collaborative environment can be created in accordance with a set of tools and method steps. As explained previously, this system differs significantly from

Petitioner Apple Inc. - Exhibit 1026, p. 505

conventional networked environments in that: (1) the environment (including access and features) is user-defined, rather than centrally defined by a system administrator; (2) each environment can be easily destroyed after completion of its intended purpose; (3) users can specify a group of participants entitled to use the environment and can define services available to those participants, including offering participation to unknown potential users; (4) the networked environment (including access features and facilities) can cross corporate and other physical boundaries; and (5) the environment offers a broad selection of tools that are oriented to communication, research, analysis, interaction, and deal-making among potential group members. Moreover, in a preferred embodiment, the environment is implemented using web browser technology, which allows functions to be provided with a minimum of programming and facilities communication over the Internet.

FIG. 11 shows various method steps that can be carried out to define, create, and destroy an environment according to a second embodiment of the invention. The term "environment" as used herein refers to a group of individuals (or computers, corporations, or similar entities) and a set of functions available for use by that group when they are operating within the environment. It is of course possible for one individual to have access to more than one environment, and for the same functions to be available to different groups of people in different environments.

The process of creating a collaborative environment involves the migration of tools and information resources available in the library of the environment generator into a specific collaborative environment. The collaborative environment can include / link to any application available to the environment generator. It can also include applications specific to the environment provided that theses are accessible through Internet protocols.

Underlying the environment is a directory of users, information about users, and their authorities. The core structure for the environment user database should conform to a directory standard – typically DAP (Directory Access Protocol) or LDAP (the lightweight directory access protocol). The environment generator has access to its own directory of users and to the user directories of the environments it has generated. The directory of an environment can be populated initially by selecting users from the environment generator's directories. These are added to the directory of the environment in one of two ways depending on the

Petitioner Apple Inc. - Exhibit 1026, p. 506

specific implementation. Directory records can be copies from the environment generators user database to a separate database for the environment or a flag can be added to the user data record in the environment generators users database to indicate that the user has access to the environment. The second, simple model is useful when all users in an environment have equal authority. A separate user database (directory) is necessary for an environment when the environment has its own security / authority model.

Additional members can be added through a set of standard application / subscription routines. These then become known to the environment generator (as well as the specific environment) providing the foundation for greater speed and efficiency in creating subsequent environment.

Beginning in step 1101, a new group is created by identifying it (i.e., giving it a name, such as "West High School Research Project," and describing it (e.g., providing a description of its purpose). The process of creating a group and defining functions to be associated with the group can be performed by a user having access to the system without the need for system administrator or other similar special privileges (e.g., file protection privileges, adding/deleting application program privileges, etc.). In this respect, environments are, according to preferred embodiments, completely user-defined according to an easy-to-use set of browser-driven user input screens. The principles described herein are thus quite different from conventional systems in which a central system administrator in a local area network can define "groups" of e-mail participants, and can install application programs such as spreadsheets, word processing packages, and the like on each computer connected to the network. Moreover, according to various preferred embodiments, the facilities provided to group members can be provided through a web-based interface, thus avoiding the need to install software packages on a user's computer.

It is also contemplated that various methods of obtaining payment for creating or joining groups can be provided. For example, when a new environment or group is created, the person or entity creating the group can be charged a fixed fee with payment made by credit card or other means. Alternatively, a service fee can be imposed based on the number of members that join, the specific functions made available to the group, or a combination of these. Moreover, fees could be charged

Petitioner Apple Inc. - Exhibit 1026, p. 507

to members that join the group. The amount of the fee could also be based on the length of time that the environment exists or is used.

Although not specifically shown in FIG. 11, step 1101 can include the step of creating a new entry in a database table (e.g., a relational or object-oriented database) to store information concerning the new group and the environment in which the group will operate. Database entries related to the group, including some or all of the information described below, can be created as the environment is defined. It is assumed that one or more computers are linked over a network as described in more detail below in order to permit the environment to be created, used, and destroyed, and that a database exists on one or more of these computers to store information concerning the environment.

In step 1102, the group members are identified. According to various embodiments, the group members can be identified in three different ways (or combinations thereof), as indicated by sub-steps 1102a, 1102b, and 1102c in FIG. 11. It is contemplated that group members can span physical networks and computer systems, such as the Internet. Consequently, group members can include employees of different corporations, government agencies, and the like. In contrast to conventional virtual private networks, both the group members and the functions made available to those group members are entirely user-selected, thus permitting a broad range of persons to easily create, use, and destroy virtual private networks and associated functionality.

First, in step 1102a, group members can be identified by selecting them from a list of known users that are to be included in the group. For example, within a corporation or similar entity, a list of internal e-mail addresses can be provided, or an electronic version of a phone list or other employee list can be provided. If the hosting computer system is associated with a school, then a list of students having accounts on the computer (or those in other schools that are known or connected to the host) can be provided. From outside a corporate entity, users can be selected based on their e-mail addresses (e.g., by specifying e-mail addresses that are accessible over the Internet or a private or virtually private network). In this step, the environment creator specifies or compels group members to belong to the group.

Second, in step 1102b, group members can be invited to join the group by composing an invitation that accomplishes that purpose. For example, a group

Petitioner Apple Inc. - Exhibit 1026, p. 508

creator may choose to send an invitation via e-mail to all members of the corporation, or all members of a particular department within the corporation, all students in a school or region, or members of a previously defined group (e.g., the accounting department, or all students in a particular teacher's class). The invitation would typically identify the purpose of the group and provide a button, hyperlink, or other facility that allows those receiving the invitation to accept or decline participation in the group. As those invited to join the group accept participation, their responses can be stored in a database to add to those members already in the group. Invitations could have an expiration date or time after which they would no longer be accepted. As invitees join the group, the group creator can be automatically notified via e-mail of their participation.

Third, in step 1102c, group members can be solicited by way of an advertisement that is sent via e-mail, banner advertisement on a web site, or the like. Persons that see the advertisement can click on it to join the group. It is also possible for advertisements to have a time limit, such that after a predetermined time period no more responses will be accepted. The primary difference between advertising participation in a group and inviting participation in a group is that invitations are sent to known entities or groups, while advertisements are displayed to potentially unknown persons or groups.

It will be appreciated that group members can be selected using combinations of steps 1102a, 1102b, and 1102c. For example, some group members can be directly selected from a list, while others are solicited by way of invitation to specifically identified invitees, and yet others are solicited by way of an advertisement made available to unknown entities.

In step 1103, the functions to be made available to the group are selected. For example, the group can be provided with access to an auction transaction engine; a survey tool; research tools; newswires or news reports; publication tools; blackboard facilities; videoconferencing facilities; and bid-and-proposal packages. Further details of these facilities and tools are provided herein. The group creator selects from among these functions, preferably by way of an easy-to-use web browser interface, and these choices are stored in a database and associated with the group members. Additionally, the group creator can specify links to other web-based or network-based applications that are not included in the list by specifying a web site

Petitioner Apple Inc. - Exhibit 1026, p. 509

address, executable file location, or the like. The group creator can also define shared data libraries that will be accessible to group members.

In step 1104, the environment is created (which can include the step of generating a web page corresponding to the group and providing user interface selection facilities such as buttons, pull-down menus or the like) to permit group members to activate the functions selected for the group. In some embodiments, access to the group may require authentication, such as a user identifier and password that acts as a gateway to a web page on which the environment is provided. Other techniques for ensuring that only group members access the group functions and shared information can also be provided. A web page can be hosted on a central computer at an address that is then broadcast to all members of the group, allowing them to easily find the environment.

In step 1105, group members collaborate and communicate with one another using the facilities and resources (e.g., shared data) available to group members. In the example provided above, for example, a group of high school students collaborating on a school research project could advertise for survey participants; conduct an on-line survey; compile the results; communicate the results among the group members; brainstorm about the results using various brainstorming tools; conduct a videoconference including group members at various physical locations; compile a report summarizing the results and exchange drafts of the report; and publish the report on a web site, where it could optionally be offered for sale through the use of an on-line catalog transaction engine. The group could even contact a book publisher and negotiate a contract to publish the report in book form using bid and proposal tools as described herein.

In step 1106, after the environment is no longer needed, it can be destroyed by the person or entity that created the group. Again, in contrast to conventional systems, the destruction of the environment is preferably controlled entirely by the user that created the environment, not a system administrator or other person that has special system privileges. Destruction of the environment would typically entail deleting group entries from the database so that they are no longer accessible.

FIG. 12 shows one possible system architecture for implementing the steps described above. As shown in FIG. 12, an Internet Protocol-accessible web server 1201 is coupled through a firewall 1202 to the Internet 1203. The web server includes

Petitioner Apple Inc. - Exhibit 1026, p. 510

an environment generator 1201a which can comprise a computer program that generates user-defined environments as described above. Further details of this computer program are provided herein with reference to FIG. 21.

Web server 1201 can include an associated system administrator terminal 1204, one or more CD-ROM archives 1205 for retaining permanent copies of files; disk drives 1206 for storing files; a database server 1207 for storing relational or object-oriented databases, including databases that define a plurality of user-controlled environments; a mail server 1208; and one or more application servers 1209 that can host application programs that implement the tools in each environment. Web server 1201 can also be coupled to an intranet 1210 using IP-compatible interfaces. Intranet 1210 can in turn be coupled to other application servers 1211 and one or more user computers 1212 from which users can create, participate in, and destroy environments as described herein, preferably using standard web browsers and IP interfaces. Web server 1201 can also be coupled to other user computers 1217 through the Internet 1203; to additional application servers 1215 through another firewall 1216; and to another IP-accessible web server 1213 through a firewall 1214.

It will be appreciated that the system architecture shown in FIG. 12 is only one possible approach for providing a physically networked system in which user-defined network environments can be created and destroyed in accordance with the principles of the present invention. It is contemplated that application programs that provide tools used in a particular user-defined environment can be located on web server 1201, on user computers 1217, on application servers 1215, on application servers 1209, on application servers 1211, or on any other computer that provides communication facilities for communicating with web server 1201. It will also be appreciated that web pages that provide access to each user-defined environment need not physically reside on web server 1201, but could instead be hosted on any of various computers shown in FIG. 12, or elsewhere.

Reference will now be made to exemplary steps and user interfaces that can be used to carry out various principles of the invention, including steps of creating a group, selecting group members, and defining functions to be made available to group members in the environment.

FIGS. 13A through 13C show one possible user interface for creating a group

Petitioner Apple Inc. - Exhibit 1026, p. 511

and identifying group members. In FIG. 13A, a user gains access to an environment creation tool by way of an authentication process. This may be a simple username and password device as shown in FIG. 13A, or it could be some other mechanism intended to verify that the user has access to the environment creation tool. In the case of a corporation, school, or other entity that already provides a log-in procedure to access the entity's network, such log-in procedure could serve to authenticate the user for the purpose of creating a new environment. It should be appreciated that user authentication is not essential to carrying out the inventive principles. Moreover, although it is contemplated that for ease of use (and to minimize programming) web browsers and web pages be used to receive user-defined information to create each environment, other approaches are of course possible.

In FIG. 13B, the user is prompted to create a new group by supplying a group name (e.g., "Joe's Homework") and a brief description of the group. This information is preferably stored in a database file and associated with group members and functions available to those group members.

In FIG. 13C, the user is prompted to identify group members. As described previously, group members are preferably identified in one of three ways (or combinations of these): (1) selection from a list of known group members; (2) inviting known candidates to join the group; or (3) advertising for new members. When the user clicks one of the options in FIG. 13C, he or she is prompted to supply additional information as shown in FIGS. 14A through 14C.

Beginning with FIG. 14A, for example, group members can be individually specified by entering an e-mail address (e.g., an internal or external e-mail address) in a text form data entry region and/or by selecting from a previously known list. This screen permits the user to compel attendance in the group by specifying names and/or e-mail addresses to which group messages will be sent. All those added to the group in this manner will be provided with access to the environment corresponding to the group. Aliases and pre-defined groups could also be specified as the basis for membership (e.g., all those in the accounting department of a corporation, or all students in a high school).

Each member of a group might have a group email account, or they may use an off-system email account. Off-system email addresses can be maintained in a database of users. Mail sent to the group email address is preferably forwarded off-

Petitioner Apple Inc. - Exhibit 1026, p. 512

system, protecting the actual email address of the person unless that person wishes to give out that address. New members can be added until the group is completed. Although not explicitly shown in FIG. 14A, it is contemplated that new members can be added to a previously defined group after the environment has already been created.

When group members are selected or specified, the user creating the environment can also create a password for each user in the group in order to enable those in the group to access the environment. Alternatively, when a user visits the environment, the environment can retrieve a "cookie" from the user's computer to determine whether the user is authorized to access the environment. If no cookie is available, the user could be prompted to supply certain authentication information (e.g., the company for whom he or she works, etc.) In yet another approach, authentication could occur by way of e-mail address (i.e., when the user first visits the environment, he or she is prompted to enter an e-mail address). If the e-mail address does not match one of those selected for the group, access to the environment would be denied.

Turning to FIG. 14B, prospective group members can also be "invited" to join the group. The user creating the environment can specify one or more e-mail addresses to which an invitation will be sent. The invitation can be a simple text message, or it could be a more sophisticated video or audio message. An expiration date can also be associated with the invitation, such that responses to the invitation received after the date will not be accepted. Software resident in web server 1201 (FIG. 12) receives responses to the invitations and adds members to the appropriate group or drops them if the expiration date has passed or the prospective group member declines participation. Prospective members can join the group by sending a reply with a certain word in the message (e.g., "OK" or "I join"); by clicking on a button in an e-mail message; or by visiting a web site identified in the invitation.

Turning to FIG. 14C, group members can also be solicited by creating an advertisement directed primarily at potential group members that are unknown. The advertisement could include, for example, a banner ad comprising text, video, and/or audio clips. The graphic should conform to the size designated for the ad on the web page. The ad could be posted on a web site by uploading the graphic through a web interface and, optionally providing a URL on the screen of FIG. 14C to link to if the

Petitioner Apple Inc. - Exhibit 1026, p. 513

advertisement is clicked. Software on the group page can render advertisements on a page either (a) every time the page is displayed, (b) in rotation with other ads; or (c) when characteristics of the user match criteria specified for the ad.

The advertisement can include an expiration date after which responses would no longer be accepted. Advertisements could range from the very specific (e.g., an advertisement posted on a school's home page advertising participation in Joe's research project on drug use at the school) to more general (e.g., an advertisement that says "we're looking for minority contractors looking to establish a long-term relationship with us" that is posted on web sites that cater to the construction industry.

A qualification option can also be provided to screen prospective group members. For example, if an advertisement seeks minority contractors to participate on a particular construction project, selecting the "qualify" option would screen responses by routing them to the user that created the group (or some other authority) before the member is added to the group. Those responding to the advertisement could be notified that they did not pass the qualifications for membership in the group, or that further information is required (e.g., documents evidencing qualifications) before participation in the group will be permitted. Alternatively, an automatic qualification process can be provided to allow a prospective member to join if the person fills in certain information on the response (e.g., e-mail address, birthdate that meets certain criteria, or the like).

As shown in FIG. 15, a banner ad displayed on a web site invites minority contractors to join a group that bids on information technology contracts. Those interested in the advertisement click a button, which leads them to another site (not shown) requiring that they provide certain information (qualification information, name, age, company registration information, etc.) This information is then forwarded to web server 1201 which either pre-screens the information according to pre-established criteria, or notifies the user creating the group that a prospective member has requested access to the group. In the latter case, the user could screen the applicant and grant access to the group.

FIG. 16 shows one possible user interface for selecting communication tools to be made available to group members. This screen can be presented to the user creating the environment after the group has been identified and its members

Petitioner Apple Inc. - Exhibit 1026, p. 514

selected. It is contemplated that a variety of communication tools can be provided, including a bulletin board service; advertisements; white pages (e.g., a listing of members, their e-mail addresses, telephone numbers, and the like); yellow pages (e.g., a listing of services or companies represented by group members, with promotional and contact information); document security (e.g., shared access secure document storage services); anonymous e-mail (described above with respect to the first embodiment); threaded dialogs; a group newsletter creation tool; videoconferencing; and even other user-provided applications that can be specified by name and location (e.g., URL). Details of these services are provided below.

According to various preferred embodiments, dynamic collaborative environments are designed to integrate tools from multiple sources provided that they are web-accessible (i.e., they operate according to Internet Protocol and/or HTML-type standards). The categories listed above provide a reasonable taxonomy of the tools necessary for collaboration, but this list can be extended to include virtually every class of software such as computer-assisted design, engineering and financial analysis tools and models, office applications (such as word processing and spreadsheets), access to public or proprietary databases, multimedia processing and editing tools, and geographic information systems. The following describes some of the communication tools that can be provided:

Bulletin boards. A bulletin board (see, e.g., FIG. 2) lists notices posted by group members, which may be offers to buy or sell, but need not be limited to such offers. Many types of bulletin board services are of course conventional and no further discussion is necessary in order to implement one of these services. Nevertheless, in one embodiment the following data items (attributes) can be provided for each notice appearing on the bulletin board: an item number, a title, the date posted, and one or more special attributes defined by the user. The attributes may include a field to indicate whether a listing is a "buy" or "sell " offer. The board can be provided with an integrated sorting capability. By clicking on the heading of each column, the user can sort the entries in, alternately, ascending or descending order. Thus, it is possible to organize the records from oldest to newest or newest to oldest, or to separate buy and sell offers. To limit the values on a board, a search capability can also be provided, such that only those entries that meet the search criteria are displayed.

Petitioner Apple Inc. - Exhibit 1026, p. 515

Advertisements. In a typical environment of a dynamically created network there are a number of fixed places for advertisements – the top of a page for a banner, the bottom of a page for a banner, and space on the side for small ads. The creator of the environment may choose to use none, any, or all of these spaces for advertisements. Once a space is designated for advertising, group members may place adds by completing a template that provides payment information (if required), the text for the ad (any standard image format), and a link to be executed if the ad is clicked by someone viewing the ad.

Each user is responsible for providing functionality behind the link. The ad may be displayed persistently (every time a page is displayed), in rotation with other ads for the same place, or may be triggered on the basis of user characteristics including purchasing history. Revenue can be collected for placement (fixed price regardless of how many times an ad is displayed), per time that the ad is displayed, or per click on the ad. The virtual private network provides the front-end to facilitate online placement of the ad. Display can be done by linking pages to standard ad display code, available off the shelf from several sources. This code provides for rotation of the ads. Software for customization (i.e. choosing the ad based on user characteristics) is available commercially from several sources.

White pages. White pages provide a comprehensive listing or directory of members with information about them and information regarding how to contact them. Various types of commercially available software can be used to manage such directories, and it is elementary to code typical directories that have fixed contents for each member.

A web-accessible directory can be used in accordance with various embodiments of the invention. One type of directory that can be provided differs from directories having fixed structures. The key differences are as follows:

(a) User control over information Users enter and maintain their own information directly, rather than through a central organization. This provides more immediate update of data and reduces transcription errors. It makes it simple, for example, for people to change their phone number when they are temporarily working at another location.

(b) Multiple points for quality control. The data regarding each user can be displayed to the user periodically (e.g.30, 60, and 90 days), and the user prompted to

Petitioner Apple Inc. - Exhibit 1026, p. 516

update and verify the data. A feedback capability can be provided for members of a group to report errors they find. Email addresses can be "pinged" periodically to determine if they still exist. In addition, server management staff can periodically review accounts that have had recent activity.

(c) Object structure. A directory entry consists of a collection of data elements. These elements include such things as name for addressing (Dr. John D. Smith), sort name (Smith, John D), or primary work telephone (800-555-1212). Traditional mail systems have a fixed number of rigidly formatted elements. In one embodiment, a more flexible approach can be used in that individuals identify which elements they wish to add to the collection comprising their directory entry. For example, a person can add 3, 4, 5 or more telephone numbers attaching a note to each explaining its use (e.g. "for emergencies after 8PM").

(d) Direct link to communications tools. Where a directory refers to a contact method (e.g. a telephone number), the method can be invoked directly from an entry if the necessary software is available. For example, phone number can be dialed, email messages initiated, or a word processing session initiated with letter and envelope templates, preloaded with address information.

(e) Descriptive information. In addition to contact information, each directory can contain information describing the entry (individual or business). The description can be different in each group or it can be the same. The descriptive is free form, with the exception that the user may drop in terms from a group-specific lexicon. This lexicon can include terms specific to the industry (e.g. "fuel system") for the automotive industry, or preferred forms of standard terms (e.g. "California" rather than "CA", "Ca", or "Calif."). Standardization of terms in this way makes search the directory more reliable.

Yellow pages. Conventional "yellow pages" products provide a one level classification of directory entries designed to facilitate identification of and access to an individual or organization with specific interests and capabilities. Within industries, and particularly online, multi-level hierarchical directories are common, with the multiple levels providing more precise classification. There are numerous commercial products for maintaining online yellow page type classification systems.

Any web-accessible directory can be connected to a DVPN group. A preferred method offered with the system integrates the classification system with the

Petitioner Apple Inc. - Exhibit 1026, p. 517

descriptive field in a directory entry. Every time a standard term pertaining to a classification is pulled from the lexicon, the entry is added to that classification in the hierarchical sort. In addition to hierarchical access, this correspondence between the traditional hierarchical sort and the free-form description with standardized terms makes it possible to access records via search rather than browsing the hierarchy. Searching makes it possible to identify an organization with multiple capabilities (e.g. "brake repair" and "frame straightening"). This search capability is much like a general web-search using a tool like AltaVista's or Inktomi's search engine and can use the same search engine, but differs in that material being search is in a precisely defined domain (group members), the information being searched is limited and highly quality controlled (i.e. group directory entries), and has a precision rooted in a precise vocabulary (the lexicon used in preparing the description).

Document repository. Any commercial web-enabled document repository can be integrated into a group. Examples are Documentum and PC DOCs. An improved version offered specifically with the DVPN package was described above.

Document security. Within the document repository various tools can be provided to protect the security of documents. These include (1) limiting access to a document to certain people or groups; (2) only displaying the directory entry for documents to people who can access it; (3) password protection; (4) encryption; (5) secure archive in read only mode on a third-party machine; (6) time-limited access and (7) a secure hash calculation.

All of the above are conventional except for time-limited access and the secure hash calculation. Software for limiting access to a document to a certain period is available from Intertrust, among others. A secure hash is a number that is characteristic of the document calculated according to a precisely defined mathematical algorithm. There are several secure hash algorithms, and implementers can develop their won. They are "trap door" in nature. That is, the calculation can be performed with reasonable effort, but the inverse of the function is computationally intractable. The classic example of a trap door function is multiplication of very large prime number (on the scale of hundreds of digits). The product can be calculated with relative ease, but factoring the product (the inverse function) is very time consuming, making if effectively impossible with generally available hardware. This method is used in public key encryption, but can be applied

Petitioner Apple Inc. - Exhibit 1026, p. 518

equally well in secure hash, though other trap door functions are preferred, in particular, the one specified by the U.S. Department of Commerce as FIPS standard 180. Code to implement this standard can be developed from published algorithms.

Anonymous e-mail (described above with respect to the first embodiment);

Threaded dialogs. Threaded dialogs are a collection of messages addressing a specific topic, added serially, not in real time. They are threaded in the sense that new topics can branch off from a single topic, and topics can merge. According to one embodiment, threaded dialogs differ from conventional news group functionality in that (1) users can initiate new topics; (2) users can post a message to one topic, then indicate that the message pertains to other topic as well; (3) browsers reading a message may continue down the original thread or one of the alternates if other topics are suggested.

Group newsletter creation tool. A newsletter creation tool can be used to link columns provided by multiple users (and maintained as separate web documents) into a whole through an integrating outline maintained by an "editor". The purpose of the tool is to provide the look and feel of an attractive single document to a disparate collection. To create the newsletter the editor generates an outline identifying an author for each component and a layout. Art for the first page can be provided. Through messaging, the authors are provided a link to upload their content. Content is templated to include a title, date, a by line, one or more graphic elements, a summary for the index, and text. The editor may allow documents to go directly to "publication" or require impose a review and editing step.

Chat groups. Real time chat room software is widely available from many sources including freeware and shareware.

Audio and videoconferencing. Commercially available tools for web-based audio and video conferencing can be included in the group functionality. Examples are Net Meeting and Picture Tel software.

FIG. 17 shows one possible user interface for selecting research tools to be made available to group members. As shown in FIG. 17, various tools such as a mortgage calculator, LEXIS/NEXIS access, news services, Valueline, and other research tools can be provided by checking the appropriate box on the display. All of these research tools are conventional and commercially available (via web-based links and the like).

Petitioner Apple Inc. - Exhibit 1026, p. 519

FIG. 18 shows one possible user interface for selecting transaction engines to be made available to group members. As shown in FIG. 18, many different types of transaction engines can be provided to group members, including electronic data interchange (EDI) ordering; online catalog ordering; various types of auctions; sealed bids; bid and proposal tools; two-party negotiated contracts; brain writing (moderated online discussion) and online Delphi (collaborative estimation of a numerical parameter). The following describes various types of transaction engines in more detail. Enhanced features (i.e., those that differ from conventional products) are highlighted in gray text.

A. Order placement (online catalog) transaction engine

An order placement or online catalog engine allows the buyer to place an order for a quantity of items at a stated fixed price, essentially ordering from an online catalog. The catalog contains the description and specification of the offerings. The catalog may be publicly accessible (Subtype 1a) or provided for a specific customer (Subtype 1b). Prices are included in the catalog but may be customer specific, may vary with quantity purchased, terms of delivery and performance (e.g. cheaper if not required immediately). The catalog can represent a single company's offering or an aggregate of the offerings from several companies. The catalog can range from a sales-oriented web site designed for viewing by customers, to a engine designed only accept orders sent via electronic data interchange (EDI). Note that the catalog can be shopper oriented (i.e. designed to sell) or a simple, machine-readable list of available items and prices. The following describes in more detail steps that can be executed to create an online catalog:

1. Enter and maintain a framework for catalog
    1.1. Enter / delete / edit categories. Categories are titles for groups of items, such as "furniture" or "solvents"
    1.2. Enter / delete / edit subcategories. Subcategories are categories within categories, effectively establishing a hierarchy of products. Example: furniture/dining room/tables.
    1.3. Create groups of categories and subcategories (e.g. "see also...."). The grouping allows a person browsing items to be referred to another category that may contains items of interest. For example, someone may reach the furniture/dining room/tables and then be referred to

Petitioner Apple Inc. - Exhibit 1026, p. 520

furniture/office/conference room tables where other suitable tables may be listed, or to furniture/dining room/chairs to buy chairs that make the table. This cross-referencing transforms the hierarchical arrangement of categories into a web.

2. Enter / edit / delete items in catalog by entering and updating the information listed below. The system allows users to enter this information and provides basic quality assurance.
   - 2.1. Catalog item number
   - 2.2. Supplier part number(s)
   - 2.3. Name of item
   - 2.4. Description
   - 2.5. Photos and drawings
   - 2.6. Specifications (depends on item type). Different items have different specifications. For example, a computer printer can have color vs. black and white, dots per inch resolution, paper size, etc. In contrast to a fixed, hard coded catalog, the specification section of the general purpose catalog engine the user prepares the specification section by selecting parameters from a list and then specifying a value for that parameter. The parameter list contains values such as length, width, height, voltage, color, resolution etc. It is can be extended by the manager of the auction environment. A lister selects a necessary parameter (e.g. length, then enter the value, such as 14"). The specification section is a concatenation of individual specifications.
   - 2.7. First available date
   - 2.8. Last available date
   - 2.9. Category (categories) into which the item fits
   - 2.10. Alternate suggestion(s) if product not available
   - 2.11. Related and associated products (e.g. printer supplies for a printer or other household items with the same pattern.
   - 2.12. Additional information at the option of the individual or organization listing the item.
3. Enter / update pricing information
   - 3.1. Simple price. The fixed prices is per item or per unit. The price must

Petitioner Apple Inc. - Exhibit 1026, p. 521

specify the

3.2. Pricing algorithm -- link to code for pricing algorithm

4. Take Orders

There are two variants: 4a: manual purchase in which a person browses a catalog and selects and item for purchase and 4b: automated order in which a purchase is initiated by an electronic message.

Variant 4a: Manual Purchase

4.1. Potential buyers access the catalog by drilling down through the category / subcategory tree or

4.2. Buyers search fields in catalog to identify the appropriate item. The search may examine the title, description, or any of the specification fields.

4.3. Display general information for item(s) meetings specifications

4.4. Allow user to modify search or to select specific item if the items displayed to do not meet his requirements

4.5. Display detailed information for selected item

4.6. Display the fixed price or calculate price if prices is based on an algorithm. The pricing algorithm may include parameter such as characteristics or affiliation of the users (e.g. affiliated with a pre-negotiated discount program) , delivery date and mode, and quantity.

4.7. Offer the option to purchase or search again if they choose not to purchase.

4.8. If the buyer opts to proceed with the purchase, then check the availability of the item by linking to the sellers inventory system

4.8.1. If the item is available then execute an 'add to basket'. That is, place it on a list of items designated for purchase.

4.8.2. If the item is not available, then execute the contingent response:

4.8.2.1. Offer delivery at predicted date

4.8.2.2. Terminate the sale, but offer to deliver or notify when next the item is next available.

4.8.2.3. Suggest alternate items

4.8.2.4. Report 'sorry' and abort transaction

4.9. Offer option to purchase addition options

4.9.1. If offer is accepted, execute from step 4.1

4.9.2. If offer is not accepted, proceed with step 4.10

Petitioner Apple Inc. - Exhibit 1026, p. 522

4.10. Conclude the transaction

4.10.1. Collect shipping information, offer options

4.10.2. Collect payment information

4.10.3. Validate payment

4.10.4. Summarize order

4.10.5. Obtain final authorization

4.10.6. Generate receipt

Variant 4b: automated order, done using an EDI (electronic data interchange) message

4.1 Accept requests for item

4.2 Return price and confirmation of availability

Note that users may conduct transactions without employing EDI. It is possible, however, for members to agree on a transaction EDI format either by completing a template within the system or selecting a pre-established EDI format from a library. This library can include formats developed by recognized standards organizations (e.g. UNEDIFACT or ANSI) or formats developed specifically for an industry or a trading environment. Once there is agreement on a format, transactions can be initiated, concluded, and confirmed through the exchange of appropriate EDI messages. As many commercial ordering, accounts payable, accounts receivable and enterprise resource planning systems have an EDI interface the collaborative environment should have the capability to forward the message to the order fulfillment system.

B. English Auction Transaction Engine

In an English Auction, a single item is offered for sale to many buyers. The auction can be open or limited to pre-qualified bidders. The buyers offer bids in turn, each succeeding all prior bids. The highest bid received at any point in the auction is visible to all buyers. The identity of the highest bidder may or may not be visible to traders. Buyers may increase their bids in response to this information. Award is to the highest bidder at the end of trading. The end of trading is reached when there are no higher bids during an interval that may be formally defined or determined by the manager of the auction at the time of execution.

There are two models for the access to the transactions. In the first model, all buyers and sellers are members of the group. In the second model, all sellers are

Petitioner Apple Inc. - Exhibit 1026, p. 523

members of the group, but buyers can include members and non-members. If non-members are allowed to buy, the creator the transaction must enter a new URL for buyers. This is a sub-URL of the main group URL. A registration process may be established for the buyer URL.

In live auctions (as opposed to online) all traders are connected at the same time, and the duration of the auction is brief – typically only a few minutes. In online trading, it is not necessary for all of the bidders to be present (i.e. connected at the same time). To distinguish between these two options they are designated (a) concurrent (everyone bidding at the same time) and (b) batch (not everyone connected simultaneously. The manager of the auction can set the minimum bid and the minimum increment.

1. The first step in conducting an auction is to collect information on the items being offered for sale. This is done online. The information collected includes:
    1.1. Identity of seller. Note that the business rules of the auction may require advance registration of sellers to verify their identity.
    1.2. Descriptions, optionally including attachments and photographs, independent certifications or appraisals, and anything else in digital form necessary or useful in determining the value of the item.
    1.3. Reserve price
    1.4. Minimum increment
    1.5. Time offered for sale
    1.6. Time bidding is scheduled to end
    1.7. Verify the seller's consent to the rules of the auction house regarding delivery, payment, responsibility for non payment, etc.
2. If the business rule of the auction house is to require payment up front, collect payment either by:
    2.1. Debiting a deposit account
    2.2. Charging to account for billing
    2.3. Collecting online payment such as through a credit card.
3. Post information about auction, including:
    3.1. Description of items to be auction
    3.2. Auctions rules:
        3.2.1. Qualification process for bidders

Petitioner Apple Inc. - Exhibit 1026, p. 524

3.2.2. Time of bidding

3.2.3. Criterion for ending bidding – time between bids

3.2.4. Legal statement – responsibilities of buyer and seller, limitation of liability

4. Execute qualification process (optional)

4.1. Admit bidders who are qualified based on past participation

4.2. Provide fill-in-the blank qualification form new bidders

4.3. Collect information

4.4. Conduct automated review or manual review

4.5. Inform prospective bidder of qualification or not

Variant (a): concurrent auction

5. Conduct Auction

5.1. Fifteen minutes prior to appointed time for auction, display "Welcome" screen with space for qualified bidder to enter an alias or handle to be used in the auction. Screen should have a description of the object. Show time until auction starts. Auto refresh at 15 second intervals.

5.2. At appointed time, display the main auction page with the following information:

5.2.1. Description / picture of item for auction stored in a separate, static frame of the PC so that it does not need to be downloaded each cycle.

5.2.2. Current bid (initially the reserve price)

5.2.3. Suggested next bid (e.g. current + 3 * increment)

5.2.4. Button to accept suggested next bid

5.2.5. Field to enter bid higher than suggested next

5.2.6. Handle of the highest bidder

5.3. Refresh main auction page at 15 second intervals

5.4. Collect bids, either

5.4.1. Notice that the suggested bid was accepted

5.4.2. Bid higher than accepted bid

5.4.3. If new bid is lower than current highest, disgard

5.4.4. If higher than current highest then

5.4.4.1. Log identity of highest bidder

5.4.4.2. Update highest bid

Petitioner Apple Inc. - Exhibit 1026, p. 525

5.4.4.3. Update next suggested bid

6. If nobody accepts the suggested bid, then

6.1. Reduce suggested next bid

6.2. If accepted, resume normal sequence

6.3. If not accepted, reduce suggested next bid

6.4. If accepted, resume normal sequence

6.5. If not, begin close

6.6. "Going once ...", if response, resume normal sequence, else

6.7. "Going twice ..." if response, resume normal sequence, else

6.8. Done. Display closing screen

7. Settle with winning bidder, two models

7.1. Connect buyer to seller for direct settlement

7.2. Collect money from buyer, deduct fee, convey amount to seller

Variant (b): batch (i.e. time limited) auction

Conventional on-line batch (time limited) auctions are common. E-bay is the most prominent example. This process description continues from step 4 of the English auction description as the startup of the concurrent and batch auctions are the same.

5. Conduct auction: Until closing time for an item:

5.1. On entry to system display the following for the potential buyer:

5.1.1. Latest listing

5.1.2. Categories

5.1.3. Search screen

5.2. On selection of categories:

5.2.1. Execute dill down

5.2.2. Retrieve count of items that meet criteria

5.2.3. If more count is less than 25 (or other small number (n) consistent with the layout of the screen) retrieve all items that meet criterion

5.2.4. If count is more than n, retrieve n auctions with nearest expiration time

5.2.5. Display link list to all items in list, sort order should be auction with nearest deadline to most distant

Petitioner Apple Inc. - Exhibit 1026, p. 526

5.2.5.1. Item name

5.2.5.2. Time till end of auction

5.2.5.3. Highest current bid

5.2.6. On user selection of the item, display same information as above plus

5.2.6.1. Description

5.2.6.2. Photo (if any)

5.2.6.3. Attachments (if any)

5.2.7. If count is more than n, display further drill-down options as well as item information above

5.3. Accept new bid through the display screen

5.3.1. Log bids in order, reject if bid is not higher than last high bid by increment.

5.3.2. If bid is rejected, tell bidder that their bid is not sufficient

5.3.3. Update database recording highest bid, bidder, time of bid

5.3.4. Display screen to user to confirm that their bid is the highest

6. When the time limit is reached, determine if a new bid has been received in the last 3 minutes (or other short time period). If so, extent the bidding time by 3 minutes (or other short time period) and execute step 5 with a new closing time.

7. When the time limit is reached, including all extensions under step 6, then

7.1. Email message to highest bidder that they won

7.2. Add transaction to completed deals

7.3. Update splash and add screens

7.4. Settle with winning bidder-- two models:

7.4.1. Connect buyer to seller for direct settlement

7.4.2. Collect money from buyer, deduct fee, convey amount to seller

C. Dutch Auction Transaction Engine

A Dutch auction, like a standard auction, involves the sale of a single item or batch with fixed specifications. There is one seller, and many potential buyers. The seller sets the prices, ideally higher than any buyer's maximum bid price. The offered price is reduced by a fixed increment at fixed intervals until a buyer accepts the price. The purchase goes to the first buyer in to accept the price. In the physical world (as opposed to the online world), Dutch auctions are rarely if ever run concurrently. In a live trading room, it could be difficult to determine which buyers

Petitioner Apple Inc. - Exhibit 1026, p. 527

was first to commit to a price when several are willing to pay the same amount. The Dutch auction is relatively simple to implement in an electronic environment. There are, at present, no online Ducth Auctions of which the inventors are aware.

1. Enter and maintain a framework for catalog
    1.1. Enter / delete / edit categories. Categories are titles for groups of items, such as "furniture" or "solvents"
    1.2. Enter / delete / edit subcategories. Subcategories are categories within categories, effectively establishing a hierarchy of products. Example: furniture/dining room/tables.
    1.3. Create groups of categories and subcategories (e.g. see also....). The grouping allows a person browsing items to be referred to another category that may contains items of interest. For example, someone may reach the furniture/dining room/tables and then be referred to furniture/office/conference room tables where other suitable tables may be listed, or to furniture/dining room/chairs to buy chairs that make the table. This cross referencing makes transforms the hierarchical arrangement of categories into a web.
2. Execute qualification process (optional)
    2.1. Admit bidders who are qualified based on past participation
    2.2. Provide fill-in-the blank qualification form new bidders
    2.3. Collect information
    2.4. Conduct automated review or manual review
    2.5. Inform prospective bidder of qualification or not
3. Collect information on items to be auctioned and owners, including
    3.1. Identity of seller
    3.2. Descriptions, optionally including attachments and photographs, independent certifications or appraisals, or other information necessary to establish the value of the tiem
    3.3. Categorization
    3.4. Starting price
    3.5. Increment, Interval for reduction
    3.6. Minimum price
    3.7. Obtain consent to rules (possibly as part of registration/qualification process)

Petitioner Apple Inc. - Exhibit 1026, p. 528

3.8. Collect to conduct auction if item is

3.9. Calculate time to take item off auction by determining the number of steps (intervals) necessary to reduce price from the starting price to the minimum

3.10. Record all of the above information in the Dutch auction database

4. Cull expired options

4.1. Search database periodically for items where current time is later than time to take item off auction (2.9)

4.2. Inform owner that item was not sold

4.3. Delete entry from database

4.4. Prompt for revised terms start of another auction, create new entry if user takes option

5. When the buyer enters the system display a list of high level categories, a prompt for search criteria, and/or a link to a search page. Allow user to drill down through categories or enter search parameters.

5.1. Retrieve count of items that meet criteria

5.2. If more count is less than 25 (or other small number (n) consistent with the layout of the screen) retrieve all items that meet criterion

5.3. If count is more than n, retrieve n auctions with nearest expiration time

5.4. Display link list to all items in list, sort order should be auction with nearest deadline to most distant

5.4.1. Item name

5.4.2. Time till end of auction

5.4.3. Current price:

5.4.3.1. Retrieve starting price (SP) and increment (I$)

5.4.3.2. Calculate number of intervals since start of auction (INT)

5.4.3.3. Determine price = SP – (INT * $)

5.5. On click, display same information as above plus

5.6. Description

5.7. Photo (if any)

5.8. Attachments (if any)

5.9. The display screen should include a button that allows the buyer to purchase the item at the selected price.

Petitioner Apple Inc. - Exhibit 1026, p. 529

6. When the user clicks the "buy" button
    6.1. Email message to highest bidder that they won
    6.2. Add transaction to completed deals database
    6.3. Settle with winning bidder-- two models:
        6.3.1. Connect buyer to seller for direct settlement
        6.3.2. Collect money from buyer, deduct fee if any for auction and payment services, convey the remainder to seller.

D. Reverse English Auction Transaction Engine

In a reverse auction, there are multiple buyers to one seller. Prices come down rather than up. There are many variants of a reverse auction. The variant discussed here is a reverse English auction. Reverse auctions have been implemented on line in Open Markets.

The process for posting an item for bid and for qualifying bidders is the same as for other auctions. The difference here is that the buyer may optionally set a maximum price.

1. Accessing the list of items sought
    Potential bidders access items sought by working through a hierarchy of categories and subcategories or entering search criteria, as for other auctions. A list of items within the category/subcategory and/or meeting the search criteria is displayed. The user may then
    1.1. Terminate the session on finding no suitable items
    1.2. Revise the search criteria
    1.3. Select an item on which to bid
2. If the user selects an item on which that may wish to bid, detailed information about the items is displayed. This item may include the following information:
    2.1. Name
    2.2. Seller
    2.3. Description
    2.4. Detailed specifications for items
    2.5. Delivery requirements
    2.6. Proposed terms
    2.7. Current low bid
3. If the user determines that they should bid, he accesses the bid entry screen from

Petitioner Apple Inc. - Exhibit 1026, p. 530

the detailed description in Step 2 above. Making a bid consists of entering the following information:

3.1. New, lower bid

3.2. Comments pertaining to any special terms, features, or conditions

3.3. Attachments containing relevant additional information and any certifications required by the buyer

4. On receipt of bid, there are two options – either all bids are accepted, or bids are accepted only after review of information by the buyer.

4.1. Case 1: all bids are accepted

4.1.1. New bid is checked to determine if it is lower than prior bid

4.1.2. If so, then

4.1.2.1. bidder is notified that their bid is currently the lowest

4.1.2.2. seller is notified of new low bid

4.1.2.3. bid database is updated

4.1.3. If not, then

4.1.3.1. Bidder is notified that their bid is not the lowest

4.1.3.2. Bid screen is displayed so that bidder may lower bid

4.2. Case 2: bids are accepted after review by buyer

4.2.1. Buyer is notified of bid via email or online message

4.2.2. Buyer accesses complete information on the proposed bid through the system

4.2.3. Buyer select accept bid or reject bid.

4.2.4. If bid is accepted, then

4.2.4.1. Bidder is notified that their bid is currently the lowest

4.2.4.2. Bid database is updated

4.2.5. If bid is not accepted, then

4.2.5.1. Buyer enters reason for not accepting bid

4.2.5.2. Bidder is informed that bid is rejected with reason stated above

4.2.5.3. Bidder may access the bid screen to revise offer

5. When time period has expired and there have been no bids within a short specified interval, then

5.1. If at least one bid less than the maximum has been received, then:

Petitioner Apple Inc. - Exhibit 1026, p. 531

5.1.1. Notify low bidder that their offer was successful

5.1.2. Add transaction to completed deals database

5.1.3. Settle with winning bidder-- two models:

5.1.3.1. Connect or introduce buyer to seller for direct settlement

5.1.3.2. Collect money from buyer, deduct fee if any for auction and payment services, and convey the remainder to seller.

5.2. If no bid less than the maximum has been received, the

5.2.1. Notify buyer

5.2.2. Allow buyer to revise bid criteria

E. Sealed Bid Transaction Engine

In a sealed bid system, the buyer publishes or distributes detailed, fixed specification to a number of potential bidders (who may or may not be prequalified). Bidders submit binding bids by a specified deadline, in a specific format that allows ready comparison. The competitive bidding process is distinguished from the bid and proposal process by the complexity of the specifications and the bids. In a simple competitive bid, competition among the bidders is along one or two readily quantified dimensions (always including price) and there is little or no room for variation in the form or specifications of the offering. Comparison of the bids is elementary.

The process for posting an item for bid and for qualifying bidders is the same as for other transactions as is the method to identify items on which to bid either using the hierarchy of categories and subcategories or a search engine.

1. If the user selects an item on which he may wish to bid, detailed information about the items is displayed. This item may include the following information:

1.1. Name

1.2. Seller

1.3. Description

1.4. Detailed specifications for items including all information necessary to prepare a bid

1.5. Bid instruction including specification for any documentation the buyer may required with a bid (e.g. proof of bonding or license)

1.6. Notice of any fees for bid registration

1.7. Delivery requirements

Petitioner Apple Inc. - Exhibit 1026, p. 532

1.8. Proposed terms

2. After review of the bid requirements, the user may choose not to bid or may enter a bid. The process for entering a bid consists of preparing a bid package, including the price offered and any necessary supporting documentation. This is done by completing an online form, with provision for attachments. The bid is submitted through the system where it goes into a database of bids that are not opened to the closing time for the bidding process.

3. At the closing time, all bid packages are conveyed to the buyer.

3.1. If there are no bids, the buyer is offered the opportunity to revise the request for bids.

3.2. If there are multiple bids, the buyer reviews the bids and selects the lowest priced qualifying bid. They buyer informs the seller and arranges payment and delivery in accord with the terms stated in the bid package.

F. Order Matching Transaction Engine

In an order-matching system there are many potential buyers. Each posts binding offer to buy (bid amount) or sell (asked amount). The process proceeds in real time. The order matching system constantly compares bid and asked and, when a match is found within a specified spread, the deal is concluded. No accepted offer can be repudiated, but offers may be withdrawn before a deal is consummated. The strike price is posted so that buyers and sellers can modify their offerings in real time. The items traded are fungible so that price is the only decision. For the market to operate efficiently the items traded must be tightly defined and the terms of sale must be fixed and determined in advance. This is typically done by the operation or an exchange, with the order-matching engine operating in the background. To insure that the items traded are well defined, and the terms of sale are rigid example of an order matching process in stock trading on an exchange.

Users of an order-matching engine are all potential buyers and seller. They are qualified in advance using a process like that outlined by for auction with the extension that deposit accounts are frequently required given the speed of transactions in exchange environments.

1. Establish and maintain items to be traded. All functions in this category are reserved to the manager of the exchange or a designee.

To add (i.e. "list" and idem), enter

Petitioner Apple Inc. - Exhibit 1026, p. 533

1.1. Unique item number or symbol

1.2. Description of item (e.g. Sears Class A Common Stock)

1.3. Terms and conditions ownership (e.g. who can own) if any

1.4. Trading units (e.g. shares, blocks, etc.)

1.5. Additional information as required by the rules of the exchange

To delete (i.e. "delist" and item)

1.6. Select the item to be deleted

1.7. Confirm deletion

2. On entry to the system, potential buyers and sellers can review the price of the last transaction of any item, either through a list or a search by item name or symbol. The current highest asked and lowest bid price are also shown.

3. An offer to sell is posted by entering the following information:

3.1. Item number or symbol

3.2. Quantity offered

3.3. Proposed price ("asked")

3.4. Seller

3.5. Offers may be revise at any time prior to consummation of a deal

4. An offer to buy is posted by entering the following information

4.1. Item number or symbol

4.2. Quantity offered

4.3. Proposed price ("asked")

4.4. Buyer

4.5. Offers may be revised at any time prior to consummation of a deal

5. Offers to buy and sell are constantly reviewed by the software. When there is an offer to buy and sell at a price within a preset difference. When prices match, buyers and sellers are notified of the transaction, and the transaction is recorded. The display of the last transaction price, the highest bid and the lowest asked price is updated.

6. The transaction is conveyed to the backend accounting system of the exchange.

G. Bid and Proposal

The bid and proposal process is typically used for procurement of large or complex products or services, in which cost is not the only factor. Cost must be weighed against the buyer's assessment of the quality and suitability of an offering

Petitioner Apple Inc. - Exhibit 1026, p. 534

and the ability of the bidder to deliver the product or perform the specified services.

The bid and proposal process is conducted between one buyer (possibly representing a consortium) and many potential sellers, sometimes organized into teams. The buyer issues specifications that may be general or highly specific, brief or very lengthy. The specifications may be distributed freely or to a list of qualified buyers.

With physical RFPs, the size and the associated cost of distribution make it common practice to advertise the availability of the RFP first, sending copies only to those that request it. Frequently, the requestors are required to supply information to establish their qualifications to bid. While cost is not an issue in electronic dissemination of RFPs, the model of advertising prior to distribution is still useful in managing the qualification process. This is addressed as variant (a) is this description. Variant (b) requires no prequalification.

In a competitive bid on fixed requirements (sealed bid or auction), there is typically very little communication between buyer and seller between publication of the request and submission of the bids. The requirements are comparatively simple, clear, and unambiguous. In contrast, the bid and proposal process may involve considerable communication between buyer and seller. The process may begin with a bidders' conference to answer questions about the requirements. Additional questions from bidders may be accepted, though not all need be answered. Questions and answers may be made available to all bidders or the response may be in private. This dialog is crucial for two reasons. First, it helps the bidders understand the requirements and to be responsive in their bids. Second, it is not unusual for the bidders' questions to identify some point of ambiguity, error, or contradiction in the specifications, leading to a modification of the RFP. The diverse perspectives of the bidders, and the close attention required on their part to prepare a bid inherently provides an excellent review of the RFP.

The initial phase of the RFP process concludes with submission of the bids, but this is far from the conclusion of the process. Commonly, questions arise from the review of the proposals. These may relate to a specific submission or have broader implications, leading to modification of the requirements. The list of bidders can be culled to the best candidates. These are asked to answer questions about their proposals and to provide additional and clarifying information.

Petitioner Apple Inc. - Exhibit 1026, p. 535

The process described here is built around the document repository described elsewhere in this application. Through this process of refinement, the list of bidders is narrowed to one or two with whom a contract is negotiated. The process of negotiation is addressed as a separate transaction type (Negotiation Engine) as it may be conducted without the bid and proposal process.

Variant (A): with pre-qualification

1. Software supports the user in creating a web site for the proposal process. Initially this site manages the process for requesting the request for proposal (RFP), qualifying bidders, and disseminating the RFP.
2. Supported by the system software, the bidder creates and RFP advertisement by
   2.1. entering a summary of the RFP.
   2.2. entering a summary of the information needed to qualify as a bidder or
   2.3. attaching a form (HTML web page or template for paper form) for entering qualifying information
3. The RFP advertisement includes file transfer software for uploading qualifying information to the repository.
4. Disseminate RFP advertising
   4.1. Post on public bulletin board or
   4.2. Disseminate via mail to selected users
5. When users access the system, issue them an encryption key and PIN to be used for subsequent uploads and communications to verify their identity.
6. Receive requests for RFP in repository
   6.1. Prompt for key
   6.2. Encrypt submission
   6.3. Upload
   6.4. Generate receipt – should include an authentication number
7. Disseminate RFP to selected user, either:
   7.1. Attach to return Email or
   7.2. Post the RFP in a repository from which qualified prospective bidders may download the file. If the repository model is used, provide notice of the posting via email including any necessary PINs and codes to access the repository
   7.3. When a prospective bidder downloads an RFP, issue an encryption key to be

Petitioner Apple Inc. - Exhibit 1026, p. 536

used in submitting proposal

8. The RFP site also includes a page through which prospective bidders can submit questions. Questions and answers are posted to the site.
9. Updates to the schedule and amendments to the RFP are posted to the site
10. All access to the site is recorded to verify that prospective bidders have received critical information. Direct contact may be used when it is determined that a bidder had not accesses the site since critical new information was posted.
11. Bidders prepare their proposal and then upload them to a repository for proposals using software built into the proposal site.
    - 11.1. Prompt for key
    - 11.2. Encrypt submission
    - 11.3. Upload
    - 11.4. Generate secure hash number to prevent tampering with the submission
    - 11.5. Generate receipt including secure hash number and authentication code
12. After initial proposals are received, the process moves into a phase commonly termed the "best and final process" in which the proposals are reviewed, the list narrowed, and the proposals refined.
    - 12.1. Create separate secure environment (i.e. web site with repository) for each respondent
    - 12.2. Exchange materials through repository (described elsewhere in this filing)
    - 12.3. Records and receipt each access
    - 12.4. Generate key for revised proposal
    - 12.5. Receive proposal using process in 11
    - 12.6. Repeat from step 11 as many times as necessary

The remainder of the process is completed as a negotiated deal, described below.

Variant B: no pre-qualification:

Proceed as above, beginning with Step 6 and not requiring a key for download of the RFP.

Petitioner Apple Inc. - Exhibit 1026, p. 537

H. Negotiation Deal Engine

An engine for negotiating a deal can be built around the capability of the system to create a temporary virtual private network through the web. A temporary network is created for the negotiation. Access to the network is limited to the parties of the negotiation, their advisors and counsel, and, potentially, arbitrators and regulators. The members of the negotiating environment have access to the complete set of tools described in this filing including those for communications (email, anonymous mail, online chat, threaded dialogs, and audio and video collaboration), the library of standard contract instruments, the tools for document signature and authentication, and the document repository. Using these tools in a secure environment they can negotiate, close, and register a deal.

FIG. 19 shows one possible user interface for selecting participation engines to be made available to group members. The term "participation engine" refers generally to collaboration tools that provide features beyond merely communicating among group members. Various services such as an on-line survey tool, a DELPHI model tool; brain writing tool; and real-time polling can be provided.

A. Online Survey

In online polling or surveying, the person creating the poll uses and automated tool (new to this application) to build simultaneously an online questionnaire and a database to collect the results. The user builds the questionnaire by entering a series of questions and an associated data collection widget for each. The polling tool builds the database and the data entry screen. The data entry screen consists of two columns. The left column is a series of questions. The right column is the data entry tool appropriate to the question. Various data entry tools can be provided to respond to the query, including such things as:

1. yes / no radio buttons
2. true / false radio buttons
3. slider with scale from 1-5, 1-10, etc.
4. fill-in-the-blank text box
5. numeric field
6. multiple check boxes (e.g. strongly disagree, disagree, agree, strongly agree)

Other data entry types may be added.

Petitioner Apple Inc. - Exhibit 1026, p. 538

As each question / data collection widget is added, the polling tool creates the database. The database includes one record per data collection form. Creating the database structure simply means adding one new field to each record definition for each question. The type of data collection widget defines the format of the field, as follows:

1. yes / no radio buttons: one character field, limited to "y" or "n"
2. true / false radio buttons: one character field, limited to "y" or "n"
3. slider: real number field, with appropriate range check
4. fill-in-the-blank text box: text box
5. numeric field: real number or integer
6. multiple check boxes: integer field with range check from 1 to number of boxes

Every data entry screen provides a "save" and "cancel" button. Save writes to the database. Cancel exits the entry screen without saving.

The survey, once composed as described above exists as a web page. This page can be embedded in web applications. It can be made available on a site available to the entire Internet, on an Intranet, or in a dynamically created environment. Alternatively, it can be distributed via e-mail. When the form is completed, the submit button transmits the value entered to the database that is created at the time the form is generated. Access to the database is controlled by the rules of the database system. It may be limited to the individual who creates the survey form and database, but it may be accessible other users in the survey developers organization, as determined by the database administrator. Distribution of the result of the analysis is at the discretion and control of the individual managing the survey. This manager may be the individual who creates the survey, but the actual creator may be acting on behalf of the survey manager. Results may be kept private, posted to the Internet, and intranet, or a collaborative environment, distributed via e-mail within an organization, or, if the information is available, sent via e-mail to the participants in the survey.

B. Online Delphi Engine

The online Delphi engine allows real-time collaboration in estimating or predicting an outcome that can be expressed numerically. For example, the method can be used to develop a consensus forecast of grain prices. The method has been

Petitioner Apple Inc. - Exhibit 1026, p. 539

in used since the 1970s, but has not previously been adapted to online processes. One possible method is as follows:

1. Establish the session
    1.1. Within an online community, the moderator of the session creates the brain writing session by entering the following information:
        1.1.1. Name of moderator
        1.1.2. Title of the session
        1.1.3. Description of the session
        1.1.4. Background reading as references or attachments
        1.1.5. Start date for the session
        1.1.6. Scheduled end for the session
        1.1.7. Access to the session:
            1.1.7.1. URL for access
            1.1.7.2. Open to all or invitees only for observation
            1.1.7.3. Open to all or invitees only for participation
        1.1.8. Payment information if required
2. Optionally, the session may be advertised on line
3. If the session is private, invitations with logon keys must be distributed via email, actual mail, or download.
4. Optionally, the moderator may run on online applications and qualification process
5. Prior to the start of the session, the moderator must describe precisely the value to be estimated. The definition must be completely unambiguous.
6. Each participant connects at the start of the session. On connecting, they question is posed (e.g. "What will be the price of West Texas intermediate oil in December?")
7. Each participant enters a number a brief (1 paragraph maximum) explanation of their reasoning.
8. When the participant is done entering their estimate, they click "Done".
9. Each participant's estimate and explanation is recorded.
10. Each participant then sees the summary screen.

Petitioner Apple Inc. - Exhibit 1026, p. 540

11. Estimates are arrayed graphically from top to bottom of the screen, from lowest to highest. The value is stated as is the associated comment, but the source of the comment is not revealed.
12. Participants can review the estimates and comments, send an anonymous message to the author or any comment, or amend their answers.
13. The session terminates when the time expires, or when the moderator determines that there it is no longer appropriate to continue. The operator may determine this is based on declining participation or, if participation is high, the moderator may extend the deadline.
14. Participants and observers may access the final display of estimates, again arrayed from top to bottom, lowest to highest.

C. Brain Writing

Brain writing is a variant of a method for facilitated group discussion termed brainstorming. The objective of brainstorming is to maintain the focus of the discussion while encouraging creative input and recognizing the contributions of all members of the group. It seeks to avoid problems with a few individuals dominating the discussion, with junior staff deferring to senior staff, and with new ideas being abandoned before than can be developed fully. Brain storming has been commonly used since the late 1960s. Brain writing is a more intense method that relies on joint writing rather than discussion. What is presented here is adaptation of that method to an online environment. It is believed to be the first such adaptation.

1. Establish the session
    1.1. Within an online community, the moderator of the session creates the brain writing session by entering the following information:
        1.1.1. Name of moderator
        1.1.2. Title of the session
        1.1.3. Description of the session
        1.1.4. Background reading as references or attachments
        1.1.5. Start date for the session
        1.1.6. Scheduled end for the session
        1.1.7. Access to the session:
            1.1.7.1. URL for access
            1.1.7.2. Open to all or invitees only for observation

Petitioner Apple Inc. - Exhibit 1026, p. 541

1.1.7.3. Open to all or invitees only for participation

1.1.8. Payment information if required

2. Optionally, the session may be advertised on line
3. If the session is private, invitations with logon keys must be distributed via email, actual mail, or download.
4. Optionally, the moderator may run on online applications and qualification process
5. Prior to the start of the session, the moderator must list some number (typically 5-10) of questions or hypotheses to be explored. (e.g. " Our company should create a spinoff to develop and commercialize the new breast cancer vaccine") This may be done by the moderator alone, in consultation with the participants, or with other outside the session.
6. Each question or hypothesis becomes a "Card".
7. Participants may enter the session any time after the start. A password may be required if the session is not open.
8. On entry into the system, a user if given a card at random. The card consists of the initial question or hypothesis plus all comments entered on the card by other participants.
9. After reviewing the card, the participant may add his or her own comments to the bottom. After entering comments, the participant clicks "Done" to return the card to the pile.
10. When a participant returns a card to the pile, they received another card, chosen at random (preferably) or selected by the user. This process continues until the opt to exit. They may reenter at any time up to the conclusion of the session.
11. When a card is returned to the pile, it is become available for assignment to the next participant. The card includes the additions of the most recent participant.
12. A participant may opt to return the card without addition if he or she has nothing to add.
13. Participants may create new cards when new ideas come to mind. These are treated in exactly the same way as original cards.
14. Observers may view any card but may not add to them.
15. The moderator may limit participation to a set number at any time so that there is a sufficient number of cards to keep the participants fully occupied.

Petitioner Apple Inc. - Exhibit 1026, p. 542

16. The session terminates when the time expires, or when the moderator determines that there it is no longer appropriate to continue. The operator can determine this based on declining participation or, if participation is high, the moderator may extend the deadline.

17. The raw cards are distributed at the conclusion to all participants. The moderator or another individual is charged preparing a summary and arranging follow-up.

FIG. 22 shows one possible scheme for storing brain card writing data elements. In accordance with one embodiment, each brain writing card comprises a data structure including the following elements:

1. Brain writing session number: Serially assigned number to differentiate brainwriting sessions. A session is the set of all cards pertaining to a particular topic.
2. Card number: A Serially assigned sequence number
3. Initial Comment : The question or comment used to initiate the discussion (e.g. "SAIC should purchase a company that produces Internet server software"
4. Date and time card started
5. Date and time card closed
6. Comments: A collection (i.e. a set of unlimited length) containing the comments added by participants in the brainwriting session.
7. Date of additional comment: Date and time that each additional comment was added.
8. Commenter: Name or user ID of the person adding each additional comment. Ideally, brainwriting should be anonymous to encourage open dialog. Accordingly, this field may be omitted from an implementation. Some organizations, however, may wish to track this information without making it visible to users, or in some cases to attribute comments.

When the user has finished defining the group and specifying its functions, environment generator 1201a (FIG. 12) creates an environment accessible to the group members and including the functions specified during the environment definition process. As shown in FIG. 20A, for example, a web page can be created for the newly created environment, including those functions that were selected by the user that created the group. All group members are notified of the existence and

Petitioner Apple Inc. - Exhibit 1026, p. 543

location of the environment, and each group member can use the functions provided in the environment to collaborate on a project or conduct business.

FIG. 20B shows what an environment might look like to a group member after entering the environment. As shown in FIG. 20B, for example, a news banner announces the latest news for the group. Additionally, specific communication tools, research tools, transaction engines, and participation engines are made available to group members, which can be executed by appropriate mouse clicks in accordance with the inventive principles. According to various inventive principles, each tool shown on the web page is accessible through a hyperlink to a web-based program that performs predefined functions as set forth above. For example, clicking on "online catalog" would link the group member to a web page that implements an online ordering engine as described previously. Users can navigate through the various tools using conventional web browser features (i.e., forward, backward, etc.). It may be desirable to implement some or all of such software using server-side scripting or other similar means consistent with the system configuration of FIG. 12.

FIG. 21 shows how environment generator 1201a can create multiple environments including virtual private facilities, which can be implemented through web pages that contain hyperlinks to functions available to members of each group or environment. An environment definition software component 2106 implements steps 1101 through 1103 of FIG. 11 in order to create one or more environments 2107. (In one embodiment, each group can also be provided with a copy of an environment generator 2106 in order to create sub-groups that draw on the applications and directory structure created for the group). As a user identifies group members and selects functions to be provided for the environment in which the group will collaborate, environment definition component 2106 stores information relating to the selected members and functions in databases. Each environment can include a web page (not shown in FIG. 21) and directories, tools and other applications specific for each created group.

Based on user selections of the type illustrated in FIGS. 13 through 19, environment generator 2106 creates an environment 2107 containing one or more web pages with links to the selected tools. Environment generator 2106 retrieves information from various information sources including a directory of communication tools 2101 (e.g., including descriptions of tools and URL/IP

Petitioner Apple Inc. - Exhibit 1026, p. 544

addresses of web applications to set up each communication tool); directory of transaction engines 2102 (e.g., including descriptions of transaction engines and the URL/IP addresses of web-based applications to set up each transaction engine); directory of research tools 2103 (similar to above); list of global data objects 2104 (e.g., a dictionary of data elements from which the directory of each group can be composed); and a directory of applications 2105 (e.g., a description of available applications and URL/IP addresses of pages to set up access to applications).

Petitioner Apple Inc. - Exhibit 1026, p. 545

WE CLAIM:

1. A method of negotiating a deal over a network of computers, the network including at least one or more computers connected to the Internet, the method comprising the steps of:

(1) posting, on an electronic list that can be viewed over the Internet, information regarding one or more offers to form a contract;

(2) posting on the electronic list one or more responses to the one or more offers;

(3) researching the one or more responses to determine whether they satisfy one or more contract criteria;

(4) negotiating over the network between at least two parties to accept or modify one or more of the responses; and

(5) electronically signing a document to consummate the contract.

2. The method of claim 1, wherein step (1) comprises the step of displaying offers and responses in a parent-daughter spatial relationship on a computer display.

3. The method of claim 1, further comprising the step of sorting the one or more offers and one or more responses according to a user-selected sort order.

4. The method of claim 1, wherein steps (1) and (2) are done anonymously, such that each party to the contract cannot determine the identity of the other party to the contract.

5. The method of claim 4, further comprising the step of simultaneous revealing the identity of each party prior to step (5).

6. The method of claim 4, wherein steps (1) and (4) comprise the step of sharing a single anonymous e-mail alias among a plurality of users.

7. The method of claim 1, further comprising the steps of:

(6) registering keywords with an electronic agent that monitors the one or more offers and providing an e-mail address to be notified upon a keyword match; and

(7) in response to the electronic agent detecting the keyword match, transmitting a message to the e-mail address provided in step (6).

8. The method of claim 1, wherein step (2) comprises the step of clicking on a hyperlink linking the information posted in step (1) to a reply card.

9. The method of claim 7, wherein step (2) comprises the step of requiring

Petitioner Apple Inc. - Exhibit 1026, p. 546

the submission of certain information before the reply card will be accepted.

10. The method of claim 1, wherein steps (3) and (4) are performed a plurality of times for a single contract, such that modifications are made to the one or more responses.

11. The method of claim 1, further comprising the step of electronically registering a plurality of entities that have signatory authority and correlating the registered entities with one or more documents to which signatures can be affixed.

12. A method of displaying information on a computer display, comprising the steps of:

(1) displaying a first plurality of graphical objects each having a shape of a file folder comprising a folder face and a labeled tab, wherein the first plurality of graphical objects are stacked in a cascading arrangement; and

(2) in response to user activation of a "flip" tab, changing the graphical objects displayed in step (1) to show a second plurality of graphical objects each having a shape of a file folder comprising a folder face and a labeled tab,

wherein each of the first and second plurality of graphical objects can be brought to a foreground position in front of other graphical objects by clicking on a corresponding labeled tab.

13. The method of claim 12, wherein each of the first and second plurality of graphical objects has associated therewith one or more functions displayed on the folder face thereof, wherein user can activate the one or more functions by clicking thereon.

14. A method of creating a user-defined networked environment across a plurality of computers without requiring system administrator-level privileges, comprising the steps of:

(1) creating a group by providing a group identifier, a group description, and by specifying a plurality of group members entitled to use the user-defined networked environment;

(2) selecting a plurality of web-based communication, collaboration, and transaction tools from a list of available tools, wherein the selected tools are to be made available to the plurality of group members specified in claim 1; and

(3) through the use of computer software, automatically creating the user-defined networked environment by creating a web page accessible to the plurality

Petitioner Apple Inc. - Exhibit 1026, p. 547

of group members selected in step (1), wherein the web page provides access to the plurality of tools selected in step (2).

15. The method of claim 14, wherein step (1) comprises the step of inviting a plurality of individuals to join the group by transmitting an invitation to prospective group members.

16. The method of claim 14, wherein step (1) comprises the step of advertising an invitation to join the group by posting an advertisement for prospective group members, wherein at least some of the prospective group members are unknown to the user creating the networked environment.

17. The method of claim 14, further comprising the step of screening prospective members that respond to the advertisement in order to determine whether they should be added to the group.

18. The method of claim 14, further comprising the steps of electronically collaborating among group members using the user-defined networked environment.

19. The method of claim 14, further comprising the step of destroying the user-defined networked environment when it is no longer needed.

20. The method of claim 14, wherein step (2) comprises the step of selecting a transaction engine that implements an auction to members of the group.

21. The method of claim 14, wherein step (2) comprises the step of selecting a transaction engine that implements an on-line electronic survey comprising survey questions that are to be answered electronically by survey participants.

22. The method of claim 14, wherein step (2) comprises the step of selecting a transaction engine that implements a bid-and-proposal tool that permits group members to electronically submit bids on one or more proposals.

23. The method of claim 14, wherein step (2) comprises the step of selecting an online ordering engine that permits group members to electronically order goods or services in the user-defined networked environment.

24. The method of claim 14, wherein step (2) comprises the step of selecting an Electronic Data Interchange (EDI) compatible interface that executes electronic commercial transactions between two or more group members.

Petitioner Apple Inc. - Exhibit 1026, p. 548

25. The method of claim 14, wherein step (2) comprises the step of a selecting an electronic brain-writing tool that permits participants to brainstorm using electronic idea cards.

26. A system for implementing a user-defined networked environment that can be created without the need for system administrator-level privileges, comprising:

a plurality of networked computers that communicate using Internet Protocol;

a plurality of web browsers executing on the plurality of networked computers;

a database that stores information concerning the user-defined networked environment; and

a computer program executing on one or more of the plurality of networked computers, wherein the computer program performs the steps of:

(1) permitting a user to create a group comprising a plurality of group members;

(2) permitting the user to select a plurality of web-based communication, collaboration, and transaction tools from a list of available tools, wherein the selected tools are to be made available to the plurality of group members; and

(3) automatically generating a web page accessible to the plurality of group members, wherein the web page provides access to the plurality of tools selected in step (2) to the plurality of group members.

Petitioner Apple Inc. - Exhibit 1026, p. 549

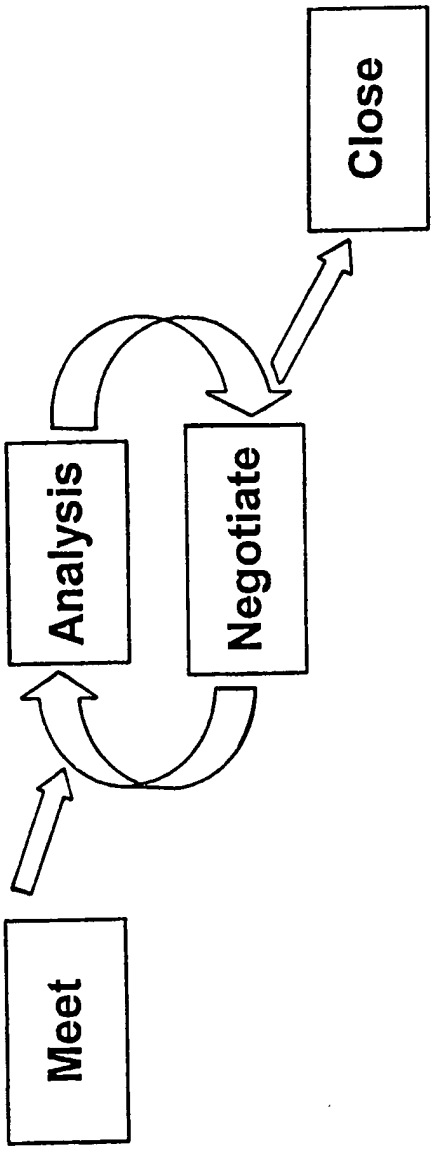


FIG. 1A

Petitioner Apple Inc. - Exhibit 1026, p. 550

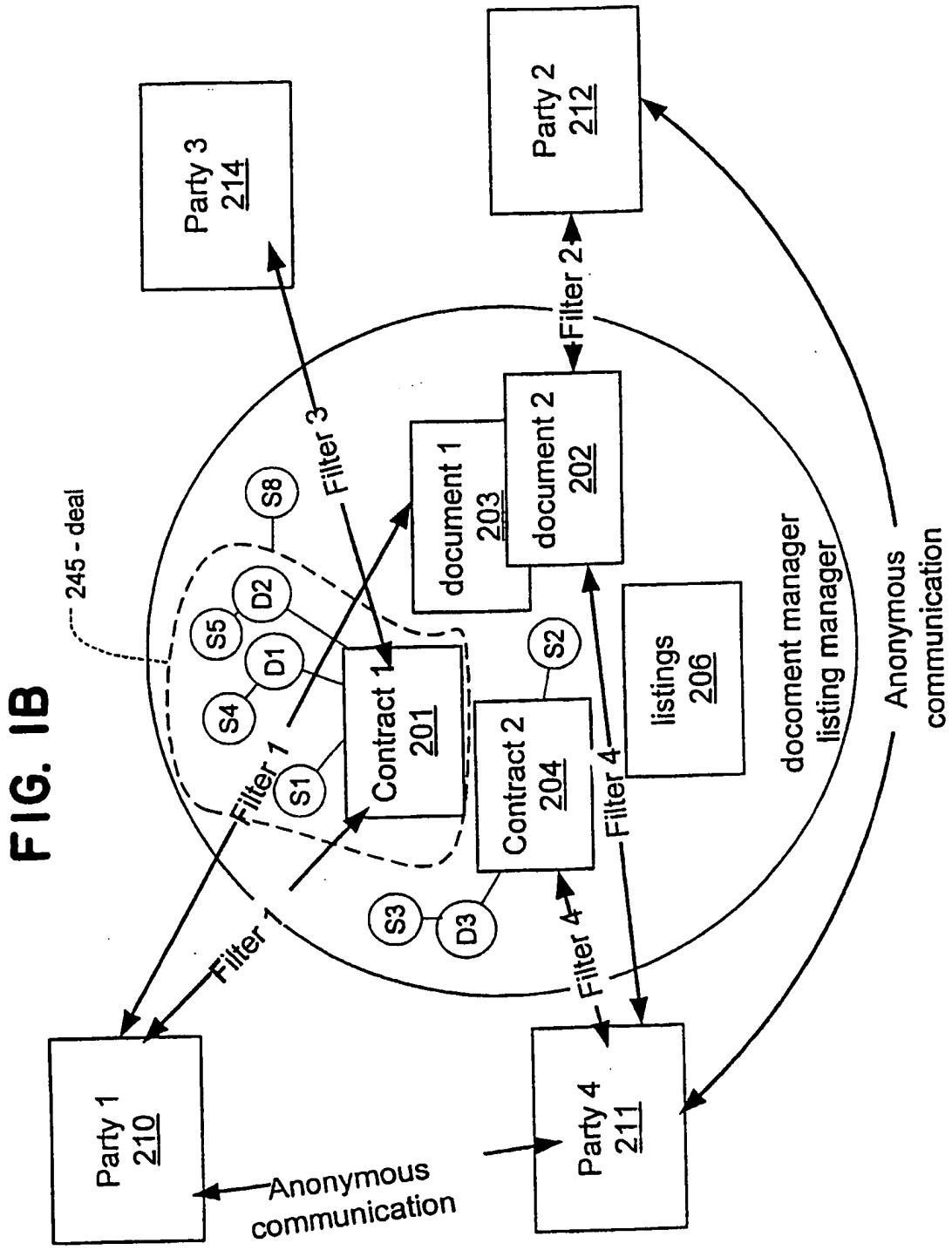
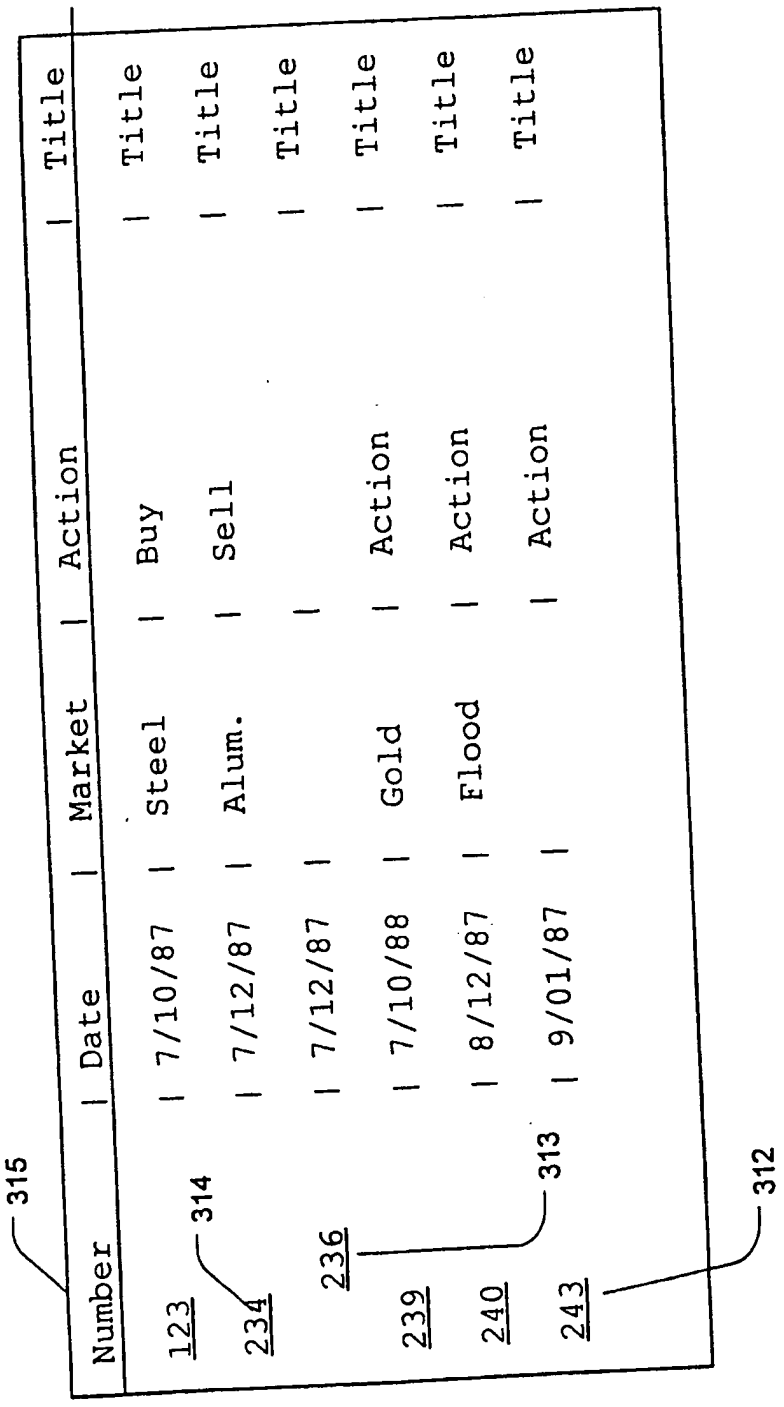


FIG. 1B

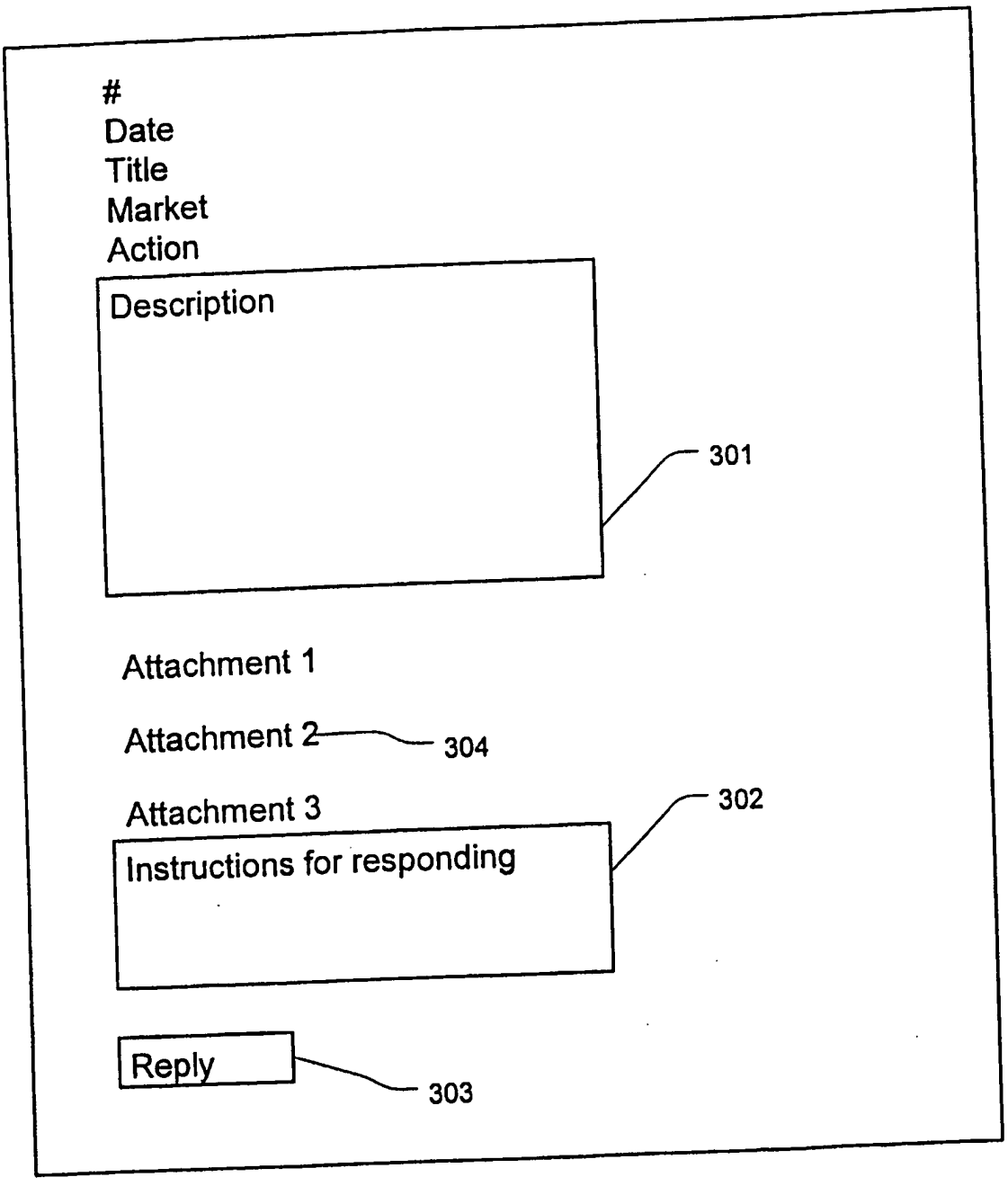
Petitioner Apple Inc. - Exhibit 1026, p. 551

FIG. 2



Petitioner Apple Inc. - Exhibit 1026, p. 552

FIG. 3



Petitioner Apple Inc. - Exhibit 1026, p. 553

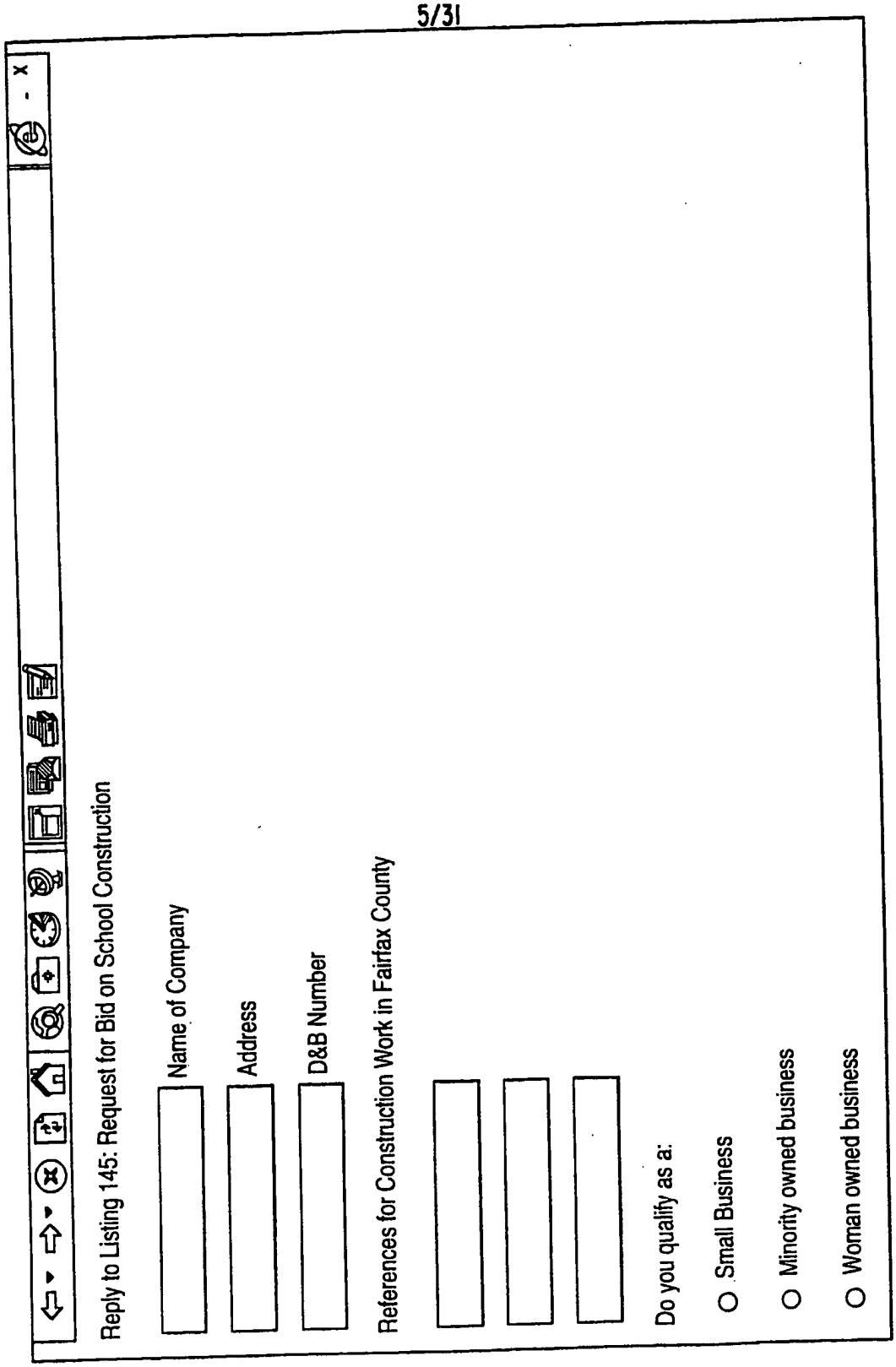


FIG. 4

Petitioner Apple Inc. - Exhibit 1026, p. 554

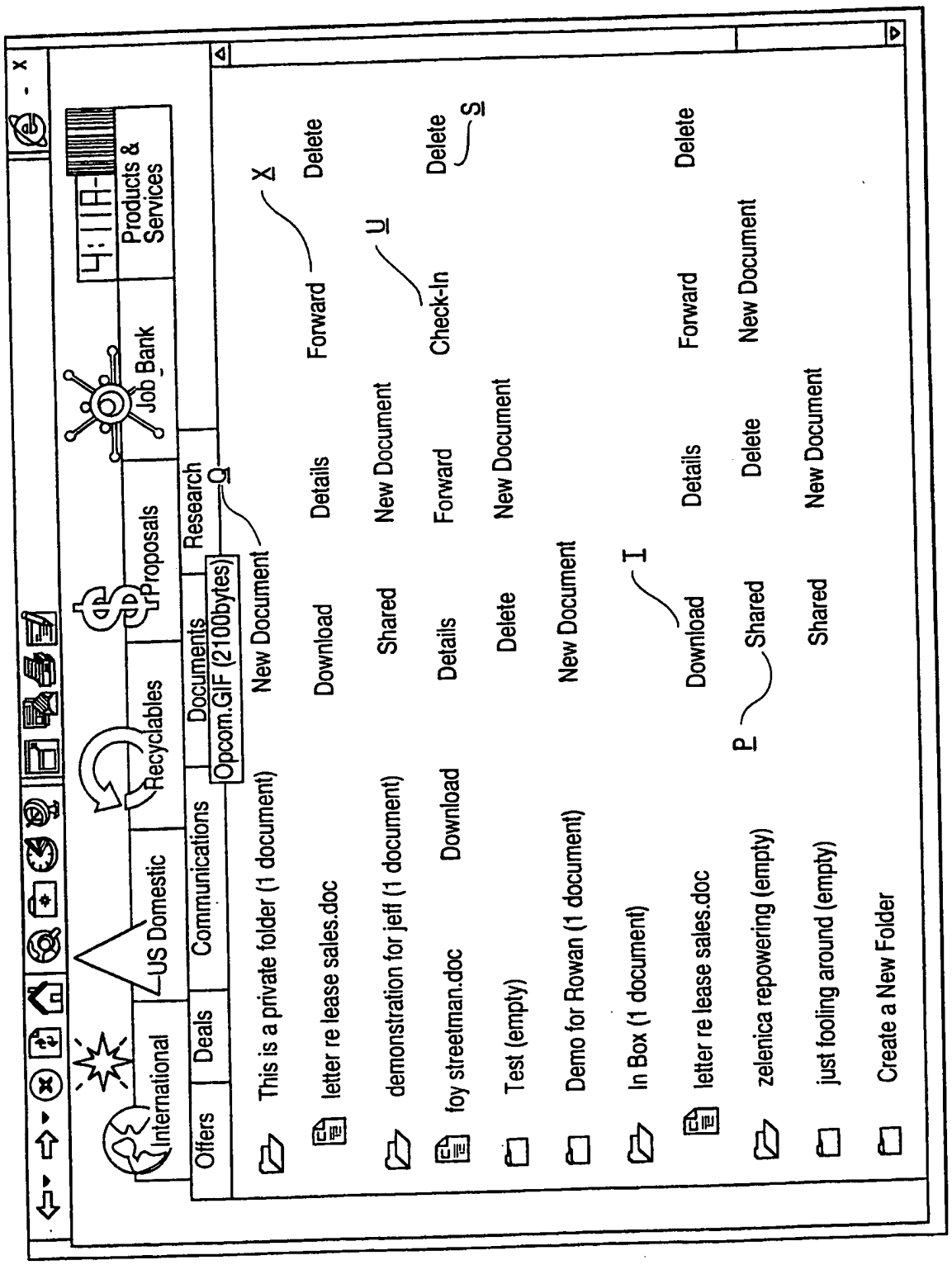


FIG. 5

Petitioner Apple Inc. - Exhibit 1026, p. 555

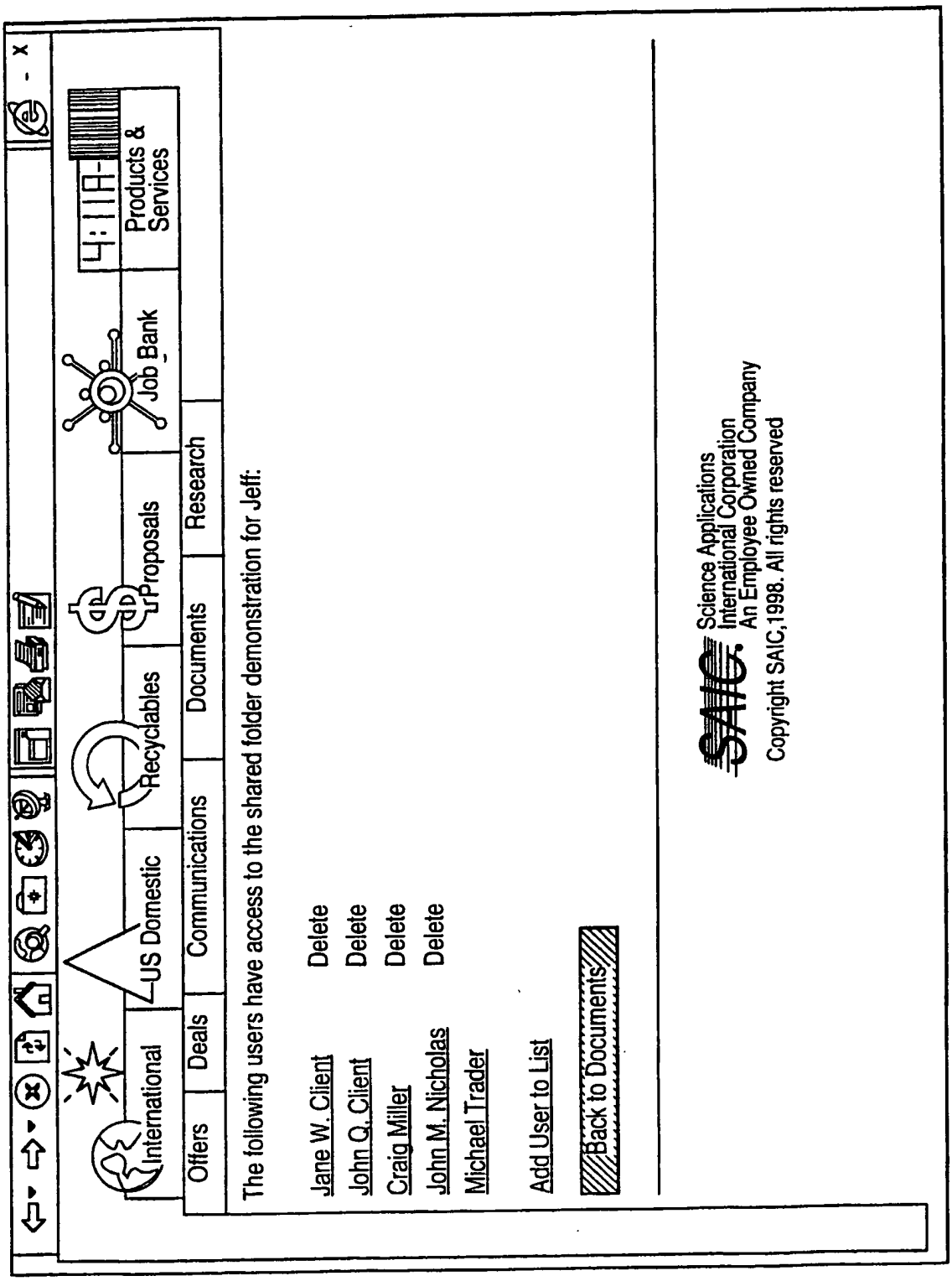


FIG. 6

Petitioner Apple Inc. - Exhibit 1026, p. 556

FIG. 7

Trade Number	Date Created	Trade Title
357	Sep 22 1998	mmmmmmmmmm
356	Sep 22 1998	World Trade Center
353	Sep 22 1998	Florida Windstorm Coverage
352	Sep 22 1998	vvv
342	Sep 1 1998	Bigger deal
341	Sep 1 1998	big deal
330	Aug 18 1998	Another trade
297	Jun 23 1998	xgsgs
295	Jun 23 1998	lkjdalskjd
293	Jun 23 1998	Test again
292	Jun 23 1998	Test of compiled tm
6	Feb 11 1998	Get in shape
5	Feb 10 1998	Big Deal
4	Feb 8 1998	Master Contract

SAIC Science Applications International Corporation An Employee Owned Company

Copyright SAIC,1998. All rights reserved

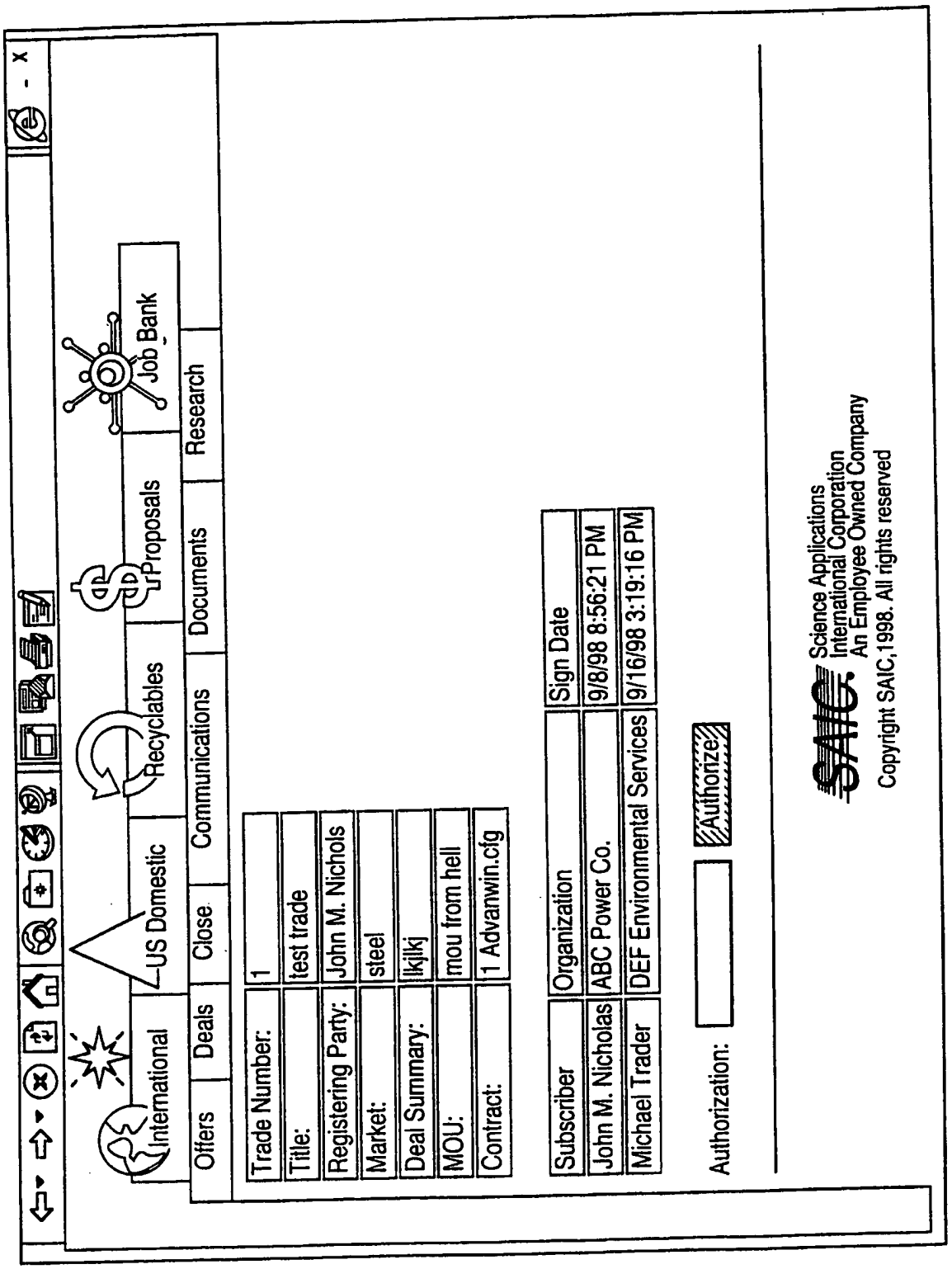


FIG. 8A

Petitioner Apple Inc. - Exhibit 1026, p. 558

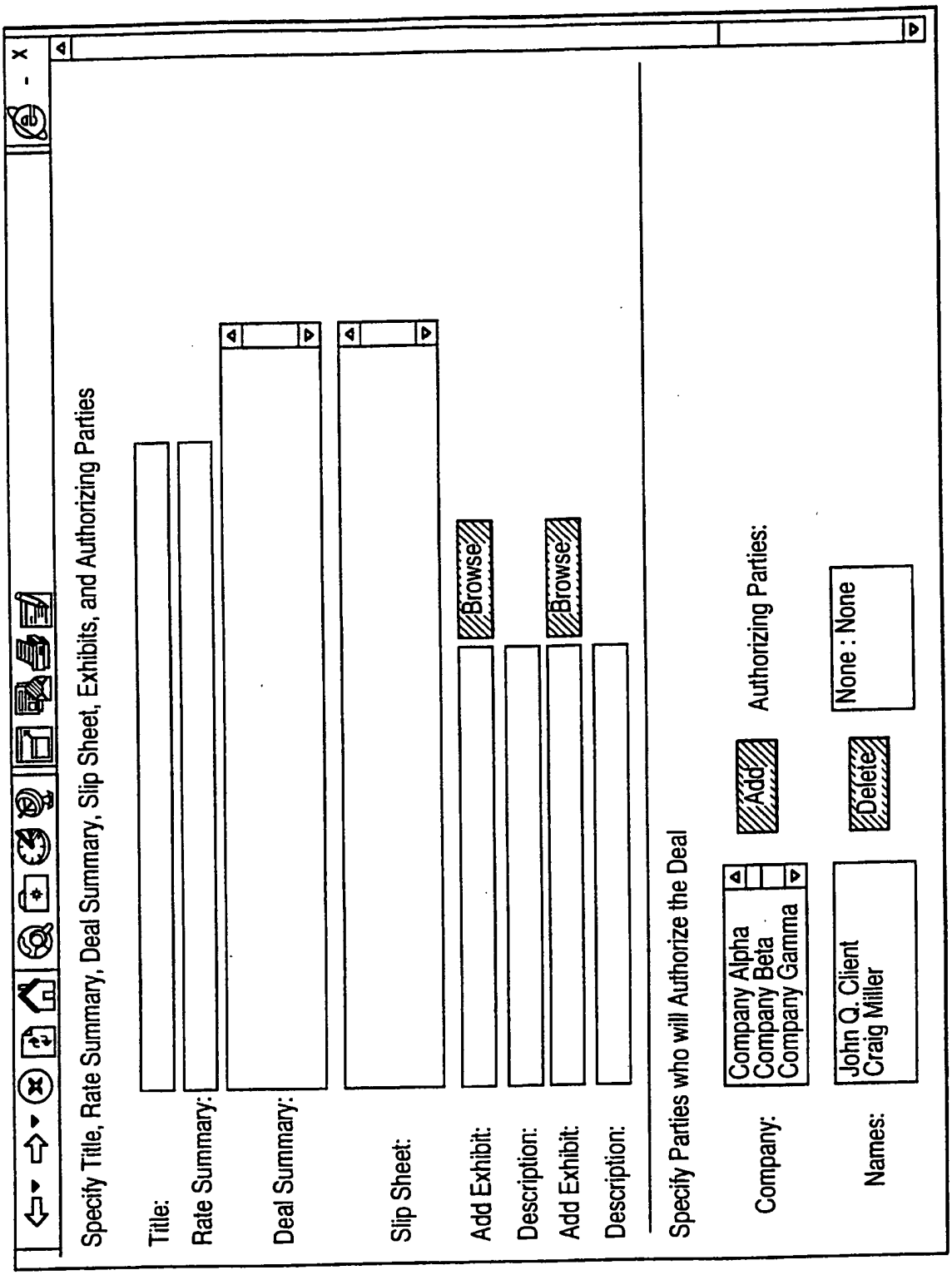


FIG. 8B

Petitioner Apple Inc. - Exhibit 1026, p. 559

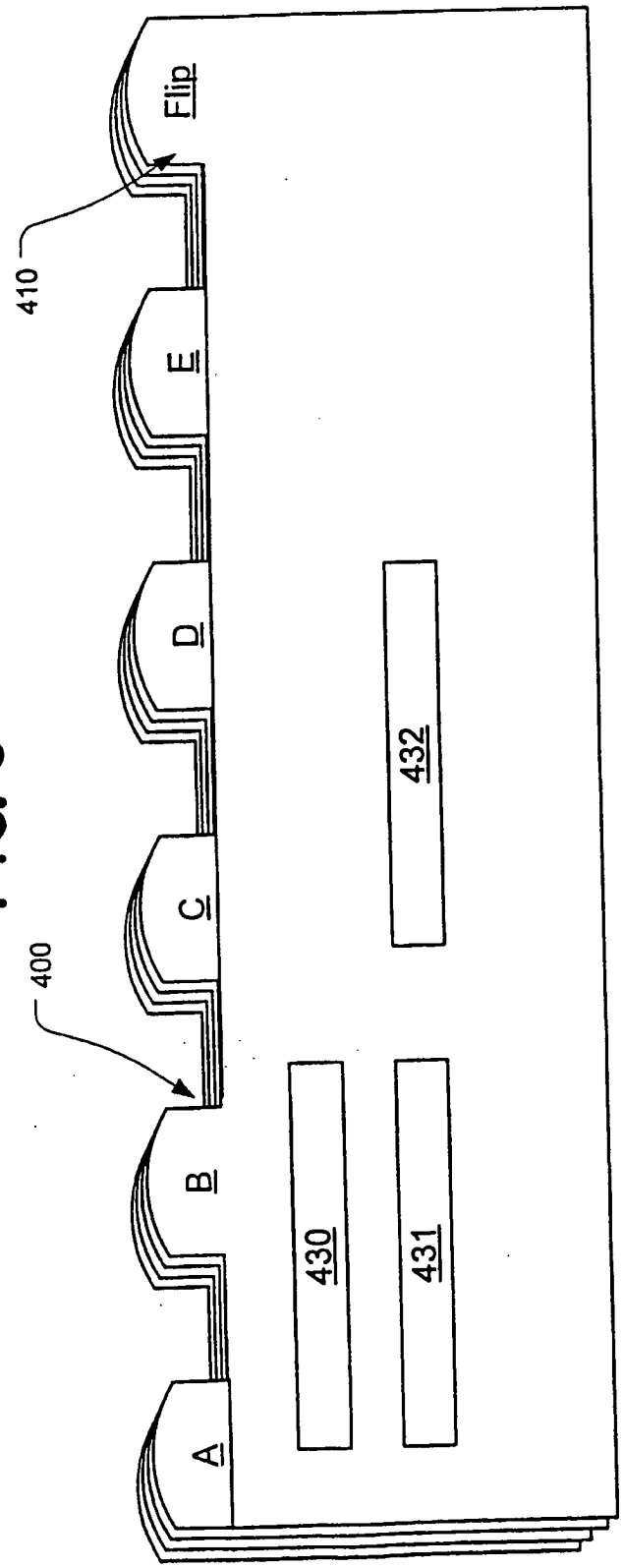


FIG. 9

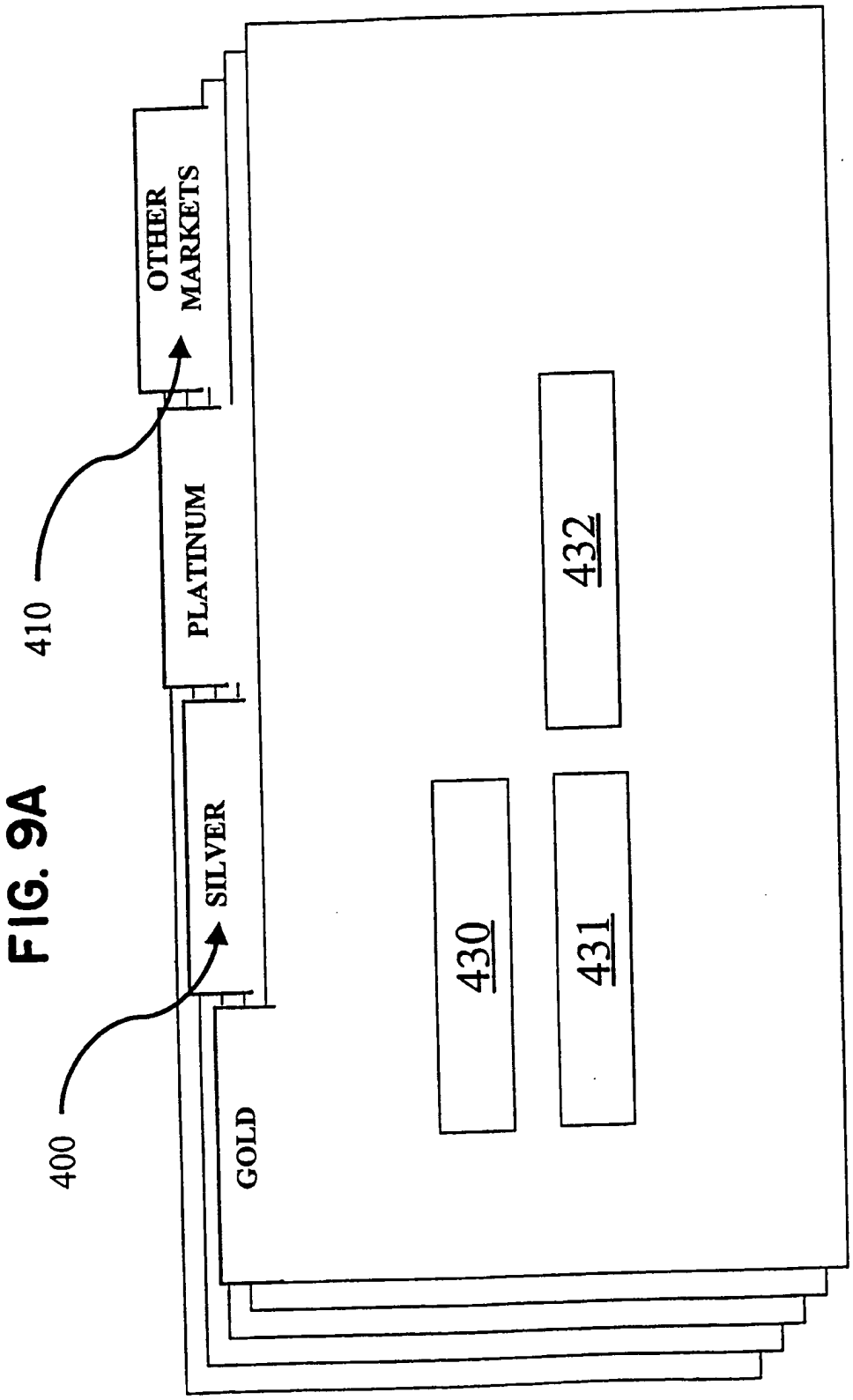


FIG. 9A

Petitioner Apple Inc. - Exhibit 1026, p. 561

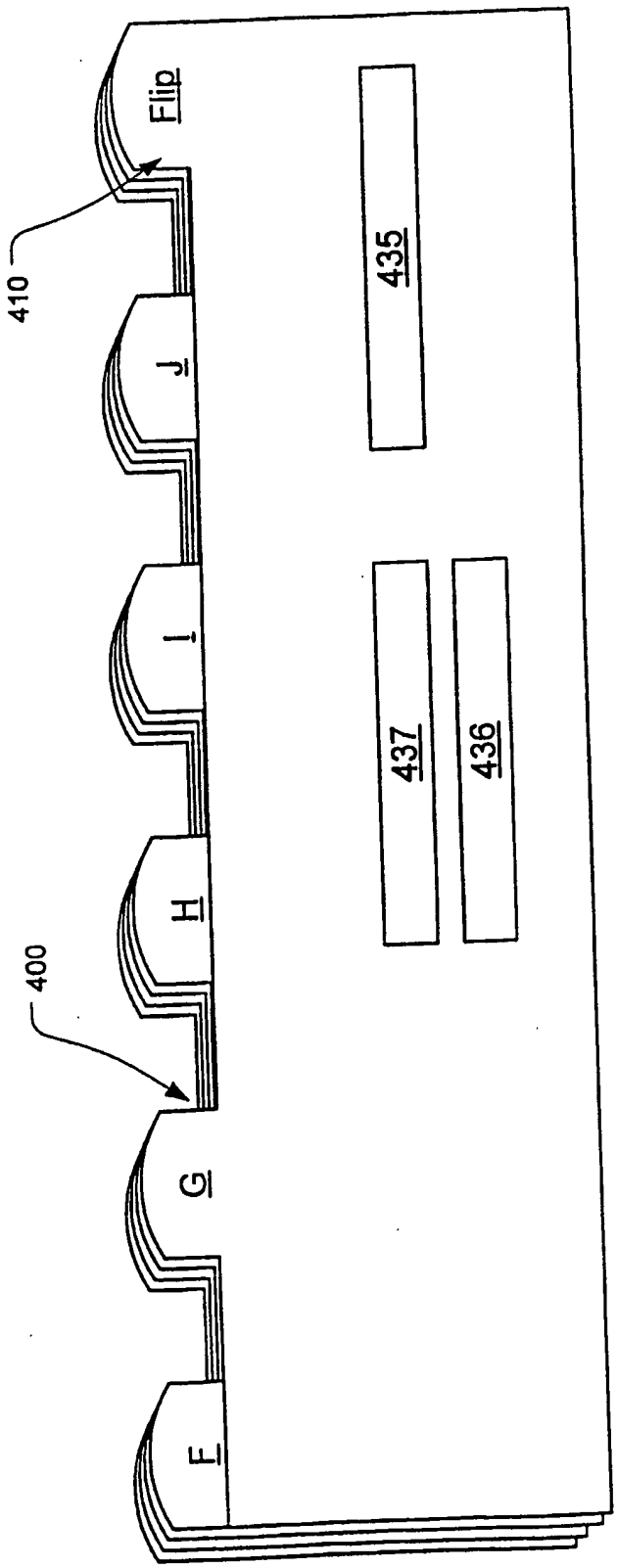


FIG. 10

Petitioner Apple Inc. - Exhibit 1026, p. 562

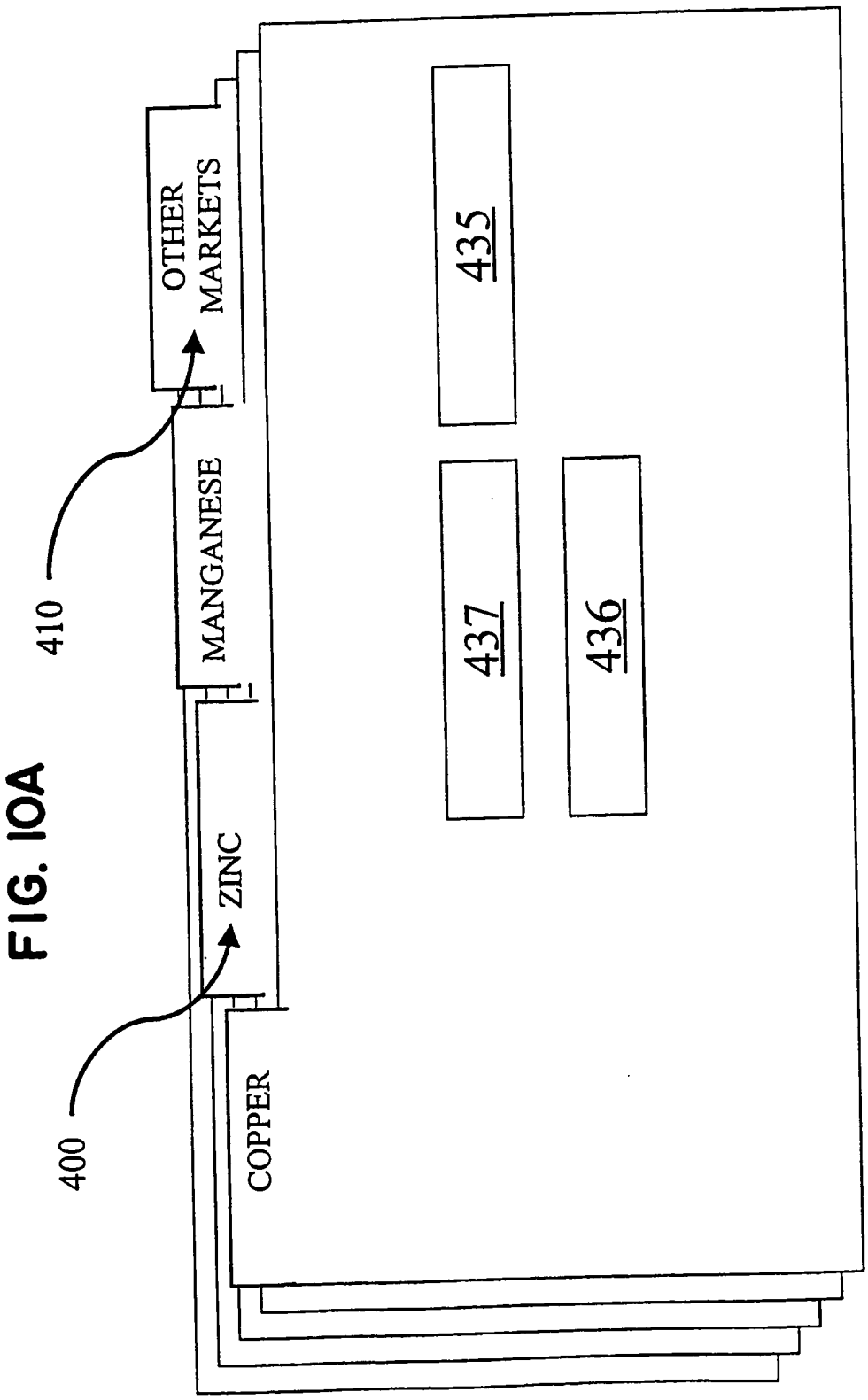


FIG. 10A

Petitioner Apple Inc. - Exhibit 1026, p. 563

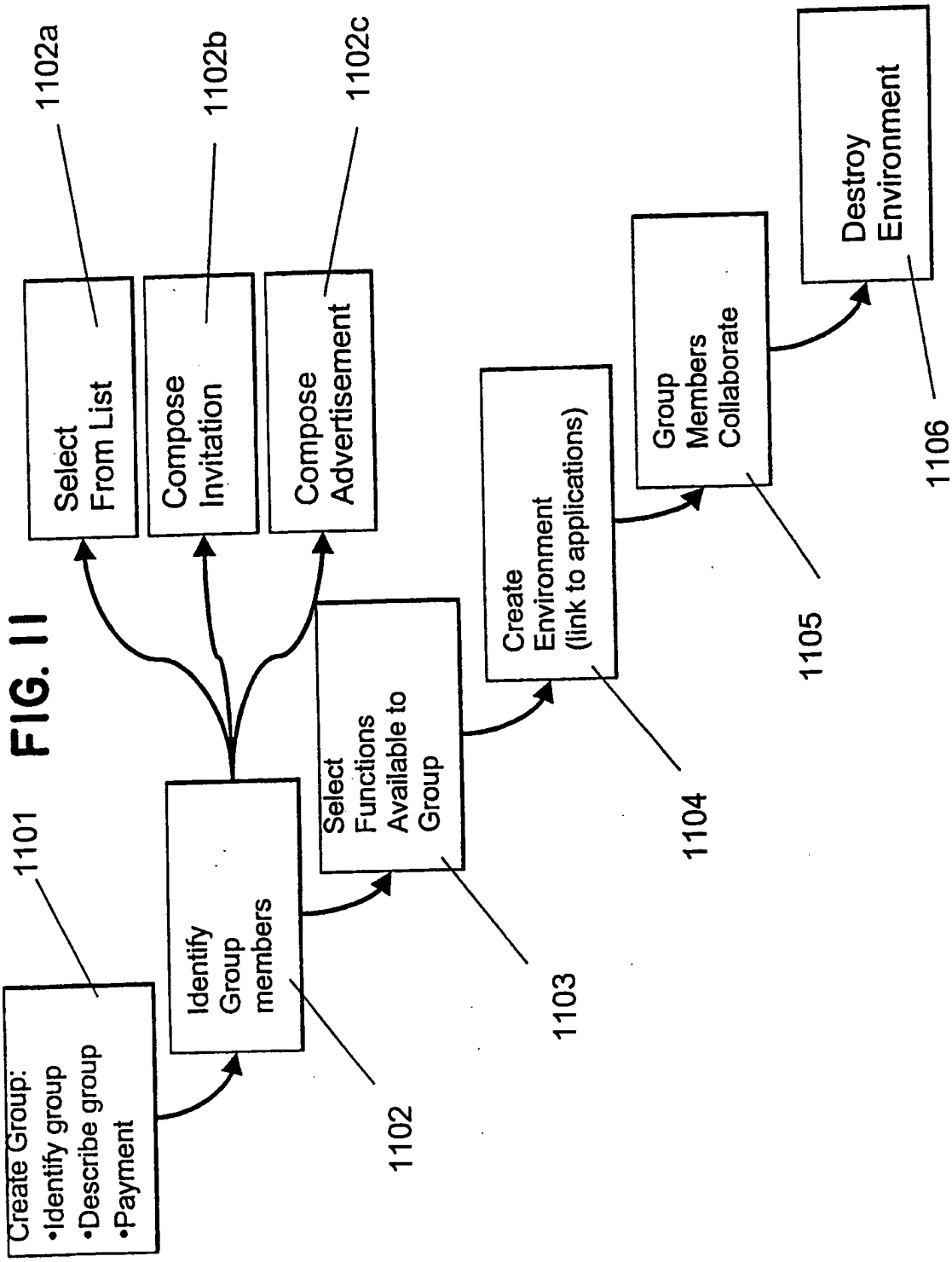


FIG. 11

Petitioner Apple Inc. - Exhibit 1026, p. 564

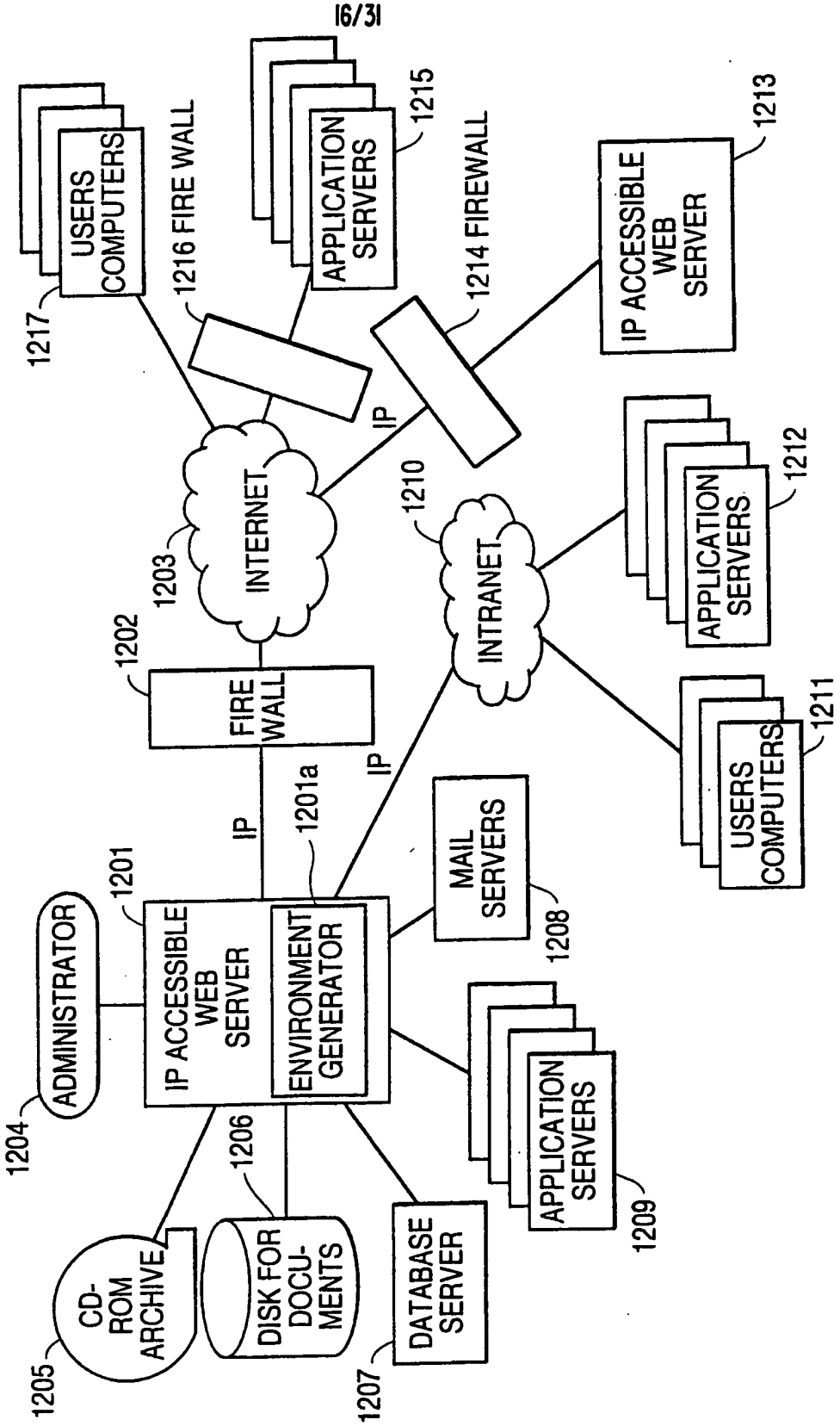


FIG. 12

Petitioner Apple Inc. - Exhibit 1026, p. 565

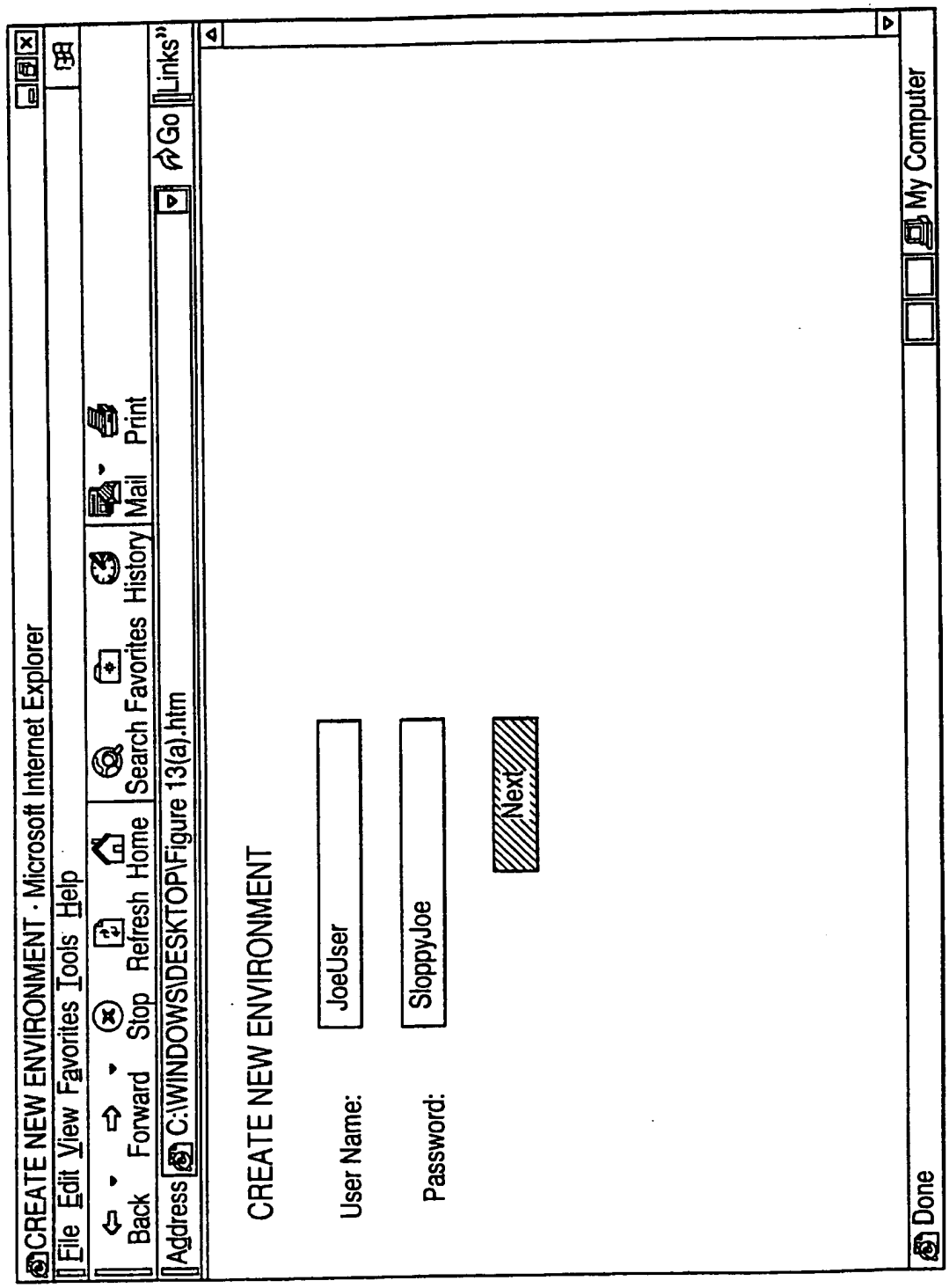


FIG. 13A

Petitioner Apple Inc. - Exhibit 1026, p. 566

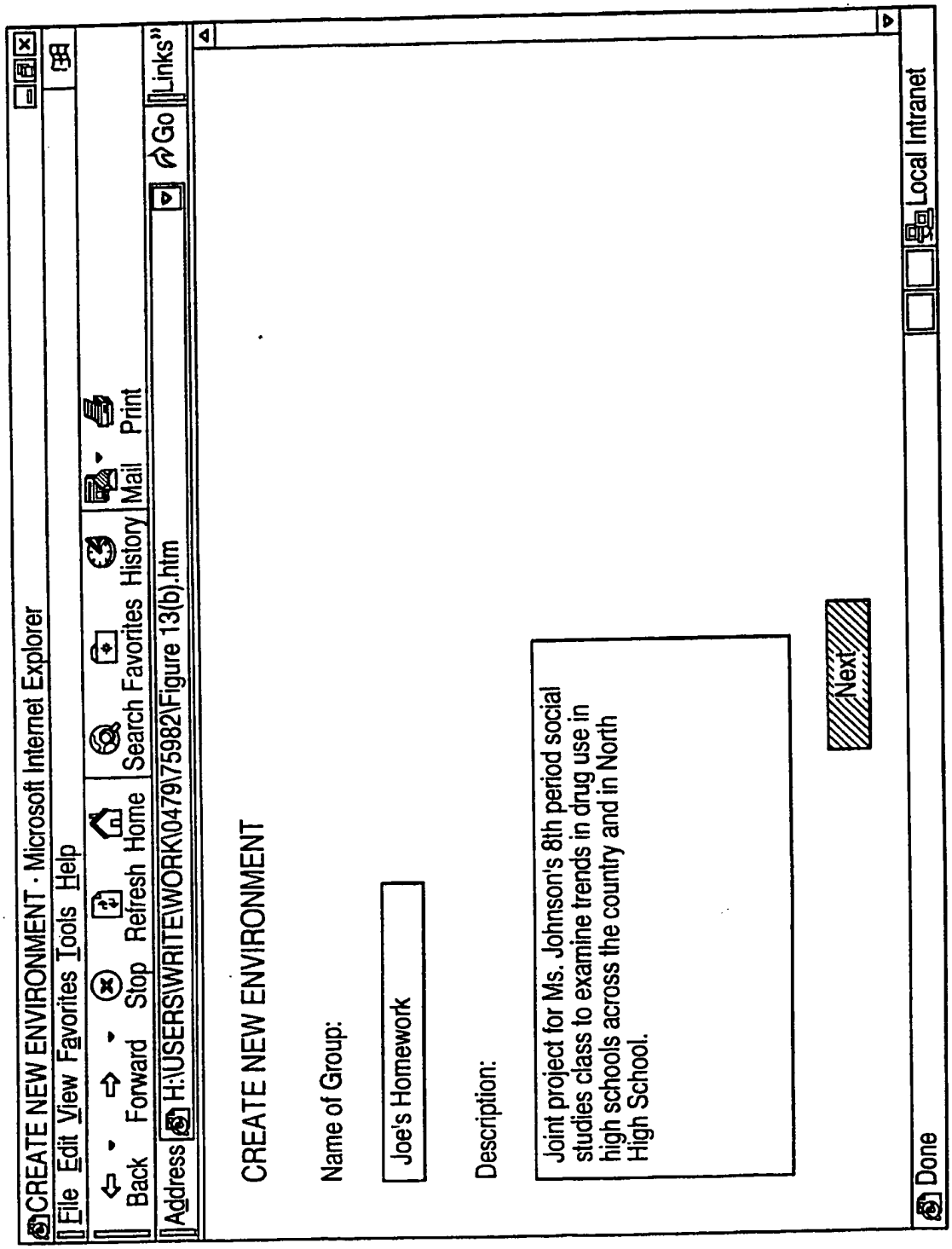


FIG. 13B

Petitioner Apple Inc. - Exhibit 1026, p. 567

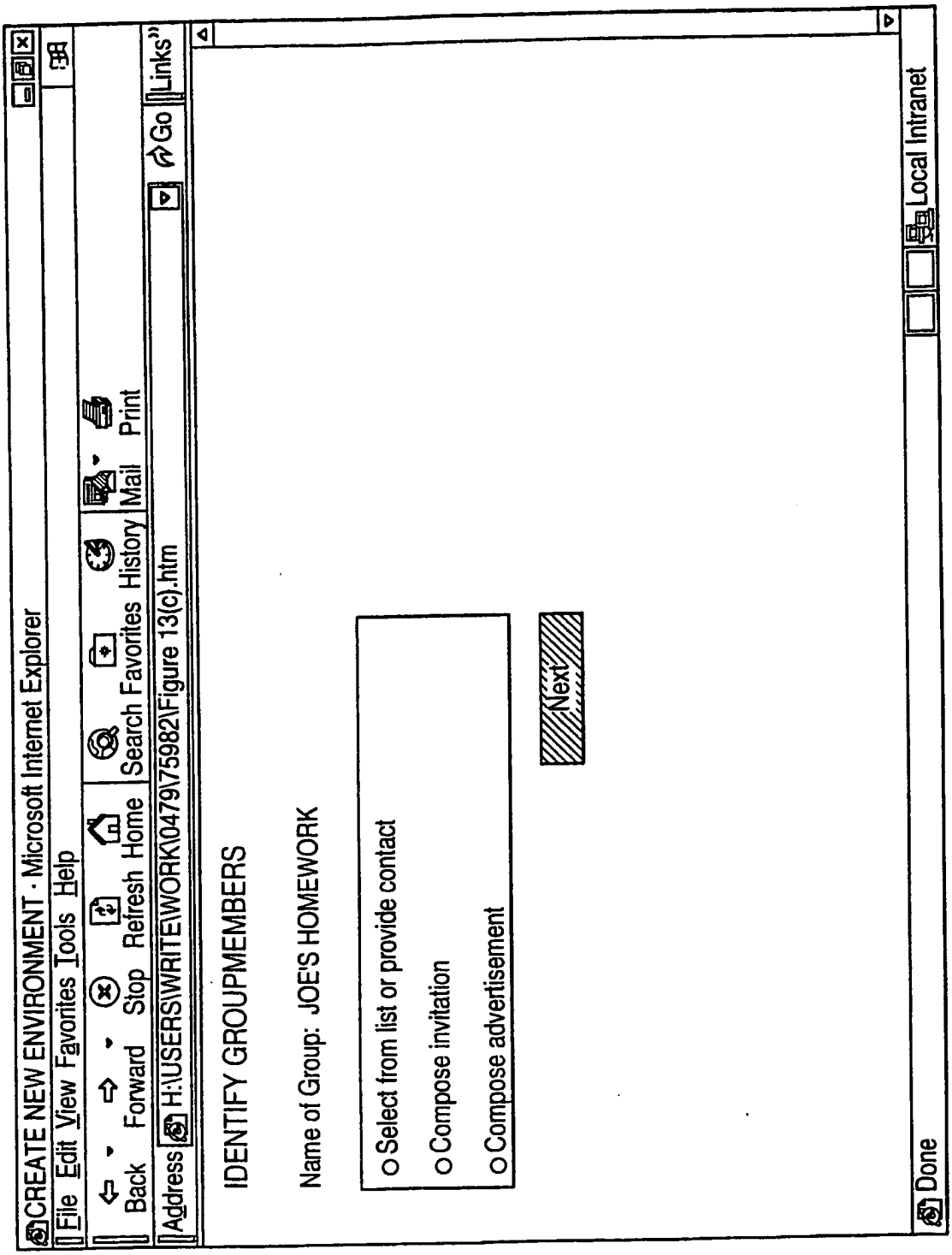


FIG. 13C

Petitioner Apple Inc. - Exhibit 1026, p. 568

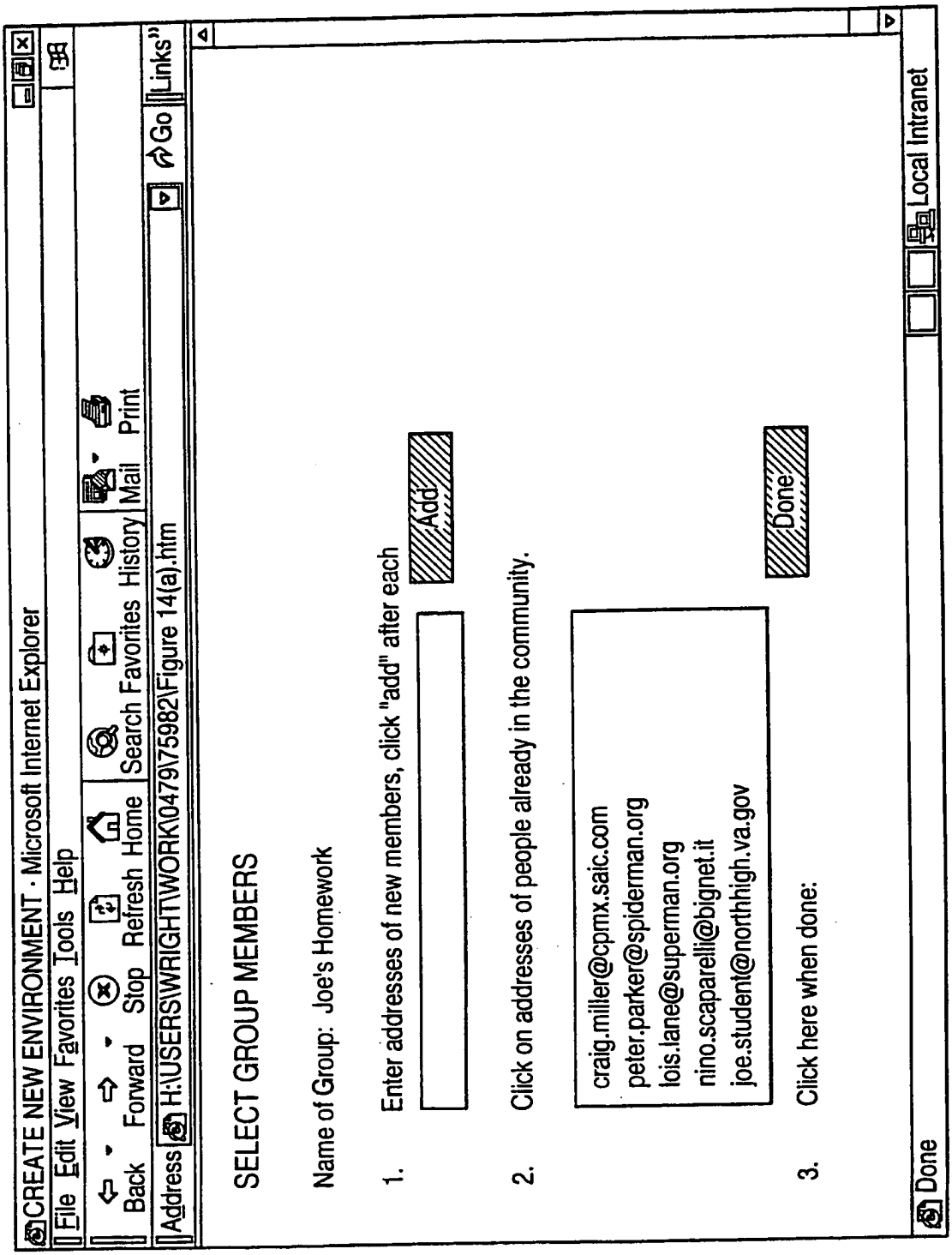


FIG. 14A

Petitioner Apple Inc. - Exhibit 1026, p. 569

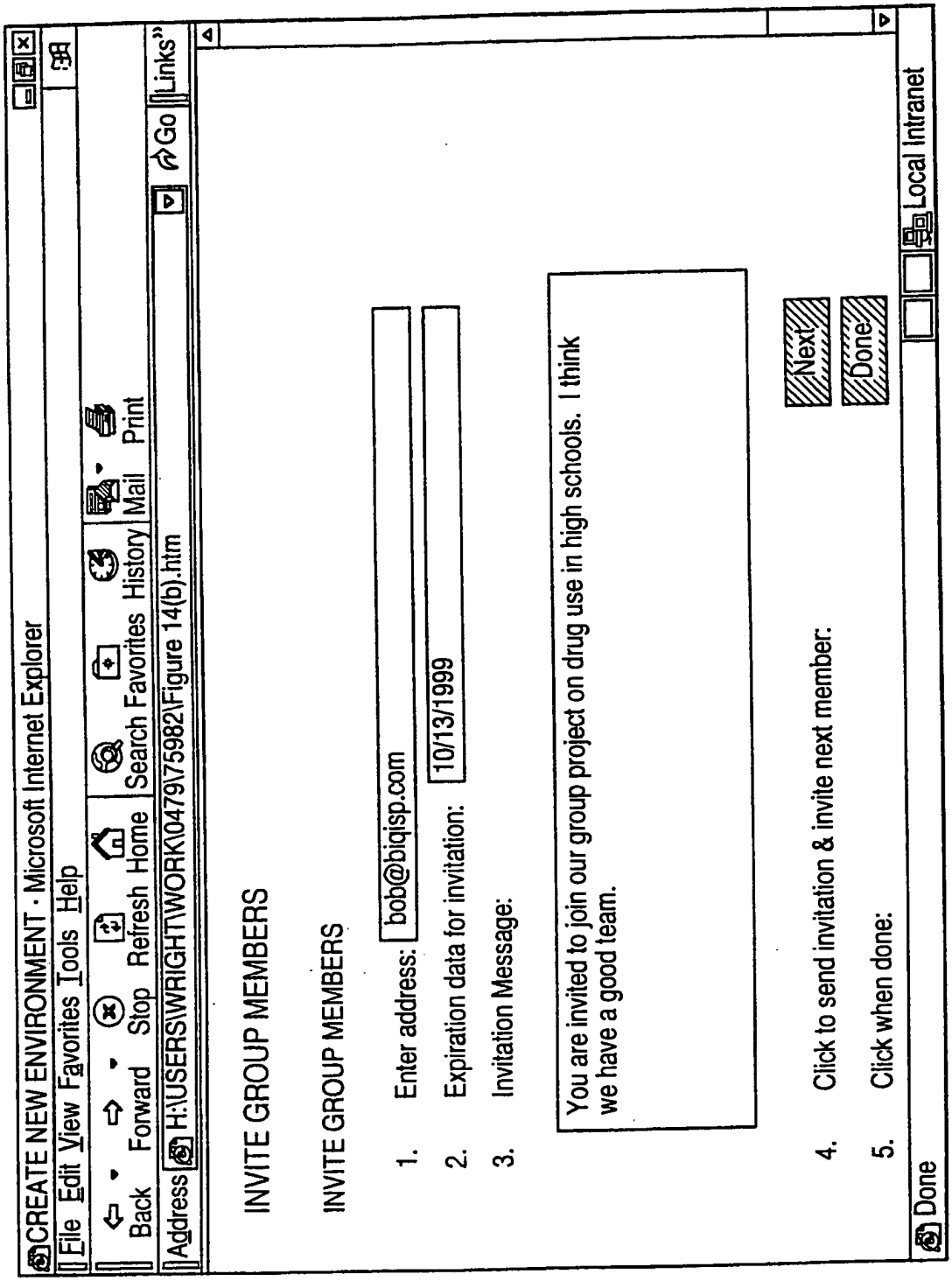


FIG. 14B

Petitioner Apple Inc. - Exhibit 1026, p. 570

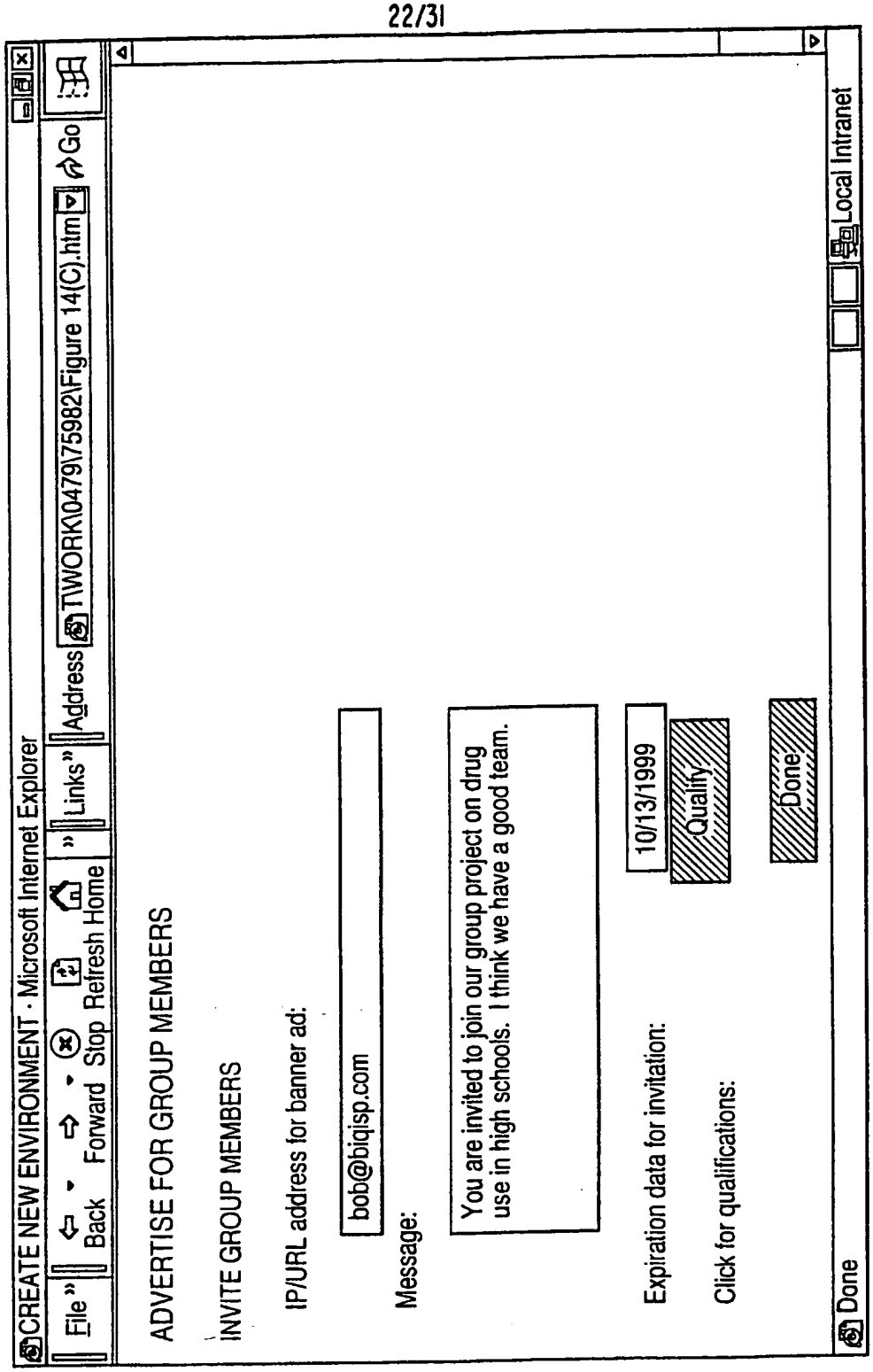


FIG. 14C

Petitioner Apple Inc. - Exhibit 1026, p. 571

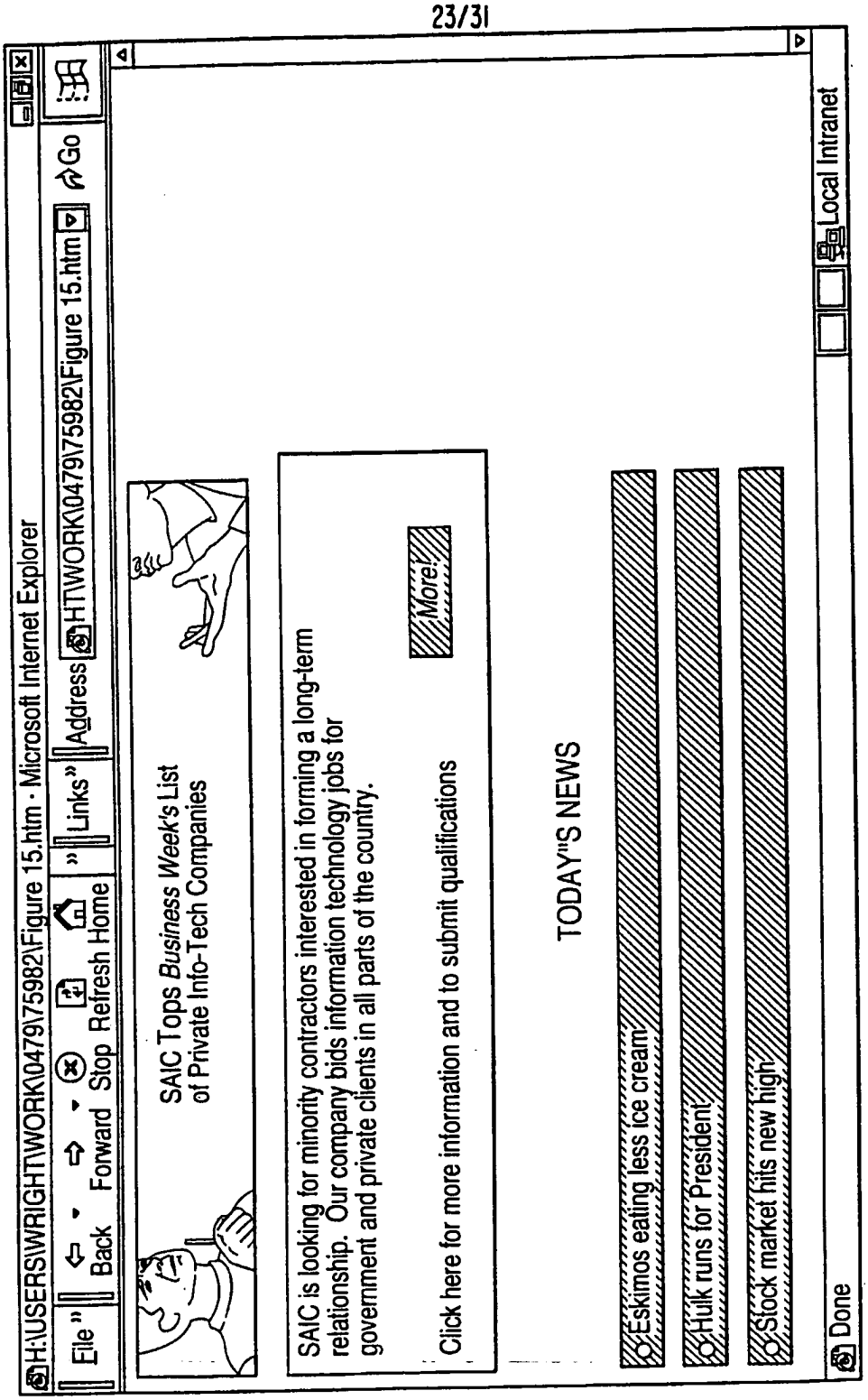


FIG. 15

Petitioner Apple Inc. - Exhibit 1026, p. 572

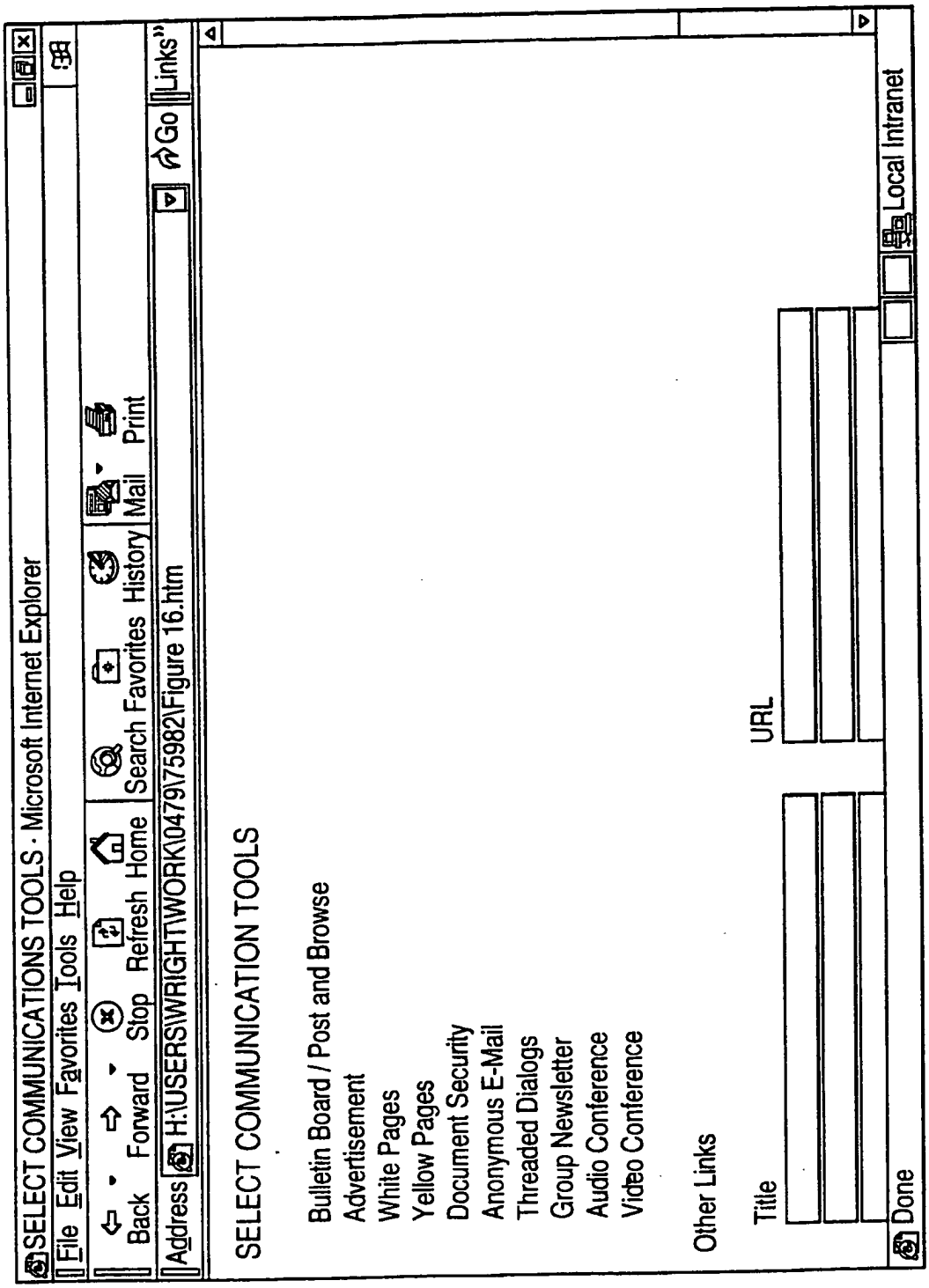


FIG. 16

Petitioner Apple Inc. - Exhibit 1026, p. 573

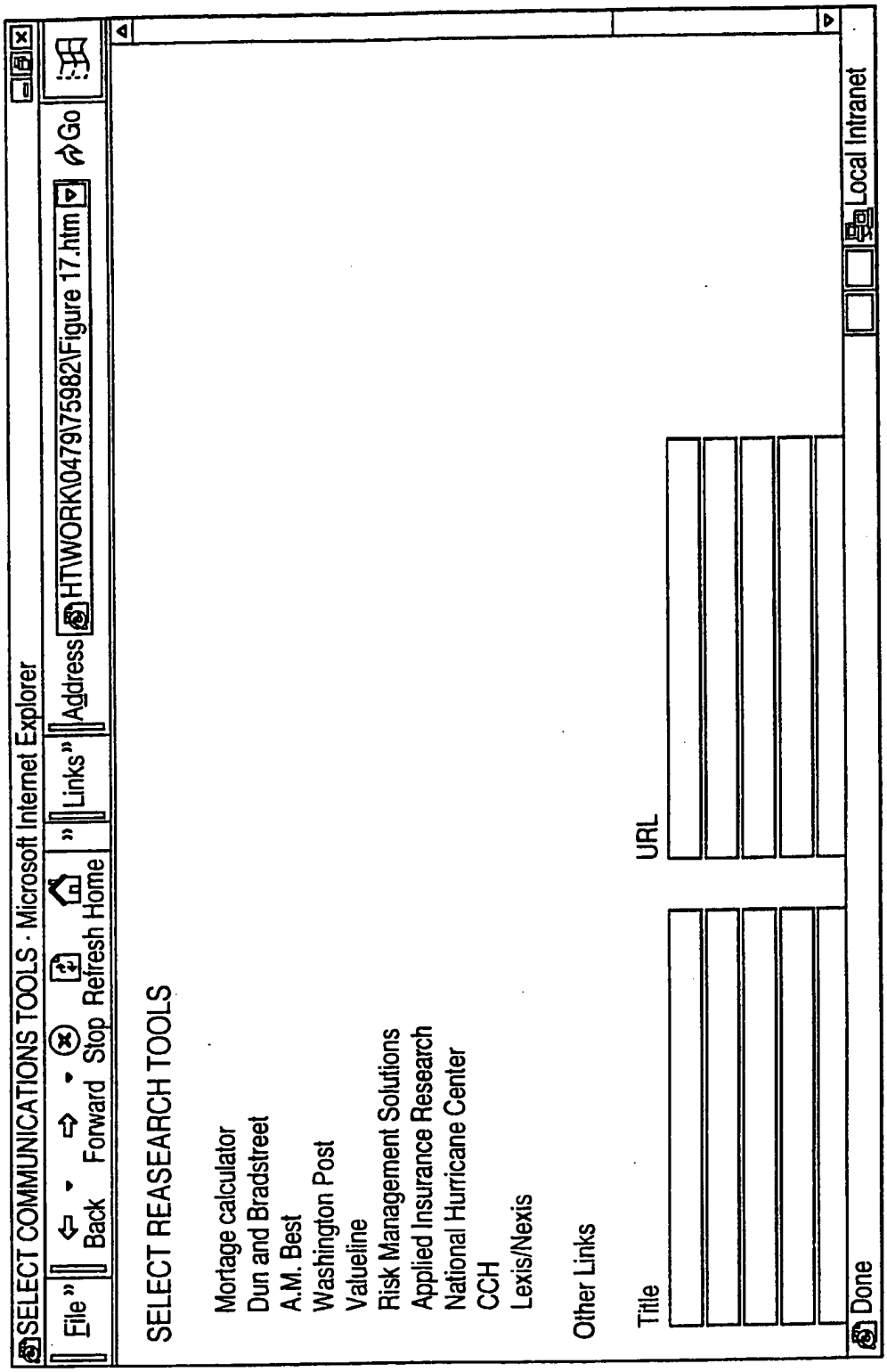


FIG. 17

Petitioner Apple Inc. - Exhibit 1026, p. 574

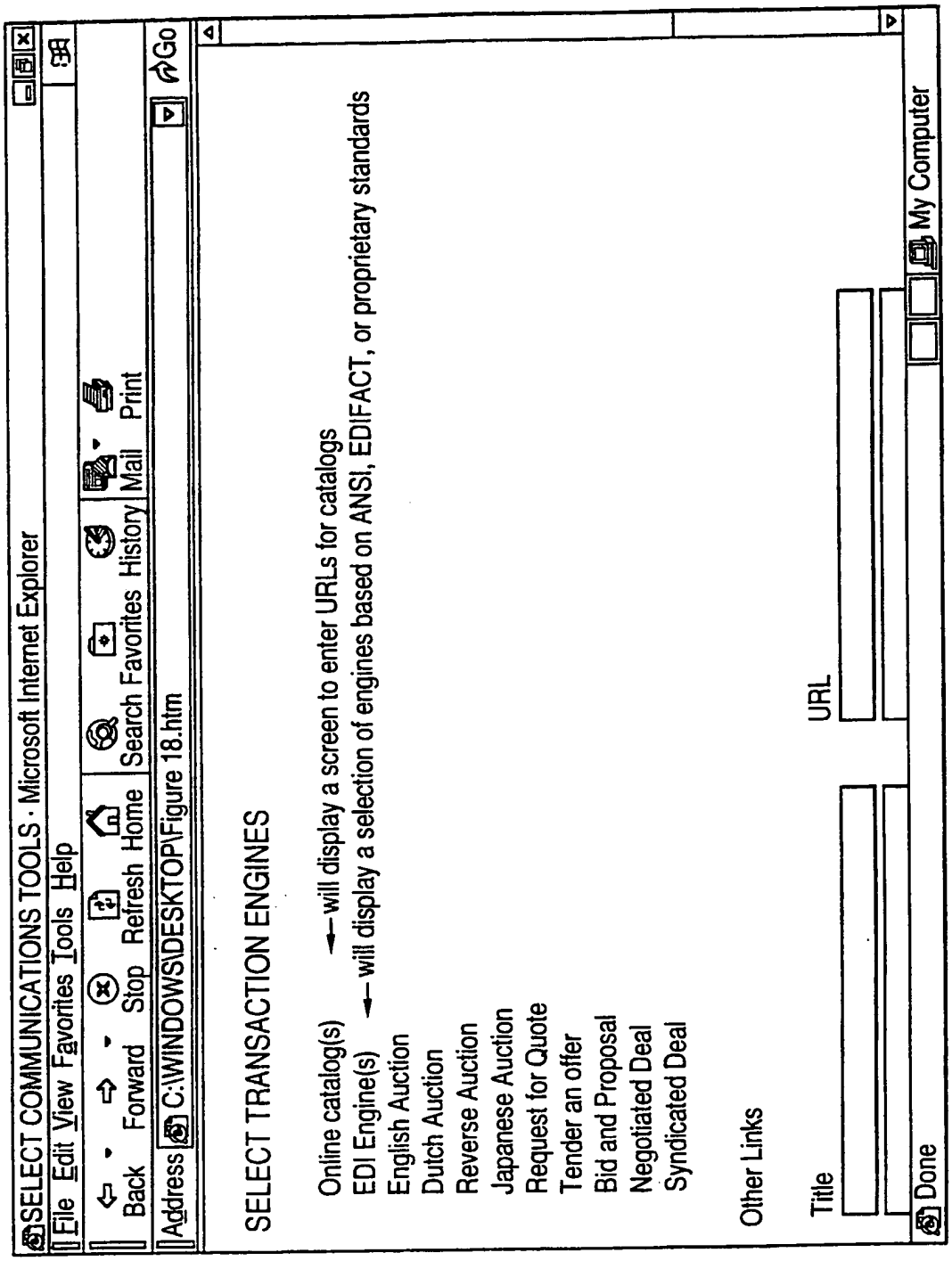


FIG. 18

Petitioner Apple Inc. - Exhibit 1026, p. 575

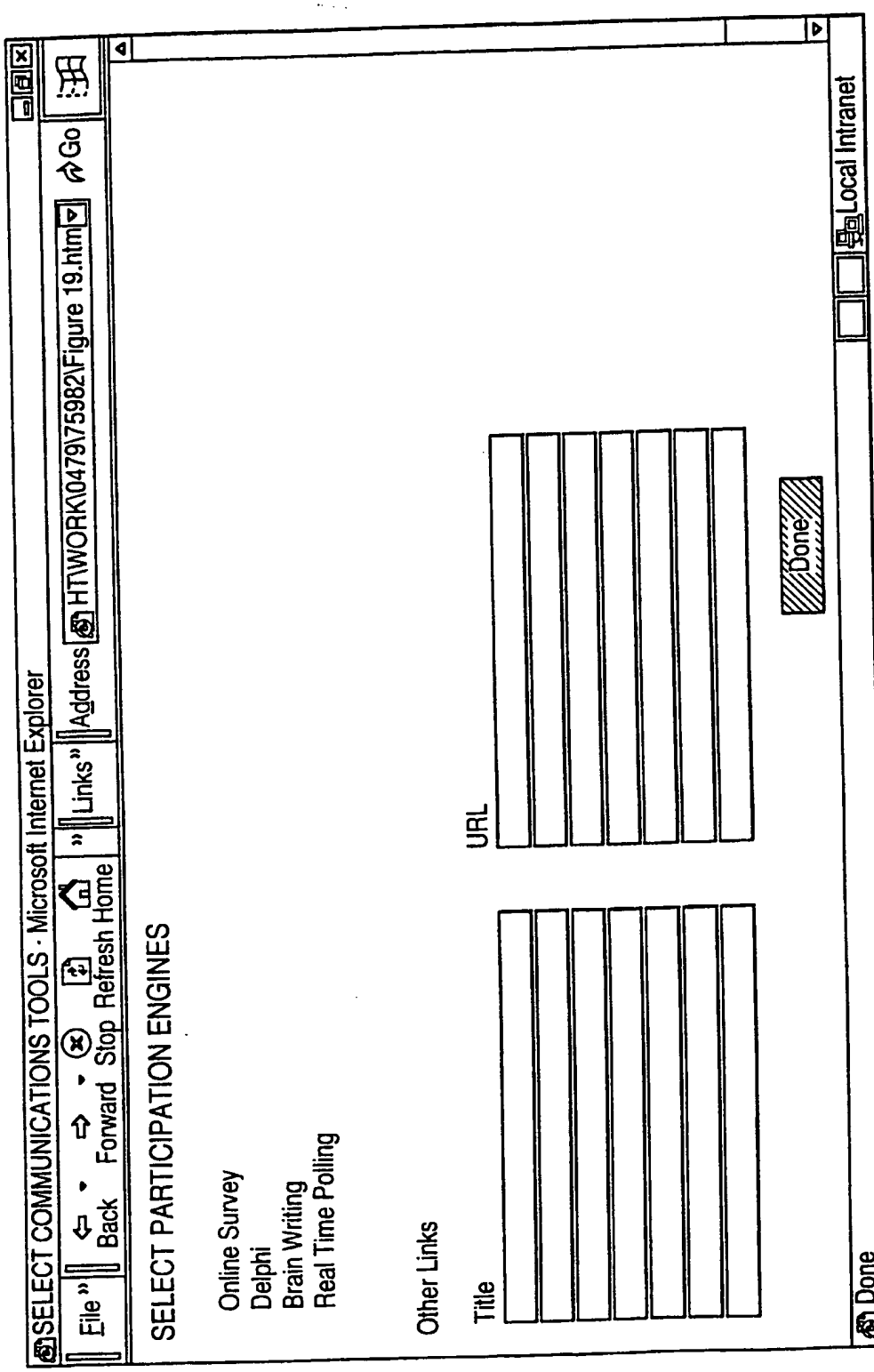


FIG. 19

Petitioner Apple Inc. - Exhibit 1026, p. 576

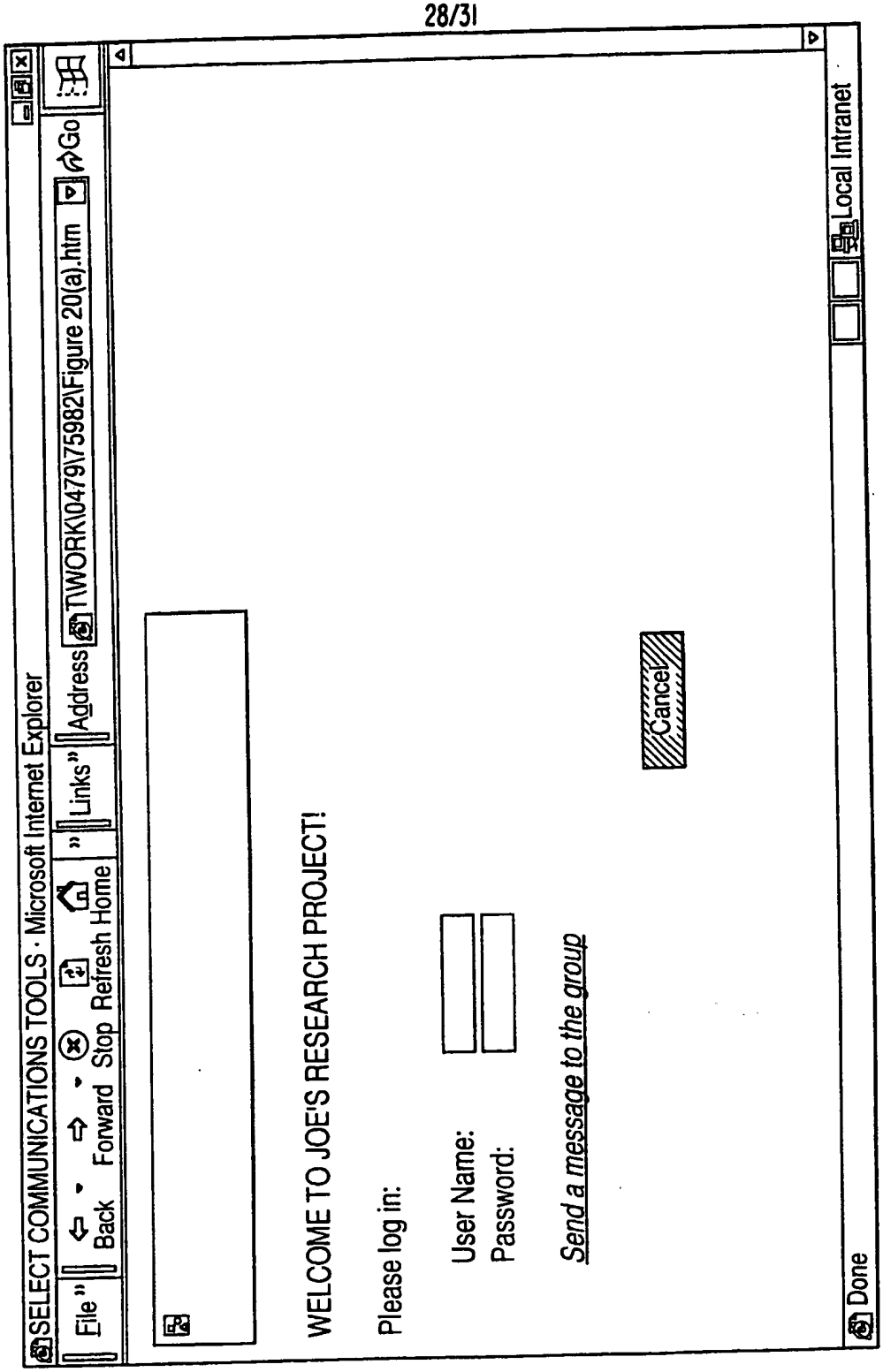


FIG. 20A

Petitioner Apple Inc. - Exhibit 1026, p. 577

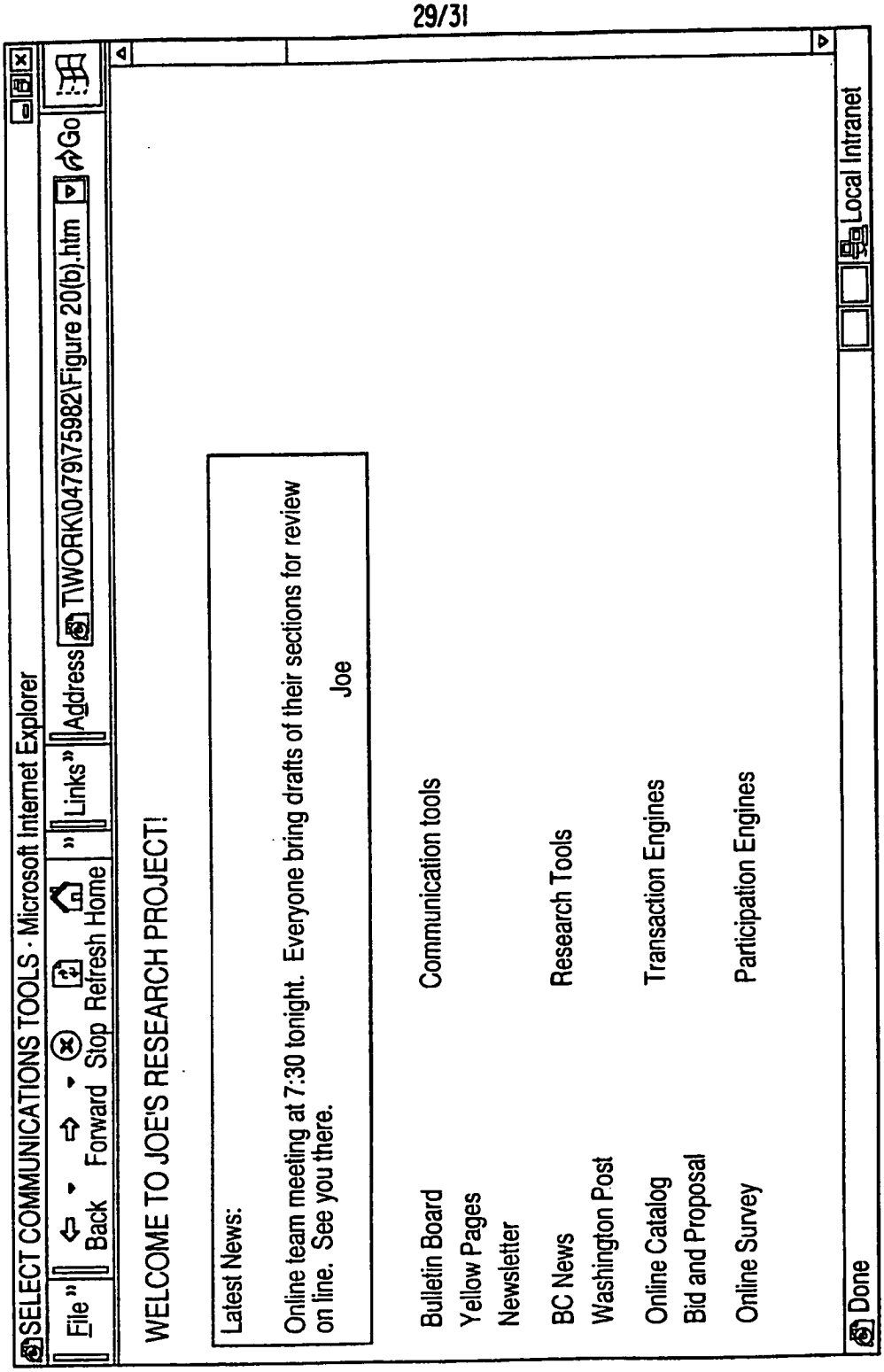


FIG. 20B

Petitioner Apple Inc. - Exhibit 1026, p. 578

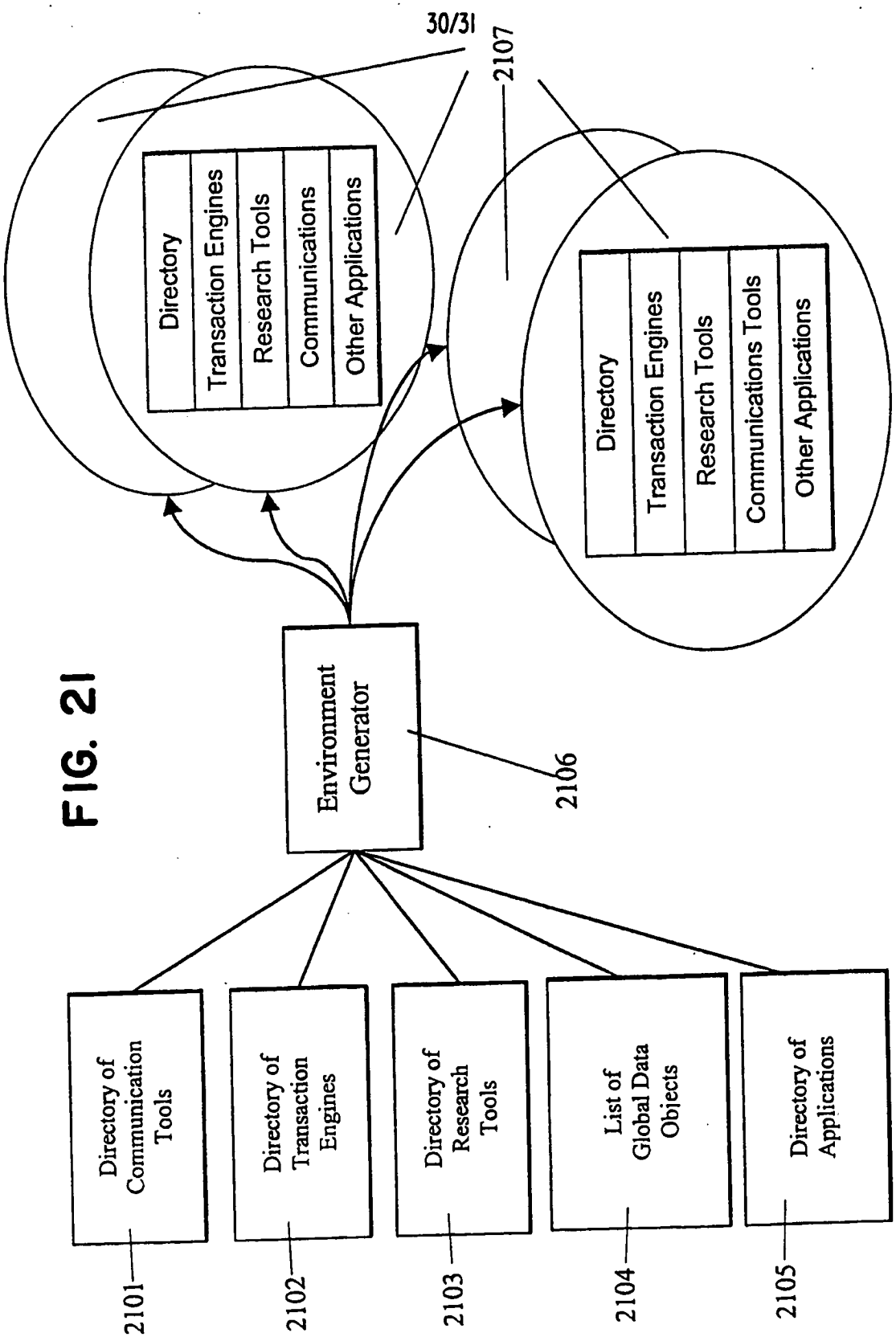
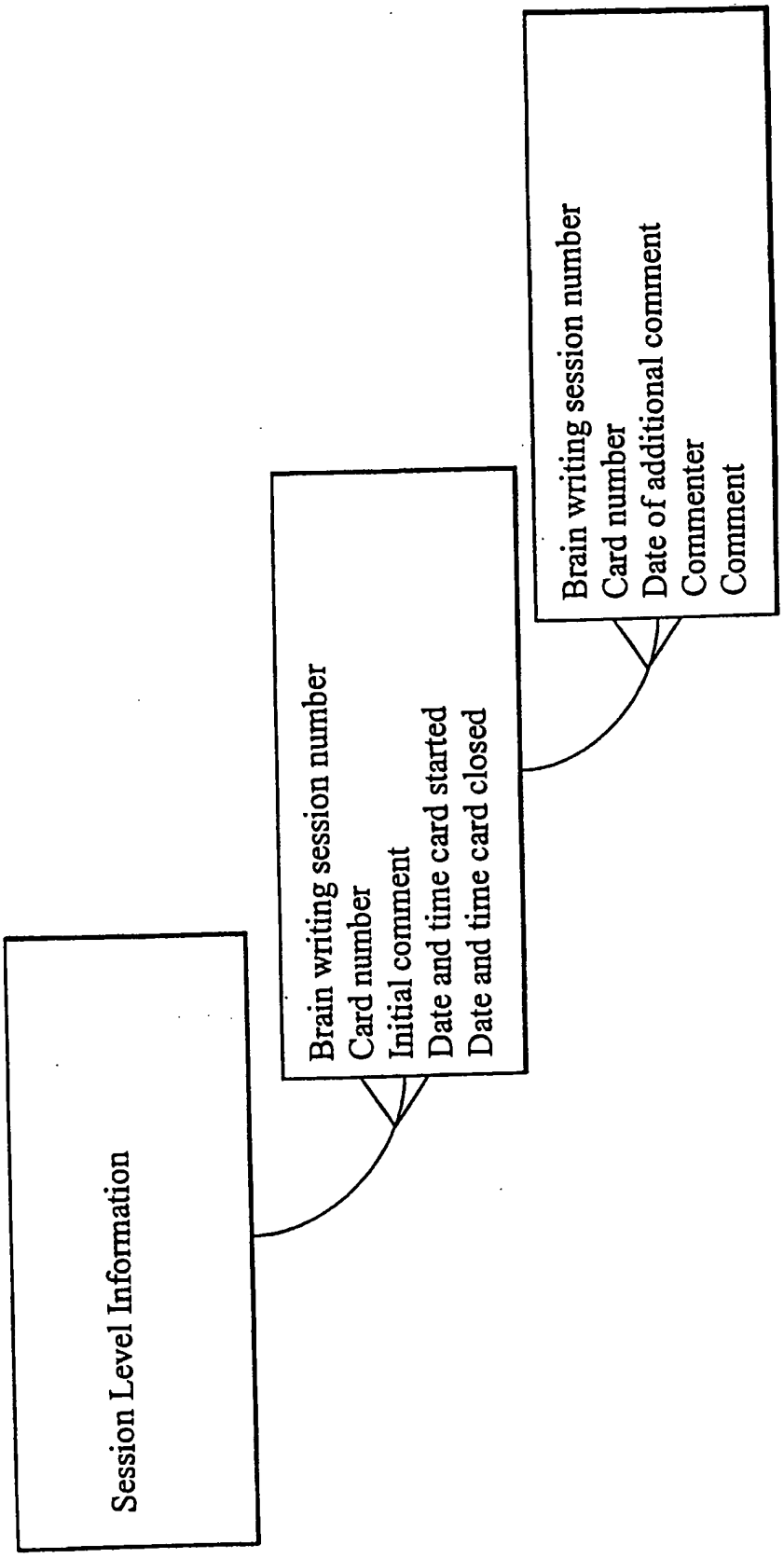


FIG. 21

Petitioner Apple Inc. - Exhibit 1026, p. 579

FIG. 22



Petitioner Apple Inc. - Exhibit 1026, p. 580

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 11/00

A1

(11) International Publication Number: WO 00/70458

(43) International Publication Date: 23 November 2000 (23.11.00)

(21) International Application Number: PCT/US00/08219

(22) International Filing Date: 15 May 2000 (15.05.00)

(30) Priority Data:
60/134,547 17 May 1999 (17.05.99) US

(71) Applicant: COMSEC CORPORATION [US/US]; 10217 Cedar Pond Drive, Vienna, VA 22182 (US).

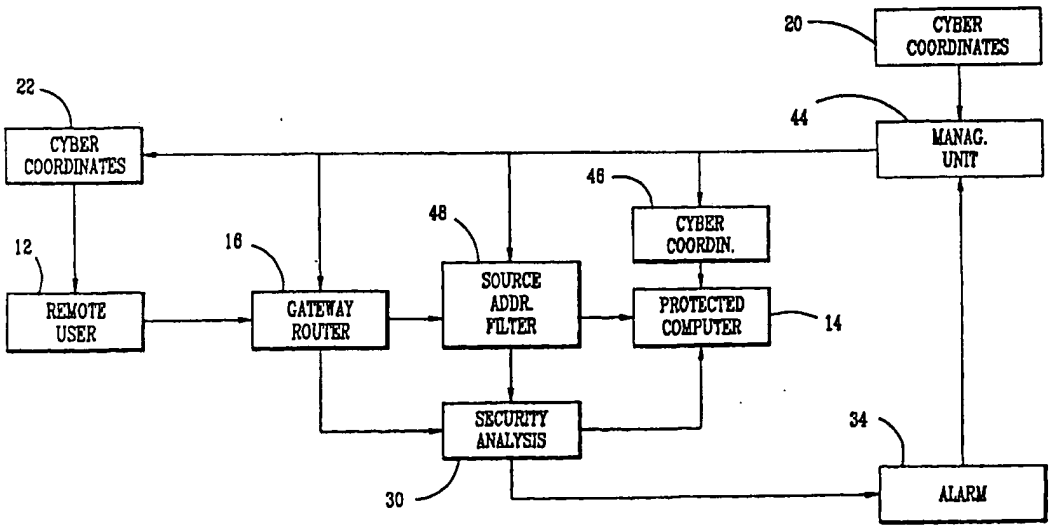
(72) Inventor: SHEYMOV, Victor, I.; 10217 Cedar Pond Drive, Vienna, VA 22182 (US).

(74) Agent: SIXBEY, Daniel, W.; Nixon Peabody LLP, Suite 800, 8180 Greensboro Drive, McLean, VA 22102 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD OF COMMUNICATIONS AND COMMUNICATION NETWORK INTRUSION PROTECTION METHODS AND INTRUSION ATTEMPT DETECTION SYSTEM



(57) Abstract

The intrusion protection method and system for a communication network provides address agility wherein the cyber coordinates of a target host (14) are changed both on a determined time schedule and when an intrusion attempt is detected. The system includes a managment unit (18) which generates a random sequence of cyber coordinates and maintains a series of tables containing the current and next set of cyber coordinates. These cyber coordinates are distributed to authorized users (12) under an encryption process to prevent unauthorized access.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD OF COMMUNICATIONS AND COMMUNICATION NETWORK INTRUSION PROTECTION METHODS AND INTRUSION ATTEMPT DETECTION SYSTEM

This application is a continuation-in-part application of U.S. Serial No. 60/134,547 filed May 17, 1999.

Background Art

Historically, every technology begins its evolution focusing mainly on performance parameters, and only at a certain developmental stage does it address the security aspects of its applications. Computer and communications networks follow this pattern in a classic way. For instance, first priorities in development of the Internet were reliability, survivability, optimization of the use of communications channels, and maximization of their speed and capacity. With a notable exception of some government systems, communications security was not an early high priority, if at all. Indeed, with a relatively low number of users at initial stages of Internet development, as well as with their exclusive nature, problems of potential cyber attacks would have been almost unnatural to address, considering the magnitude of other technical and organizational problems to overcome at that time. Furthermore, one of the ideas of the Internet was "democratization" of communications channels and of access to information, which is almost contradictory to the concept of security. Now we are faced with a situation, which requires adequate levels of security in communications while preserving already achieved "democratization" of communications channels and access to information.

All the initial objectives of the original developers of the Internet were achieved with results spectacular enough to almost certainly surpass their expectations. One of the most remarkable results of the Internet development to date is the mentioned "democratization". However in its unguarded way "democratization" apparently is either premature to a certain percentage of the Internet users, or contrary to human nature, or both. The fact remains that this very percentage of users presents a serious threat to the integrity of national critical infrastructure, to privacy of information, and to further advance of commerce by utilization

of the Internet capabilities. At this stage it seems crucial to address security issues but, as usual, it is desirable to be done within already existing structures and technological conventions.

Existing communications protocols, while streamlining communications, still lack underlying entropy sufficient for security purposes. One way to increase entropy, of course, is encryption as illustrated by U.S. Patent No. 5,742,666 to Finley. Here each node in the Internet encrypts the destination address with a code which only the next node can unscramble.

Encryption alone has not proven to be a viable security solution for many communications applications. Even within its core purpose, encryption still retains certain security problems, including distribution and safeguarding of the keys. Besides, encryption represents a "ballast", substantially reducing information processing speed and transfer time. These factors discourage its use in many borderline cases.

Another way is the use of the passwords. This method has been sufficient against humans, but it is clearly not working against computers. Any security success of the password-based security is temporary at best. Rapid advances in computing power make even the most sophisticated password arrangement a short-term solution.

Recent studies clearly indicate that the firewall technology, as illustrated by U.S. Patent No. 5,898,830 to Wesinger et al., also does not provide a sufficient long-term solution to the security problem. While useful to some extent, it cannot alone withstand the modern levels of intrusion cyber attacks.

On the top of everything else, none of the existing security methods, including encryption, provides protection against denial of service attacks. Protection against denial of service attacks has become a critical aspect of communication system security. All existing log-on security systems, including those using encryption, are practically defenseless against such attacks. Given a malicious intent of a potential attacker, it is reasonable to assume that, even having failed with an intrusion attempt, the attacker is still capable of doing harm by disabling the system with a denial of service attack. Since existing systems by definition have to deal with every log-on attempt, legitimate or not, it is certain that these systems cannot defend themselves against a denial of service attack.

The deficiencies of existing security methods for protecting communications systems leads to the conclusion that a new generation of cyber protection technology is needed to achieve acceptable levels of security in network communications.

Summary of the Invention

It is a primary object of the present invention to provide a novel and improved method of communications, and a novel and improved communication network intrusion protection method and systems and novel and improved intrusion attempt detection method and systems, adapted for use with a wide variety of communication networks including Internet based computers, corporate and organizational computer networks (LANs), e-commerce systems, wireless computer communications networks, telephone dial-up systems, wireless dial-up systems, wireless telephone and computer communications systems, cellular and satellite telephone systems, mobile telephone and mobile communications systems, cable based systems and computer databases, as well as protection of network nodes such as routers, switches, gateways, bridges, and frame relays.

Another object of the present invention is to provide a novel and improved communication network intrusion protection method and system which provides address agility combined with a limited allowable number of log-on attempts.

Yet another object of the present invention is to provide a novel and improved intrusion protection method for a wide variety of communication and other devices which may be accessed by a number, address code, and/or access code. This number, address code, and/or access code is periodically changed and the new number, address code, or access code is provided only to authorized users. The new number, address code, or access code may be provided to a computer or a device for the authorized user and not be accessible to others. This identifier causes the user's computer to transmit the otherwise unknown and inaccessible number, address code, and/or access code.

A still further object of the present invention is to provide a novel and improved communication network intrusion protection method and system wherein a plurality of different cyber coordinates must be correctly provided before access is granted to a protected communications unit or a particular piece of information. If all or some cyber coordinates

are not correctly provided, access is denied, an alarm situation is instigated and the affected cyber coordinates may be instantly changed.

For the purposes of this invention cyber coordinates are defined as a set of statements determining location of an object (such as a computer) or a piece of information (such as a computer file) in cyber space. Cyber coordinates include but are not limited to private or public protocol network addresses such as an IP address in the Internet, a computer port number or designator, a computer or database directory, a file name or designator, a telephone number , an access number and/or code, etc.

These and other objects of the present invention are achieved by providing a communication network intrusion protection method and system where a potential intruder must first guess where a target computer such as a host workstation is in cyber space and to predict where the target computer such as a workstation will next be located in cyber space. This is achieved by changing a cyber coordinate (the address) or a plurality of cyber coordinates for the computers such as workstations on a determined or random time schedule and making an unscheduled cyber coordinates change when the system detects an intrusion attempt. A limited number of log-on attempts may be permitted before an intrusion attempt is confirmed and the cyber coordinates are changed. A management unit is provided for generating a random sequence of cyber coordinates and which maintains a series of tables containing current and the next set of addresses. These addresses are distributed to authorized parties, usually with use of an encryption process.

The present invention further provides for a piece of information, a computer or a database intrusion protection method and system where a potential intruder must first guess where a target piece of information such as a computer file or a directory is in cyber space and to predict where the target piece of information will be next in cyber space. This is achieved by changing a cyber coordinate or a plurality of cyber coordinates for the piece of information on a determined or random time schedule and making an unscheduled cyber coordinates change when the system detects an intrusion attempt. A limited number of log-on attempts may be permitted before an intrusion attempt is confirmed and the coordinates changed. A management unit is provided for generating a random sequence of cyber coordinates and which maintains a series of tables containing current and the next set of cyber coordinates. These coordinates are distributed to authorized parties, usually by means

of an encryption process.

The intrusion attempt detection methods and systems are provided to the protected devices and pieces of information as described above by means of categorizing a log-on attempt when all or some of the correct cyber coordinates are not present as an intrusion attempt and by instigating an alarm situation.

Brief Description of the Drawings

Figure 1 is a block diagram of the communication network protection system of the present invention;

Figure 2 is a flow diagram showing the operation of the system of Figure 1;

Figure 3 is a block diagram of a second embodiment of the communication network protection system of the present invention;

Figure 4 is a flow diagram showing the operation of the system of Figure 3;

Figure 5 is a block diagram of a third embodiment of the communication network protection system of the present invention;

Figure 6 is a flow diagram showing the operation of the system of Figure 5; and

Figure 7 is a block diagram of a fourth embodiment of the communication network protection system of the present invention.

Description of the Preferred Embodiments

Existing communications systems use fixed coordinates in cyber space for the communications source and communications receiver. Commonly accepted terminology for the Internet refers to these cyber coordinates as source and destination IP addresses. For

purposes of an unauthorized intrusion into these communication systems, the situation of a cyber attack might be described in military terms as shooting at a stationary target positioned at known coordinates in cyber space. Obviously, a moving target is more secure than the stationary one, and a moving target with coordinates unknown to the intruder is more secure yet. The method of the present invention takes advantage of the cyber space environment and the fact that the correlation between the physical coordinates of computers or other communication devices and their cyber coordinates is insignificant.

While it is difficult to change the physical coordinates of computers or other communications devices, their cyber coordinates (cyber addresses) can be changed much easier, and in accordance with the present invention, may be variable and changing over time. In addition to varying the cyber coordinates over time, the cyber coordinates can immediately be changed when an attempted intrusion is sensed. Furthermore, making the current cyber coordinates available to only authorized parties makes a computer or other communications device a moving target with cyber coordinates unknown to potential attackers. In effect, this method creates a device which perpetually moves in cyber space.

Considering first the method of the present invention as applied to computers and computer networks, the computer's current cyber address may serve also as its initial log-on password with a difference that this initial log-on password is variable. A user, however, has to deal only with a computer's permanent identifier, which is, effectively its assigned "name" within a corresponding network. Any permanent identifier system can be used, and an alphabetic "name" system seems to be reasonably user-friendly. One of such arrangements would call for using a computer's alphabetic Domain Name System, as a cyber address permanent identifier, while subjecting its numeric, or any other cyber address to a periodic change with regular or irregular intervals. This separation will make the security system transparent to the user, who will have to deal only with the alphabetic addresses. In effect, the user's computer would contain an "address book" where the alphabetic addresses are permanent, and the corresponding variable addresses are more complex and periodically updated by a network's management. While a user is working with other members of the network on the name or the alphabetic address basis, the computer conducts communications based on the corresponding variable numeric or other addresses assigned for that particular time.

A variable address system can relatively easily be made to contain virtually any level of entropy, and certainly enough entropy to defy most sophisticated attacks. Obviously, the level of protection is directly related to the level of entropy contained in the variable address system and to the frequency of the cyber address change.

This scenario places a potential attacker in a very difficult situation when he has to find the target before launching an attack. If a restriction on a number of allowable log-on tries is implemented, it becomes more difficult for an attacker to find the target than to actually attack it. This task of locating the target can be made difficult if a network's cyber address system contains sufficient entropy. This difficulty is greatly increased if the security system also limits the number of allowable log-on tries, significantly raising the entropy density.

For the purpose of this invention, entropy density is defined as entropy per one attempt to guess a value of a random variable.

Figure 1 illustrates a simple computer intrusion protection system 10 which operates in accordance with the method of the present invention. Here, a remote user's computer 12 is connected to a protected computer 14 by a gateway router or bridge 16. A management system 18 periodically changes the address for the computer 14 by providing a new address from a cyber address book 20 which stores a plurality of cyber addresses. Each new cyber address is provided by the management system 18 to the router 16 and to a user computer address book 22. The address book 22 contains both the alphabetic destination address for the computer 14 which is available to the user and the variable numeric cyber address which is not available to the user. When the user wants to transmit a packet of information with the alphabetic address for the computer 14, this alphabetic address is automatically substituted for the current numerical cyber address and used in the packet.

With the reference to Figures 1 and 2, when a packet is received by the gateway router or bridge 16 as indicated at 24, the cyber address is checked by the gateway router or bridge at 26, and if the destination address is correct, the packet is passed at 28 to the computer 14. If the destination address is not correct, the packet is directed to a security analysis section 30 which, at 32 determines if the packet is retransmitted with a correct address within a limited number of log-in attempts. If this occurs, the security analysis section transmits the packet to the computer 14 at 28. However, if no correct address is

received within the allowed limited number of log-in attempts, the packet is not transmitted to the computer 14 and the security analysis section activates an alarm section 34 at 36 which in turn causes the management section to immediately operate at 38 to change the cyber address.

Sophisticated cyber attacks often include intrusion through computer ports other than the port intended for a client log-on. If a system principally described in connection with Figures 1 and 2 is implemented, the port vulnerability still represents an opening for an attack from within the network, that is if an attacker has even a low-level authorized access to a particular computer and thus knows its current variable address.

Computer ports can be protected in a way similar to protection of the computer itself. In this case port assignment for the computer becomes variable and is changed periodically in a manner similar to that described in connection with Figures 1 and 2. Then, a current assignment of a particular port is communicated only to appropriate parties and is not known to others. At the same time, similarly to methods described, a computer user would deal with permanent port assignments, which would serve as the ports' permanent "names".

This arrangement in itself may not be sufficient, however, to reliably protect against a port attack using substantial computing power because of a possible insufficient entropy density. Such a protection can be achieved by implementing an internal computer "port router" which would serve essentially the same role for port identifiers as the common gateway router or bridge 16 serves for computer destination addresses.

With reference to Figures 3 and 4 wherein like reference numerals are used for components and operations which are the same as those previously described in connection with Figures 1 and 2, a port router 40 is provided prior to the protected computer 14, and this port router is provided with a port number or designator by the management unit 18. This port number or designator is also provided to the user address book 22 and will be changed when the cyber address is changed, or separately. Thus, with reference to Figure 4, once the cyber address has been cleared at 26, the port number or designator is examined at 42. If the port number is also correct, the data packet will be passed to the computer 14 at 28. If the port number is initially incorrect, the packet is directed to the security analysis section 30 which at 32 determines if the packet is retransmitted with the correct port number within the limited number of log-in attempts.

The port protection feature can be used independently of other features of the system. It can effectively protect nodes of the infrastructure such as routers, gateways, bridges, and frame relays from unauthorized access. This can protect systems from an attacker staging a cyber attack from such nodes.

The method and system of the present invention may be adapted to provide security for both Internet based computer networks and private computer networks such as LANs.

Internet structure allows the creation of an Internet based Private Cyber Network (PCN) among a number of Internet-connected computers. The main concern for using the Internet for this purpose as an alternative to the actual private networks with dedicated communication channels is security of Internet-based networks.

The present invention facilitates establishment of adequate and controllable level of security for the PCNs. Furthermore, this new technology provides means for flexible structure of a PCN, allowing easy and practically instant changes in its membership. Furthermore, it allows preservation of adequate security in an environment where a computer could be a member of multiple PCNs with different security requirements. Utilizing the described concept, a protected computer becomes a "moving target" for the potential intruders where its cyber coordinates are periodically changed and the new coordinates are communicated on a "need to know" basis only to the other members of the PCN authorized to access this computer along with appropriate routers and gateways. This change of cyber coordinates can be performed either by previous arrangement or by communicating future addresses to the authorized members prior to the change. Feasible frequency of such a change can range from a low extreme of a stationary system changing cyber coordinates only upon detection of a cyber attack to an extremely high frequency such as with every packet. The future coordinates can be transmitted either encrypted or unencrypted. Furthermore, each change of position of each PCN member can be made random in terms of both its current cyber coordinates and the time of the coordinates change. These parameters of a protected PCN member's cyber moves are known only to the PCN management, other PCN members with authorization to communicate with this particular member, and appropriate gateways and routers. PCN management would implement and coordinate periodic cyber coordinates changes for all members of the PCN. While the PCN management is the logical party to make all the notification of the cyber coordinates changes, in certain instances it

could be advantageous to shift a part of this task to a PCN member computer itself. With certain limitations, the routers and gateways with the "need to know" the current address of the protected computer are located in cyber space in the general vicinity of the protected computer. In such instances the protected computer could be in a better position to make the mentioned notifications of nearby routers and gateways.

The address changes could be done simultaneously for all the members of the PCN, or separately, particularly if security requirements for the members substantially differ. The latter method is advantageous, for instance, if some of the computers within the PCN are much more likely than others to be targeted by potential intruders. A retail banking PCN could be an example of such an arrangement where the bank's computer is much more likely to be attacked than a customer's computer. It should be noted that, while in certain cases some members of the PCN may not require any protection at all, it still is prudent to provide it as long as the computer belongs to a protected PCN. The correct "signature" of the current "return address" would serve as additional authenticity verification. In the above example of the retail banking, while many customers' computers may not require any protection, assigning variable addresses to them would serve as an additional assurance to the bank that every log-on is authorized. In fact, this system automatically provides two-tier security. In order to reach a protected computer, the client computer has to know the server computer current cyber address in the first place. Then, even if a potential intruder against odds "hits" the correct current address the information packet is screened for the correct "signature" or return address. If that signature does not belong to the list of the PCN's current addresses, the packet is rejected. In high security instances this should trigger an unscheduled address change of the protected computer.

With the reference to Figures 5 and 6 which illustrate this two-tier security system, a network management unit 44 provides different unique cyber coordinates to the address books for each computer in the system (two computers 12 and 14 with address books 22 and 46 respectively being shown). Now when the computer 12 sends a data packet to the computer 14, the gateway router or bridge 16, first checks for the correct current destination address for the computer 14 at 26 in the manner previously described. If the destination address is correct, a source address sensor 48 checks at 50 to determine if the correct source address (i.e. return address) for the computer 12 is also present. If both correct addresses are

present, the data packet is passed to the computer 14 at 28, but if the correct source address is not present, the data packet is passed to the security analysis section 30 where at 32 where it is determined if a correct source address is received within the acceptable number of log-on tries. If the correct return address is not received, an alarm situation is activated at 36 and the network management system operates at 38 to change the cyber address of the computer 14

In addition to the penetration (hacking) detection and protection, the system above provides real-time detection of a cyber attack and protection against "flooding" denial of service attacks. A gateway router or bridge 16 filters all the incorrectly addressed packets thus protecting against "flooding". Further yet, since the "address book" of the protected network contains only trusted destinations, this system also protects against instructive viruses or worms if such are present or introduced into the network. For the purpose of this invention, an instructive virus or worm is defined as a foreign unit of software introduced into a computer system so it sends certain computer data to otherwise unauthorized parties outside of the system.

Elements of the system described above are: a gateway router or bridge 16, a computer protection unit, and a management unit. A gateway router or bridge represents an element of collective defense for the network, while the source address filter and the "port router" and filter represent a unit of individual defense for a member computer. This individual defense unit (server unit) can be implemented either as a standalone computer, as a card in the protected computer, as software in the protected computer, or imbedded into the protected computer operating system. For further improvement of the overall security, port assignments can be generated autonomously from the management unit thus creating a "two keys" system in a cryptographic sense. This would allow for security to still be in place even if a security breach happened at the security management level.

The method and system of the present invention minimize human involvement in the system. The system can be configured in such a way that computer users deal only with simple identifiers or names permanently assigned to every computer in the network. All the real (current) cyber coordinates can be stored separately and be inaccessible to the user, and could be available to the appropriate computers only. This approach both enhances security and makes this security system transparent to the user. The user deals only with the simple

alphabetic side of the "address book", and is not bothered with the inner workings of the security system. A telephone equivalent of this configuration is an electronic white pages residing in a computerized telephone set, which is automatically updated by the telephone company. The user just has to find a name, and push the "connect" button while the telephone set does the rest of the task.

A numeric cyber address system, based on the Internet host number could be relatively easily utilized for the discussed security purposes, however a limitation exists for this address system in its current form represented by the IPv.4 protocol. This limitation is posed by the fact that the address is represented by a 32-bit number. 32-bit format does not contain sufficient entropy in the address system to enable establishment of adequate security. This is a particularly serious limitation in regard to securing an entire network. The availability of the network numbers are limited to the extent that not only entropy, but a simple permanently assigned number is becoming more and more difficult to obtain with the rapid expansion of the Internet.

If this address system is to be used for the security purposes, than the format of the host number should be adequately expanded to create sufficient size of the address numbers field in the system. If this is done, than the corresponding address in the Domain Name System (DNS) could be conveniently used as permanent identifier for a particular computer and the Internet host number would be variable, creating a moving regime of a protected computer. Currently being implemented IPv.6 (IPNG) protocol solves this problem by providing sufficient entropy.

Another way to achieve the same goal is to use the DNS address as a variable for security purposes. This way, the traditional Internet DNS address system would not be affected and no change in format is required. The relevant part of the protected computer's DNS address would become a variable, utilizing more characters than the alphabet, with a very large number of variations, also creating sufficient level of entropy.

Yet another way to implement the same method is to utilize the geographic zone-based system. While its utilization is somewhat similar to the DNS system, it offers some practical advantages for security use. Naturally, when a computer is protected by a security system, it is still essential to preserve the communication redundancy of the Internet communications. However, the redundancy may suffer if only a limited number of the

routers and gateways are informed of the protected computer current cyber address. This effect could be particularly important with the members of a particular protected network vastly remote in geographic terms. The necessary notification of a large number of the routers and gateways can also become problematic, not only technically, but also because it can decrease the level of security. In this sense a geographic zone-based system offers advantages since the variable part of the computer's cyber address could be made to involve only certain geographic locale while initial routing of the information packet could be done by the traditional method. After the packet has been moved to the general vicinity of the addressee computer, it would get into the area of the "informed" routers and gateways. This scheme would simplify the notification process of the routers as well as improve security by limiting the number of the "need to know" parties. It is important to recognize that, after the "general" part of the cyber address caused the information packet to arrive in a cyber vicinity of the addressee, virtually any, even private, address system can be used for the rest of he the delivery. This would further increase the level of underlying entropy in the system.

While certain specific address systems have been discussed, it is an important quality of the present invention that it can be implemented with virtually any address system.

Corporate and organizational computer networks such as LANs or, at least those in closed configurations, do not possess as much vulnerability to cyber attacks as Internet-based networks. However, even in these cases, their remote access security is a subject of concern. This is especially visible when a private network (PN) contains information of different levels of confidentiality with access restricted to appropriate parties. In other words, along with other generally accessible organizational information, an organizational PN can contain information restricted to certain limited groups. Enforcement of these restrictions requires a remote access security system. Usually these security systems employ a password-based scheme of one type or another and, perhaps, a firewall. However, reliance on passwords may not be entirely justified since the passwords can be lost or stolen, giving a malicious insider with a low access level a reasonable chance of access to information intended only for higher levels of access. Furthermore, in some cases use of cracking techniques from such a position is not entirely out of the question. Such an occurrence can relatively easily defeat both the password and the firewall. This would prevent a LAN from a cyber attack launched from within the network.

The present invention provides adequate security to such PCNs without reliance on the passwords and to limit access to only appropriate computers. Then, the task of overall information access security practically would be narrowed down to control of physical access to a particular computer, usually a less complicated feat.

Similarly to the systems described for Internet-based networks, a "closed" LAN as well as an Internet-based LAN can be protected by implementation of periodic changes of the members' network addresses and communicating those changes to the appropriate parties. This way, the lowest access level computers would have the lowest rate of address change. The rate of the address change would increase with the level of access. This system would ensure that all the PCN computers with legitimate access to a particular computer within the PCN would be informed of its location. Furthermore, it will ensure that the current location of a computer with restricted information would be unknown to the parties without the legitimate access clearance. For instance, a superior's computer would be able to access his subordinate's computer but not vice versa.

Also similarly to the systems described for the PCNs, a PCN computer would contain an "address book" where the user can see and use only the permanent side of it with identifiers of all computers accessible to him while the actual communication functions are performed by the computer using the variable side of the "address book" periodically updated by the PN management. To further enhance security, in addition to the computer address system management, the PCN Administrator can implement an automatic security monitoring system where all wrongly addressed log-on attempts would be registered and analyzed for security purposes.

Thus the method and system of the present invention would allow reliable protection against unauthorized remote access to information from within a PN while providing a great deal of flexibility, where the granted access can be revised easily and quickly.

A greatly enhanced intrusion protection system and method can be achieved by combining the operating systems of Figures 1-6. Now an arriving data packet would first be screened by a gateway router or a similar device for a correct destination address. If the destination address is correct, the packet is passed for further processing. If the destination address is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

The packet with correct destination address is then screened for a correct source address. If the source address is correct, the packet is passed to the receiver computer. If the source address is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

Then, the packet with a correct destination address and a correct source address is screened for a correct allowed port coordinate such as port number. If the port coordinate is correct, the packet is passed for further processing. If the port coordinate is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

Finally, the packet with a correct destination and source addresses and a correct port designator is screened for data integrity by application of authentication check such as a checksum. If the authentication check is passed, the packet is passed to the addressee computer. If the authentication check is failed, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

The security managing unit analyses all the alarms and makes decisions on necessary unscheduled changes of addresses for appropriate network servers. Also, it can notify law enforcement and pass appropriate data on to it.

Figure 7 illustrates an enhanced computer intrusion protection system indicated generally at 52 for one or more network computers 54. A gateway router or a bridge 58 includes a destination address filter 60 which receives data packets which pass in through a load distribution switch 62. A non-interrogatable network address book 64 stores current network server addresses for the destination address filter 60, and the destination address filter checks each data packet to determine if a legitimate destination address is present.

Packets with legitimate destination addresses are forwarded to a source address filter 66, while packets with illegitimate destination addresses are sent to a security analysis section 68 in a management unit 70.

When a preset traffic load level is reached indicating that an attempt at flooding is being made, the destination address filter causes the load distribution switch 62 to distribute traffic to one or more parallel gateway routers or bridges which collectively forward legitimate traffic and dump the flooding traffic. An alternative arrangement would call for the load distribution function to be done irrespective of the load, utilizing all the parallel

gateways all the time. A source address table 74 stores accessible server's designators and corresponding current addresses for all system servers which may legitimately have access to the computer or computers 54. These addresses are accessed by the source address filter which determines whether or not an incoming data packet with the proper destination address originates from a source with a legitimate source address entered in the source address table 74. If the source address is determined to be legitimate, the data packet is passed to a port address filter 76. Data packets with an illegitimate source address are directed to the security analysis section 68. Alternatively, source address screening can be done at the gateway router or bridge 58 first prior to port filter 76.

A port protection table 78 includes the current port assignments for the computer or computers 54, and these port assignments are accessed by the port designator filter 76 which then determines if an incoming data packet contains legitimate port designation. If it does, it is passed to an actual address translator 80 which forwards the data packet to the specific computer or computers 54 which are to receive the packet. If an illegitimate port address is found by the port address filter 76, the data packet is transmitted to the security analysis section 68.

The management unit 70 is under the control of a security administrator 82. A network membership master file 84 stores a master list of legitimate server's designators along with respective authorized access lists and corresponding current cyber coordinates. The security administrator can update the master list by adding or removing authorized access for every protected computer. An access authorization unit 86 distributes the upgraded relevant portions of the master lists to the address books of the respective authorized servers.

A random character generator 88 generates random characters for use in forming current port designators, and provides these characters to a port designator forming block 90. This port designator forming block forms the next set of network current port designators in conjunction with the master list and these are incorporated for transmission by a port table block 92. Alternatively, port designators can be formed in the computer unit instead of the management unit.

Similarly, a random character generator 94 generates random characters for use in forming current server addresses, and provides these characters to a server address forming

block 96. This server address forming block forms the next set of current network server addresses, and an address table 98 assigns addresses to servers designated on the master list.

A coordinator/dispatcher block 100 coordinates scheduled move of network servers to their next current addresses, provides the next set of network addresses for appropriate servers and routers and coordinates unscheduled changes of addresses on command from the security analysis unit 68. The coordinator/dispatcher block 100 may be connected to an encode/decode block 102 which decodes received address book upgrades from input 104 and encodes new port and server destination addresses to be sent to authorized servers in the system over output 106. Where encoding of new cyber coordinates is used, each authorized computer in the network will have a similar encoding/decoding unit.

The security analysis unit 68 analyses received illegitimate data packets and detects attack attempts. If needed, the security analysis unit orders the coordinator/dispatcher block 100 to provide an unscheduled address change and diverts the attack data packets to an investigation unit 108. This investigation unit simulates the target server keeping a dialog alive with the attacker to permit security personnel to engage and follow the progress of the attacker while tracing the origin of the attack.

Providing security against intrusion for e-commerce systems presents a unique problem, for an important peculiarity of an e-commerce system is that its address must be publicly known. This aspect represents a contradiction to the requirement of the address being known to authorized parties only. However, the only information intended for the general public usually relates to a company catalog and similar material. The rest of the information on a merchant's network is usually considered private and thus should be protected. Using this distinction, a merchant's e-commerce site should be split into two parts: public and private. The public part is set up on a public "catalog" server with a fixed IP address and should contain only information intended for the general public. The rest of the corporate information should be placed in a separate network and protected as described in relation to Figures 1-7.

When a customer has completed shopping and made purchasing decisions concerning the terms and price of the sale, pertinent for the transaction, information is placed in a separate register. This register is periodically swept by a server handling financial transactions ("financial" server), which belongs to the protected corporate network. In fact,

the "catalog" server does not know the current address of the financial transactions server. Thus, even if an intruder penetrates the "catalog" server, the damage is limited to the contents of the catalog and the intruder cannot get an entry to the protected corporate network.

The financial server, having received pending transaction data, contacts the customer, offering a short-term temporary access for finalizing the transaction. In other words, the customer is allowed access just long enough to communicate pertinent financial data such as a credit card number and to receive a transaction confirmation at which point the session is terminated, the customer is diverted back to the catalog server and the financial server is moved to a new cyber address thus making obtained knowledge of its location during the transaction obsolete.

Dial-up communications systems, in respect to their infrastructure channels susceptibility to transmission intercept by unrelated parties, can be separated into two broad categories: easily interceptable, such as cellular and satellite telephone systems and relatively protected such as conventional land-line based telephone systems. Relatively protected systems such as conventional land-line based telephone systems can be protected in the following way. Phone numbers, assigned by a telephone company to a dial-up telephone-based private network serve as the members' computer addresses. As described previously, such a private network can be protected from unauthorized remote access by implementing periodic changes in the addresses, i.e. telephone numbers assigned to the members for transmission by the network along with other designators such as access codes and communicating the changed numbers to the appropriate parties.

For the conventional land-line dial-up telephone systems, while the "last mile" connection remains constant, the assigned telephone number is periodically changed, making the corresponding computer a moving target for a potential attacker. In this case the telephone company serves as the security system manager. It assigns the current variable telephone numbers to the members of a protected, private network, performs notification of all the appropriate parties, and changes the members' current numbers to a new set at an appropriate time. The telephone company switches naturally serve in the role of routers, and thus they can be programmed to perform surveillance of the system, to detect potential intrusion attacks and to issue appropriate alarms.

Periodically changing the current assigned numbers creates system entropy for a potential intruder, making unauthorized access difficult. Obviously, the implementation of this security system is dependent on availability of sufficient vacant numbers at a particular facility of the telephone company. Furthermore, for a variety of practical reasons it is advisable to keep a just vacated number unassigned for a certain period of time. All this may require additional number capacity at the telephone company facility in order to enable it to provide remote access security to a larger number of personal networks while preserving a comfortable level of system entropy.

If the mentioned additional capacity is not available, or a still higher level of entropy is desired, it could be artificially increased by adding an access code to the assigned number. This would amount to adding virtual capacity to the system, and would make a combination of the phone number and access code an equivalent of a computer's telephone address. In effect, this would make a dialed number larger than the conventional format. This method makes a virtual number capacity practically unlimited and, since the process is handled by computers without human involvement, it should not put any additional burden on a user. With or without a virtual number capacity, utilization of this method allows the intrusion attempts to be easily identified by their wrong number and/or code. At the same time, implementation of this system might require some changes in dialing protocols as well as additional capabilities of the telephone switching equipment.

Entropy density can be increased by limiting the number of allowable connection attempts. Similarly to the method described previously, telephone company switching equipment can be made to perform a role of an outside security barrier for the private network. In this case wrongly addressed connection attempts should be analyzed in order to detect possible "sweeping". If such an attempt is detected, tracing the origin of the attempt and notifying the appropriate phone company should not present a problem even with the existing technology.

The simplest form of private network protection under the proposed method and system is when at a predetermined time all the members of a particular network are switched to the new "telephone book" of the network. However, in some cases required level of security for some members of the same private network could substantially differ, or they may face different levels of security risk. In such cases frequency of the phone number

change could be set individually with appropriate notification of the other members of the network. This differentiation enables the telephone company to offer differentiated levels of security protection to its customers even within the same private network.

A telephone company can also offer its customers protected voice private networks which would provide a higher level of privacy protection than the presently used "unlisted numbers." In this configuration the customers' telephone sets are equipped with a computerized dialing device with remotely upgradeable memory which would allow each member of a protected voice network to contain the network "telephone book" and that book is periodically updated by the telephone company.

The telephone company would periodically change the assigned telephone numbers of a protected network to a new set of current numbers. These new numbers would be communicated to the members of a protected voice network through updating their computerized dialing devices.

As a derivative of the described system, an updateable electronic telephone directory system can be also implemented. In this case a customer's phone set would include a computerized dialing device with electronic memory containing a conventional telephone directory and a personal directory as well. This telephone directory can be periodically updated on-line by the telephone company.

Easily interceptable systems such as cellular and satellite telephone systems, in addition to the protection described above, can be protected from "cloning" when their signals can be intercepted and the "identity" of the phone can be cloned for gaining unauthorized access and use of the system by unauthorized parties.

Mobile telephone and mobile communications systems are protected in a manner similar to networks or land based telephone systems. In this instance, the novel and improved method of changing cyber coordinates is designed to reliably protect mobile phone systems from unauthorized use commonly known as cloning as well as to make intercept of wireless communications more difficult than it is at present. With this system the static wireless phone number or other similar identifier is not used for identification and authorization. Instead, a set of private identifiers is generated known only to the phone company and base stations controlling mobile phone calls and used to continually update the mobile phone and base station directories with current valid identifiers. This approach provides vastly superior

protection over current methods requiring that each call be intercepted in order to track and keep current with changing identifiers. Immediate detection of unauthorized attempts to use a cloned phone is realized and law enforcement may be notified in near real time for appropriate action.

Other electronic devices using wireless communications can be protected by the methods and systems described above.

Finally, computers often contain databases with a variety of information. That information in a database often has wide-ranging levels of sensitivity or commercial value. This creates a situation when large computers serve multiple users with vastly different levels of access. Furthermore, even within the same level of access, security considerations require compartmentalization of information when each user has to have access to only a small portion of the database.

The existing systems try to solve this situation by utilizing passwords and internal firewalls. As it was mentioned earlier, password-based systems and firewalls are not sufficient against computerized attacks. In practical terms it means that a legitimate user with a low level of access, utilizing hacking techniques from his station, potentially can break into even the most restricted areas of the database.

This problem can be solved by using the method of the present invention. A piece of information such as a file or a directory in a computer exists in cyber space. Accordingly, it has its cyber address, usually expressed as a directory and/or a file name which defines its position in a particular computer file system. This, in effect, represents the cyber coordinates of that piece of information within a computer.

As described earlier, information security can be provided if a system manager periodically changes the directories and/or file names in the system, i.e. the cyber addresses of the information, and notifies only appropriate parties of the current file names. This method would ensure that each user computer knows locations of only files to which it has legitimate access. Furthermore, a user would not even know of existence of the files to which he has no access.

To further strengthen the system and make it user-friendly, the user would have a personal directory similar to an address book, where only permanent directory and/or file names are accessible to him, while the variable side of the "address book" would be

accessible only to the system manager and upgraded periodically. In this arrangement variable directory and/or file names can contain any required level of entropy, further increasing resistance to attacks from within the system. Additionally, an internal "router" or "filter" can also perform information security monitoring functions, detect intrusion attempts and issue appropriate alarms in real time.

Obviously, in order to ensure information security in such arrangement any computer-wide search by keywords or subject should be disabled and substituted with a search within specific clients' "address books".

The systems and methods described above allow for creation of a feasible infrastructure protection system such as a national or international infrastructure protection system. When detected at specific points cyber attacks are referred to such a system for further analysis and a possible action by law enforcement authorities.

I claim:

1. A method for protecting a communications device which is connected to a communications system against an unauthorized intrusion which includes:

providing the communications device with at least one identifier,

providing the at least one identifier for use in accessing the communications device to entities authorized to access said communications device,

sensing the presence or absence of said identifier before granting access to said communications device,

providing access to said communications device when the use of said at least one correct identifier is sensed

denying access to said communications device and providing said communications device with at least one new identifier when the absence of the correct at least one identifier is sensed during an attempt to access said communications device, and providing said at least one new identifier to entities authorized to access said communications device.

2. The method of claim 1 which includes periodically changing the at least one identifier and providing the changed at least one identifier to the entities authorized to access said communications device.

3. The method of claim 1 which includes providing said communications device with a plurality of separate identifiers,

sensing the presence or absence of all of said plurality of identifiers before granting access to said communications device,

providing access to said communications device when the use of all of said identifiers is sensed, and

denying access to said communications device and providing said communications device with a new plurality of identifiers to replace the previous plurality of identifiers when the absence of any one of the correct identifiers is sensed.

4. The method of claim 3 which includes periodically changing said plurality of

separate identifiers and providing the changed identifiers to the entities authorized to access said communications device.

5. The method of claim 1 which includes permitting a predetermined number of attempts to access said communications device with a correct at least one identifier after the absence of the correct at least one identifier is sensed before providing said communications device with at least one new identifier,

and providing access to said communications device if the correct at least one identifier is sensed during the predetermined number of attempts to access.

6. The method of claim 2 wherein said communications system is a telephone system and said communications device is a telephone.

7. The method of claim 1 wherein said communications system is a computer network with said entities authorized to access said communications device being authorized computers having access to said computer network, said communications device including at least one host computer having access to said computer network.

8. The method of claim 7 which includes periodically changing the at least one identifier for the host computer and providing the changed at least one identifier to the authorized computers.

9. The method of claim 7 which includes providing the authorized computers with an unchangeable, accessible address for the host computer which is used by the authorized computer to activate and transmit the at least one identifier for the host computer when the authorized computer initiates access to the host computer.

10. The method of claim 8 which includes providing each authorized computer with an authorized computer identifier,

providing the host computer with a destination identifier,

causing each authorized computer to access said host computer with at least a host

computer destination identifier and the authorized computer identifier,

sensing the presence or absence of both said host computer destination identifier and an authorized computer identifier before granting access to said host computer,

providing access to said host computer when the use of both a correct host computer destination identifier and an authorized computer identifier is sensed, and

denying access to said host computer and providing said host computer with a new host computer destination identifier when the absence of either a correct host computer destination identifier or a correct authorized computer identifier is sensed.

11. The method of claim 10 which includes permitting a predetermined number of attempts to access said host computer with both a correct host computer destination identifier and an authorized computer identifier after the absence of a correct host computer destination identifier or an authorized computer identifier is sensed before providing said host computer with a new host computer destination identifier, and

providing access to said host computer if correct host computer destination and authorized computer identifier are sensed during the predetermined number of attempts to access the host computer.

12. The method of claim 11 which includes storing said host computer destination identifier as an inaccessible identifier in said authorized computers, and providing said authorized computers with an unchangeable, accessible host computer address, which will activate and transmit the host computer destination identifier when an authorized computer initiates access to the host computer.

13. The method of claim 8 which includes providing said host computer with a host computer destination identifier and a host computer port identifier,

causing each authorized computer to access said host computer with at least the host computer destination identifier and the host computer port identifier,

sensing the presence or absence of both said host computer destination identifier and said host computer port identifier before granting access to said host computer,

providing access to said host computer when the use of both a correct host computer

destination identifier and a correct host computer port identifier are sensed, and

denying access to said host computer and providing said host computer with a new destination identifier and port identifier when the absence of either or both of a correct host computer destination or port identifier is sensed.

14. The method of claim 13 which includes permitting a predetermined number of attempts to access said host computer with both a correct host computer destination and port identifier when either or both an incorrect host computer destination or port identifier is sensed before providing said host computer with a new destination and port identifier, and

providing access to said host computer if both correct host computer destination and port identifiers are sensed during the predetermined number of attempts to access said host computer.

15. The method of claim 14 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computers and providing said authorized computers with an unchangeable, accessible host computer address which will activate and transmit the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

16. An intrusion protection method for protecting a host computer connected to a computer communications system which includes one or more authorized computers having access to said computer communications system which are authorized to access said host computer which includes:

providing each authorized computer with an authorized computer identifying address,

providing said host computer with a host computer destination identifier and a host computer port identifier,

providing said host computer destination identifier and said host computer port identifier to said authorized computers,

causing each authorized computer to access said host computer with the host computer destination and port identifiers and said authorized computer identifying address,

sensing the presence or absence of said host computer destination and port identifiers

and said authorized computer identifying address before granting access to said host computer,

providing access to said host computer when the use of correct computer destination and port identifiers and a correct authorized computer identifying address is sensed, and

denying immediate access to said host computer when the absence of any one or more of the correct host computer destination and port identifiers or the authorized computer identifying address is sensed.

17. The method of claim 16 which includes periodically changing the host computer destination and port identifiers and providing these changes to the authorized computers.

18. The method of claim 17 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and transmit the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

19. The method of claim 16 which includes changing the host computer destination and port identifiers when access is denied to said host computer after at least one access attempt has been made and providing these changed identifiers to the authorized computers.

20. The method of claim 16 which includes permitting a predetermined number of attempts to access said host computer with correct host computer destination and port identifiers and a correct authorized computer identifying address after the absence of at least a correct one of said identifiers and authorized computer identifying address is sensed by the host computer and

providing access to said host computer if correct host computer destination and port identifiers and a correct authorized computer identifying address are sensed during the predetermined number of attempts to access said host computer.

21. The method of claim 19 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and cause transmission of the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

22. The method of claim 20 which includes changing the host computer destination and port identifiers when access is denied to said host computer after at least one access attempt has been made and providing these changed identifiers to the authorized computers.

23. The method of claim 22 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and cause transmission of the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

24. A method of communication with a remote entity over a communication system which includes

providing the remote entity with at least one remote entity cyber coordinate identifier,

providing the remote entity cyber coordinate identifier to one or more base entities authorized to communicate with said remote entity,

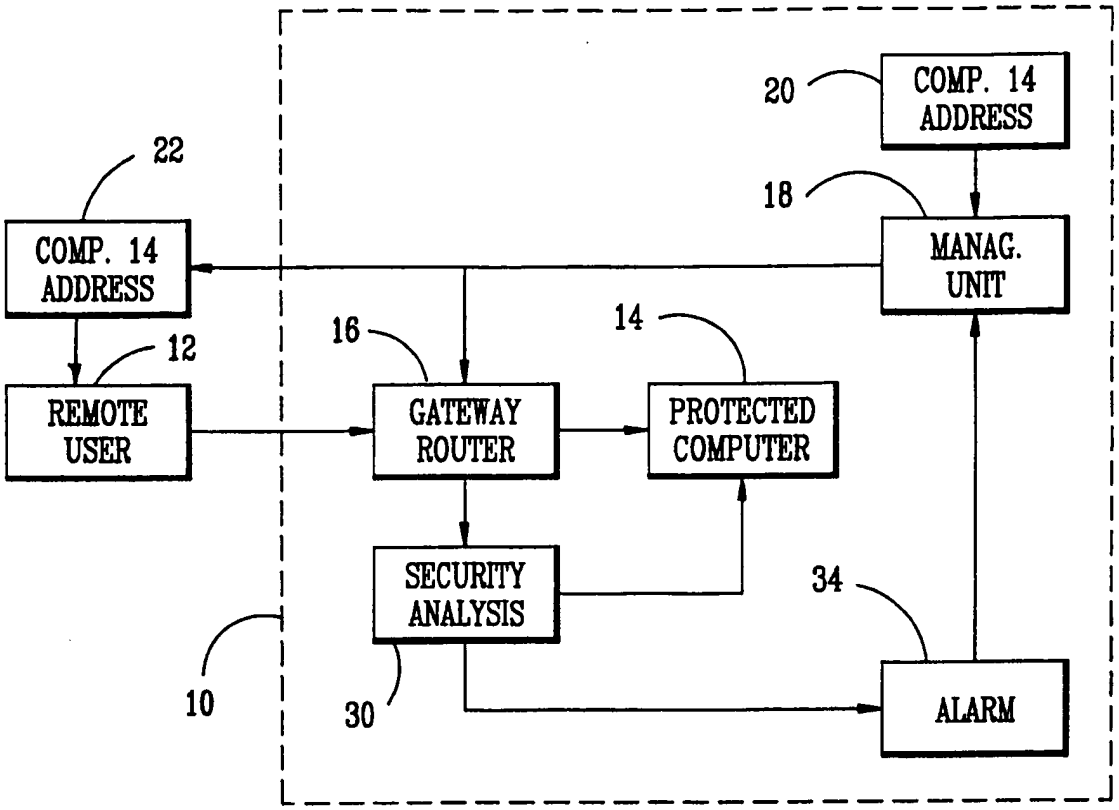
periodically changing the remote entity cyber coordinate identifier to a new remote entity cyber coordinate identifier and

providing the new remote entity cyber coordinate identifier to said one or more base entities.

25. The method of claim 24 which includes changing the remote entity cyber coordinate identifier to a new cyber coordinate identifier in response to an attempt to communicate with said remote entity with an incorrect remote entity cyber coordinate identifier and

providing the new remote entity cyber coordinate identifier to said one or more base entities.

FIG. 1



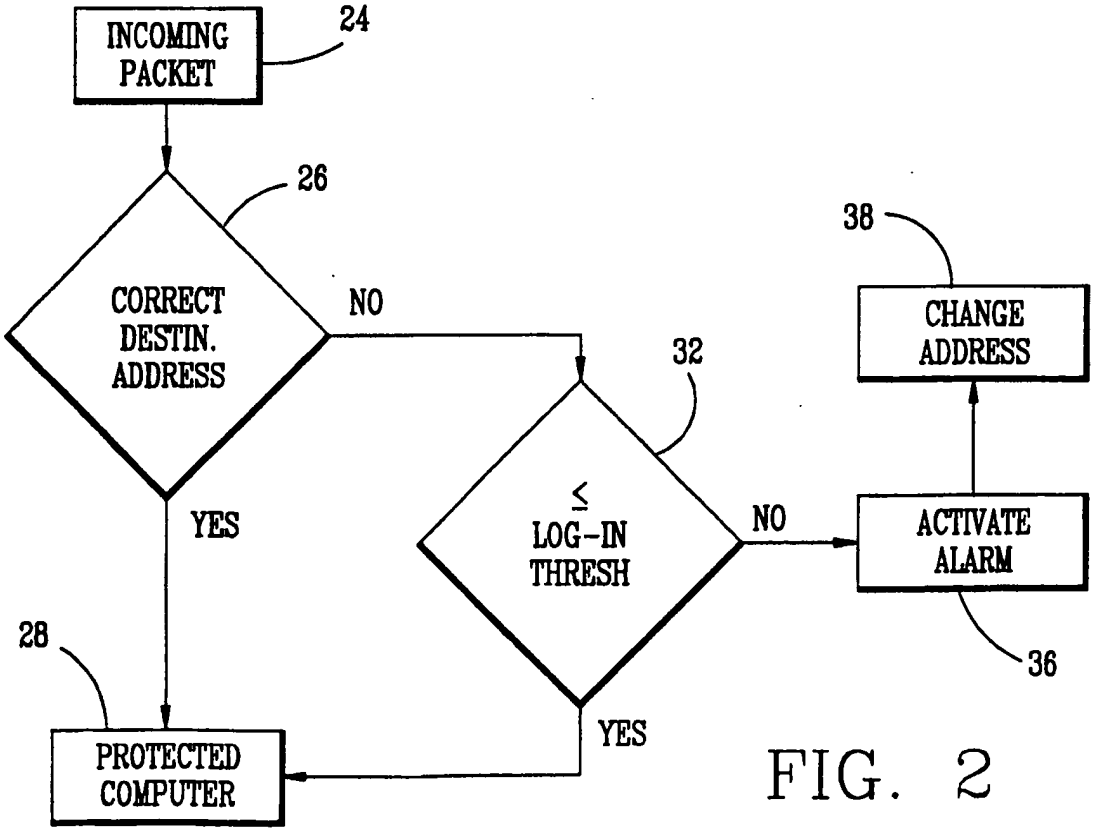


FIG. 2

Petitioner Apple Inc. - Exhibit 1026, p. 612

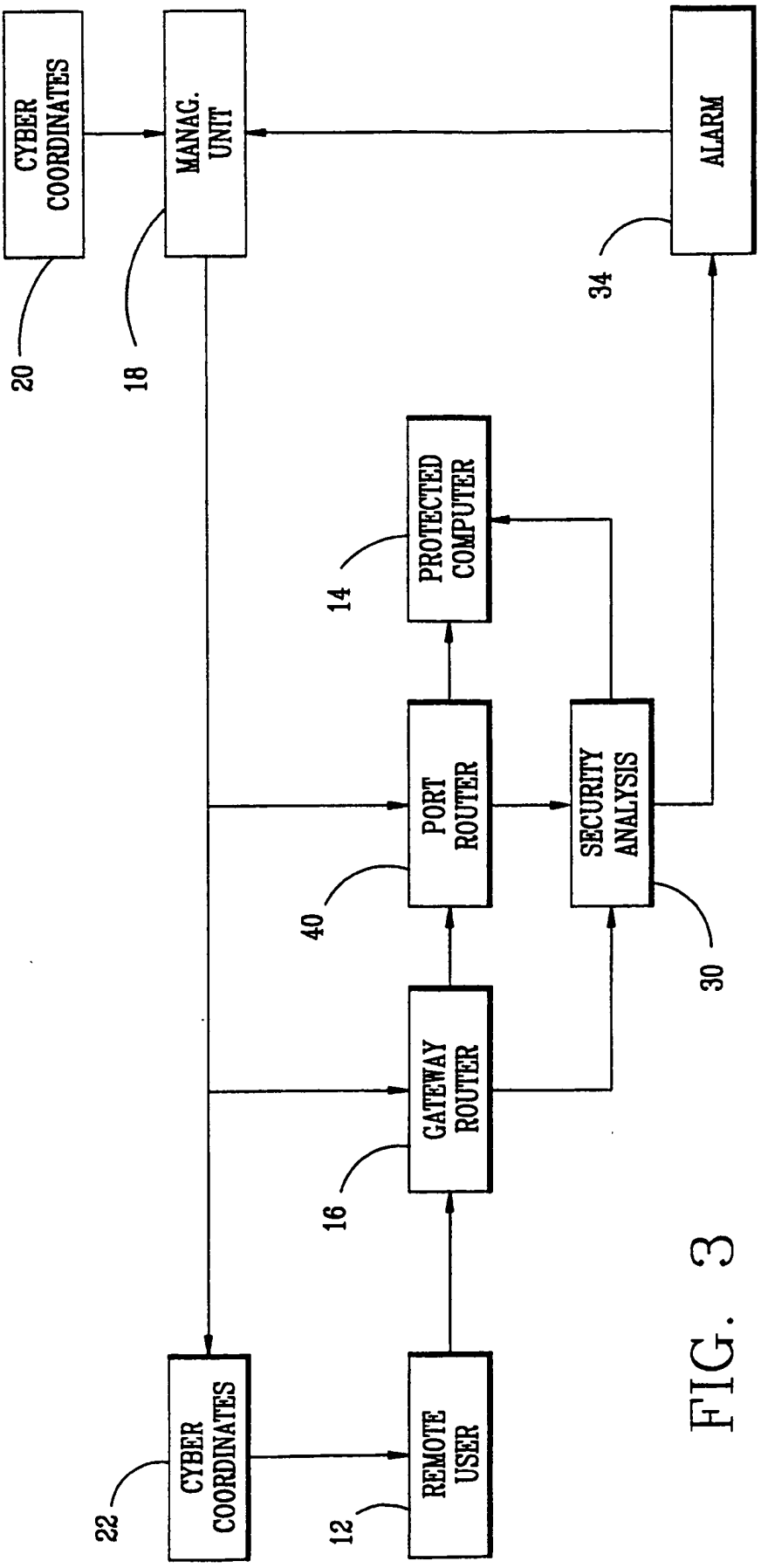

CYBER COORDINATES
MANAG. UNIT
ALARM
20
18
34
PROTECTED COMPUTER
14
PORT ROUTER
SECURITY ANALYSIS
40
30
GATEWAY ROUTER
16
CYBER COORDINATES
REMOTE USER
22
12

FIG. 3

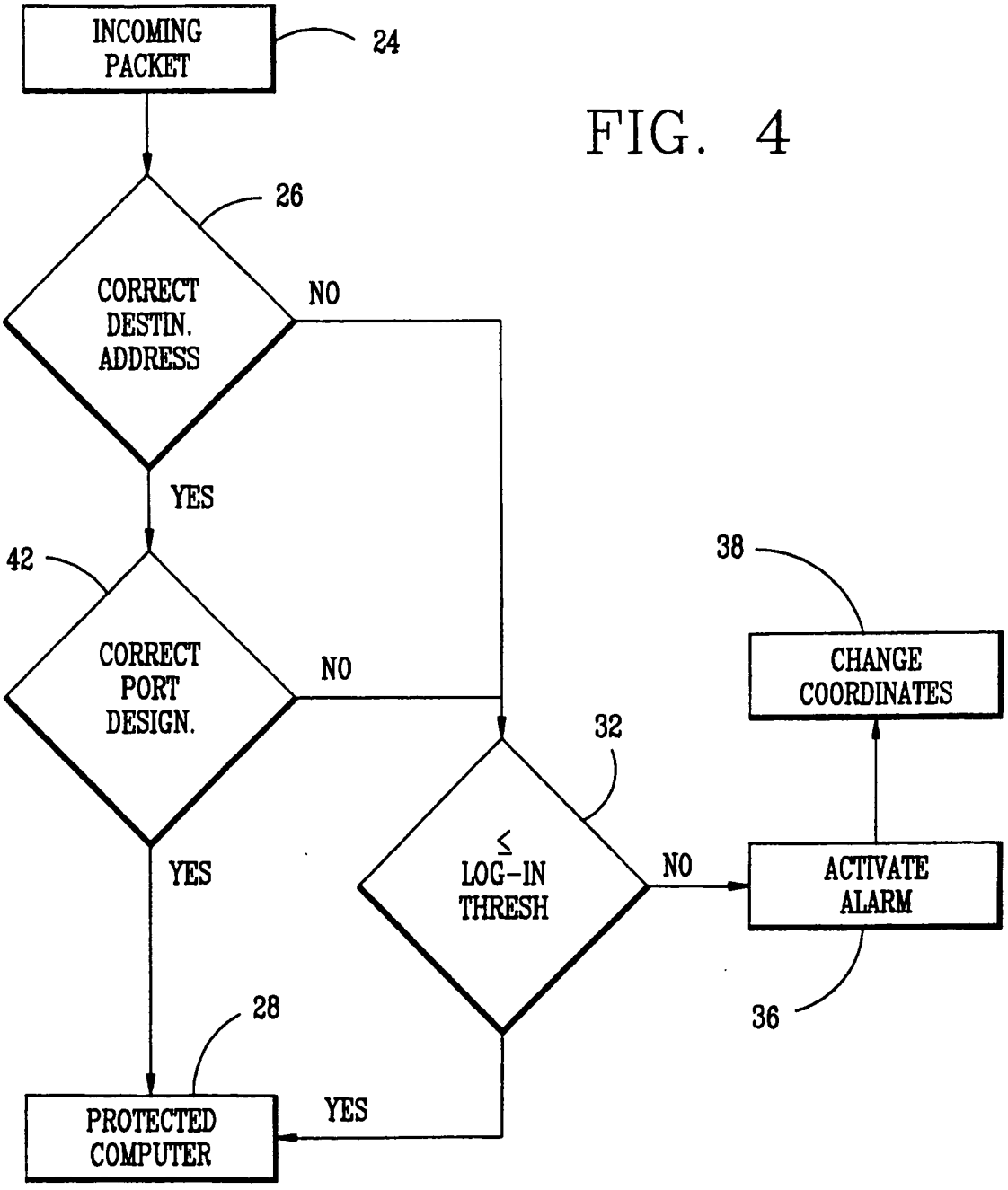

INCOMING PACKET
24
26
CORRECT DESTIN. ADDRESS
NO
YES
42
CORRECT PORT DESIGN.
NO
YES
32
≤
LOG-IN THRESH
NO
38
CHANGE COORDINATES
ACTIVATE ALARM
36
28
PROTECTED COMPUTER
YES

FIG. 4

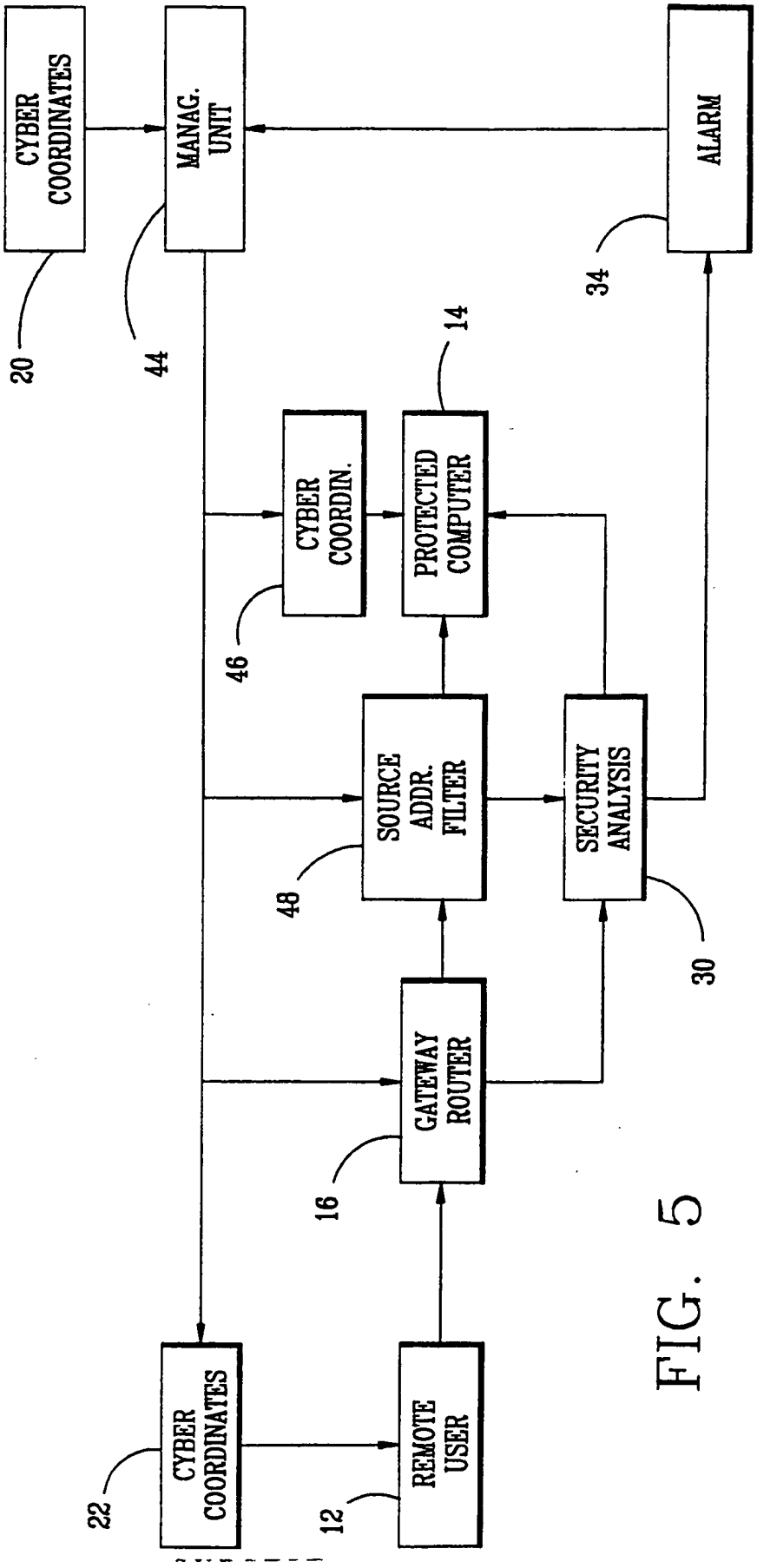

CYBER COORDINATES
MANAG. UNIT
ALARM
20
44
34
14
CYBER COORDIN.
PROTECTED COMPUTER
46
SOURCE ADDR. FILTER
SECURITY ANALYSIS
48
30
GATEWAY ROUTER
16
CYBER COORDINATES
REMOTE USER
22
12

FIG. 5

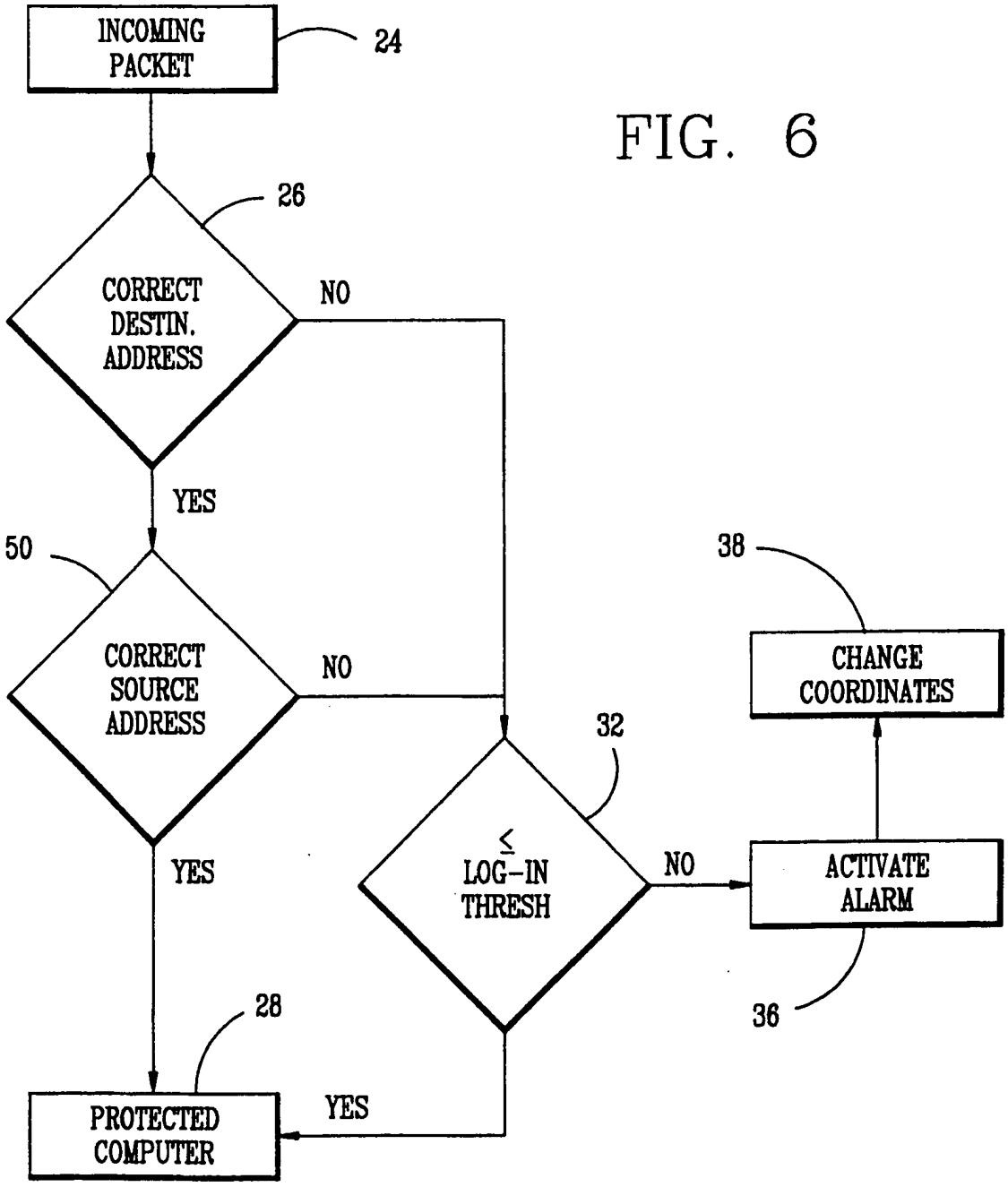
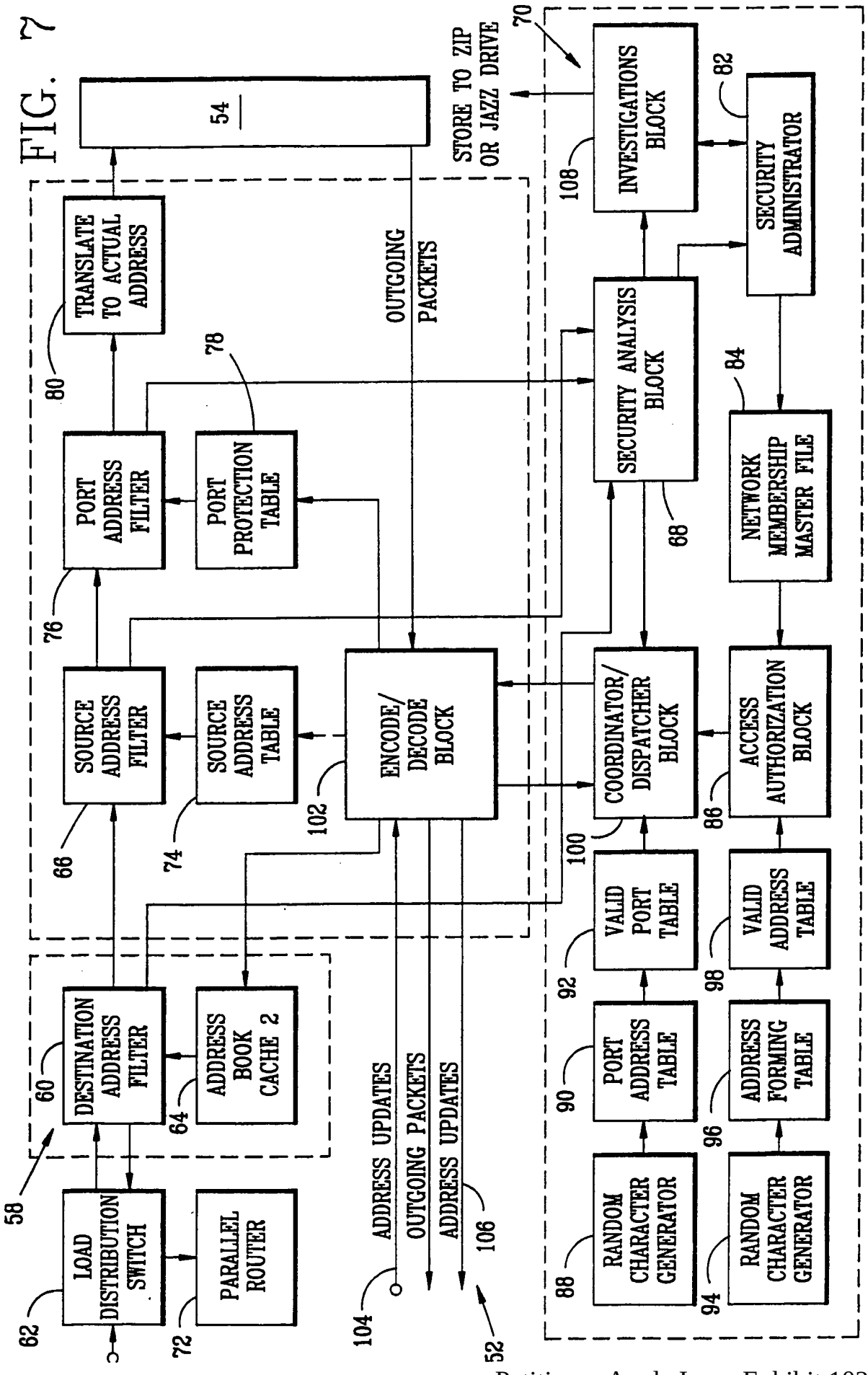

INCOMING PACKET
24
26
CORRECT DESTIN. ADDRESS
NO
YES
50
CORRECT SOURCE ADDRESS
NO
YES
32
≤ LOG-IN THRESH
NO
38
CHANGE COORDINATES
ACTIVATE ALARM
36
28
PROTECTED COMPUTER
YES

FIG. 6

FIG. 7



Petitioner Apple Inc. - Exhibit 1026, p. 617

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08219

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 11/00
US CL : 713/201

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/201,200,202; 340/825.31,825.34; 380/255;

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS US PATENT FILE; WEST; JPAB; EPAB; DWPI; TDBD;

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,805,801 A (HOLLOWAY ET AL) 08 SEPTEMBER 1998, Entire document.	1-25
Y	US 5,796,942 A (ESBENSEN) 18 AUGUST 1998, Entire document.	1-25
Y,P	US 5,905,859 A (HOLLOWAY ET AL) 18 MAY 1999, Entire document.	1-25
Y	US 5,892,903 A (KLAUS) 06 APRIL 1999, Entire document.	1-25
A	US 5,537,099 A (LIANG) 16 JULY 1996, Entire document.	1-25
A	US 5,278,901 A (SHIEH ET AL) 11 JANUARY 1994, Entire document.	1-25

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 20 JULY 2000	Date of mailing of the international search report 22 AUG 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer NADEEM IQBAL Telephone No. (703) 308-5228

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08219

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,991,881 A (CONKLIN ET AL) 23 NOVEMBER 1999, Entire document.	1-25

Form PCT/ISA/210 (continuation of second sheet) (July 1998)★

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

B1002

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 March 2001 (08.03.2001)

PCT

(10) International Publication Number
WO 01/016766 A1

(51) International Patent Classification[7]: G06F 13/00

(21) International Application Number: PCT/US00/23774

(22) International Filing Date: 31 August 2000 (31.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/151,563 31 August 1999 (31.08.1999) US

(71) Applicant: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION [US/US]; 10260 Campus Point Drive, San Diego, CA 92121 (US).

(72) Inventors: WHITTLE, Bryan; 73 Zion-Wertsville Road, Skillman, NJ 08558 (US). TESINK, Kaj; 140 Park Road, Fair Haven, NJ 07704 (US).

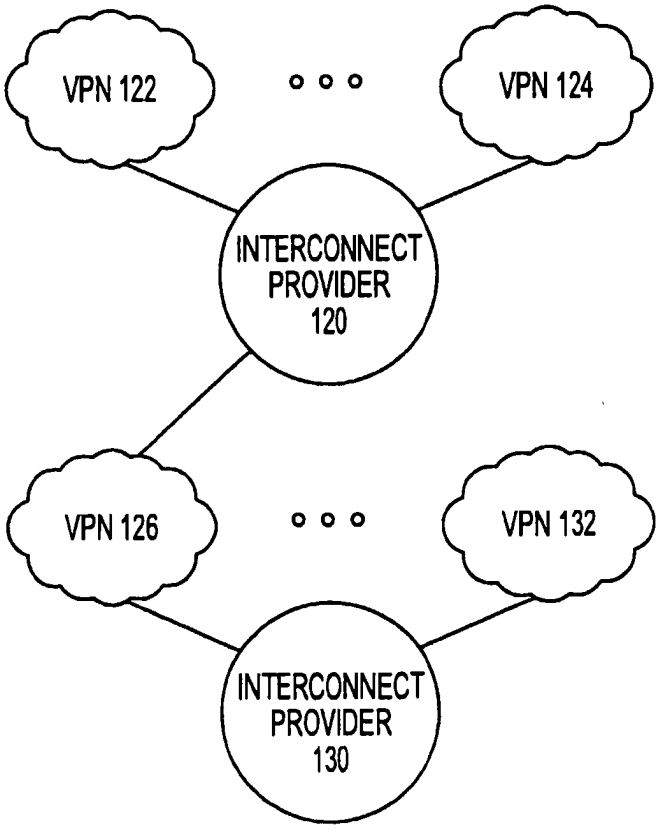
(74) Agents: ROBINSON, Douglas, W. et al.; Banner & Witcoff, Ltd., Eleventh Floor, 1001 G Street, N.W., Washington, D.C 20001-4597 (US).

(81) Designated States *(national)*: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR INTERCONNECTING MULTIPLE VIRTUAL PRIVATE NETWORKS



(57) Abstract: A system and method for interconnecting multiple VPNs (122, 124, 126, 132), each using multiple service providers (120, 130), while offering a minimum standard of end-to-end connection quality and reliability. The system and method utilizes an overseer that resolves end-to-end issues across multiple interconnected virtual private networks (122, 124, 126, 132). When connecting multiple virtual private networks (122, 124, 126, 132) multiple interconnect providers (120, 130) are interconnected so that the end-to-end service quality standard. The certification of service providers, exchange points, transit service providers and IPSec devices permits interoperability for encryption, integrity and authentication across the product of all IPSec vendors. When two subscribers both use certified IPSec equipment then they can provide each other with controlled access to each other's networks.

WO 01/016766 A1

Published:
— *with international search report*

(48) Date of publication of this corrected version:
12 September 2002

(15) Information about Correction:
see PCT Gazette No. 37/2002 of 12 September 2002, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR INTERCONNECTING MULTIPLE VIRTUAL PRIVATE NETWORKS

This application claims priority to the following provisional patent applications, which are incorporated herein by reference in their entireties:

(1) Provisional Application Serial No. 60/151,563, titled "Method & Apparatus For a Globalized Automotive Network & Exchange," filed on August 31, 1999, and having reference no. 99,532 (479.83581).

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to virtual private networks. More particularly, the present invention relates to virtual private networks wherein in each virtual private network, multiple service providers can be utilized by the trading partners of the virtual private network. The end-to-end service quality of the connection within the virtual private network is guaranteed to meet minimum requirements. The end-to-end service quality encompasses numerous factors including: network services; interoperability; performance; reliability; disaster recovery and business continuity; security; customer care; and trouble handling. The system and method of the present invention is directed to the interconnection of multiple virtual private networks each having multiple service providers. Furthermore the present invention encompasses a system and method for interconnecting multiple interconnect providers, such as exchange points, exchange networks, direct connect or transit service providers, between the multiple virtual private networks. Finally, the present invention employs an end-to-end overseer across the multiple virtual private networks.

Description of the Related Art

Early in 1994, the automotive industry recognized the need for global network services that would support more new demanding automotive business applications. The purpose of this network service was to simplify complex, redundant, outdated connection methods while minimizing costs and ensuring the management, security, reliability, and performance essential to the automotive industry. Transport Control Protocol/Internet Protocol (TCP/IP) was endorsed as the standard suite for electronic data communications.

Petitioner Apple Inc. - Exhibit 1026, p. 622

Ultimately in 1995, the industry formed a Telecommunications Project Team to oversee the design and development of a common global communication infrastructure supporting automotive industry application initiatives (later called the Automotive Network eXchange (ANX) Implementation Task Force). The Task Force, in June 1997, published the initial results of the technical design process for this new network service, called the Automotive Network eXchange (ANX), in "ANX Release 1 Draft Document Publication" (TEL-2 01.00). This reference is incorporated herein by reference in its entirety. The TEL-2 specification undergoes constant updating and correction.

The ANX system is a business-to-business communications infrastructure that provides a uniform, secured link between trading partners, such as manufacturers and suppliers, in the automotive industry. The ANX is a subscription-based network composed of Certified Service Providers (CSP). CSPs are providers of IP network service that have satisfied certain service end-to-end quality. CASPs are certificate authority service providers. The Certified Exchange Point Operator (CEPO) provides services to interconnect CSPs. CEPOs also must satisfy certain end-to-end service quality requirements.

Trading Partners (TP) are registered end users, or subscribers, of the ANX system such as automotive parts manufacturers, suppliers, original equipment manufacturers, and car manufacturers. The ANX system allows TPs to communicate, exchange information, and transact business with other TPs over the ANX network. The TP may utilize any TCP/IP-compliant application program to exchange information with other TPs. The registered TP selects the TPs with which it wants to communicate and thereafter may gain access to and receive communications from those selected TPs. As a result, the ANX system allows each TP to develop its own virtual private network with its customers and vendors.

The ANX system significantly reduces the complexity of connecting to multiple trading partners. Since there are diverse communication protocols for the trading partners, separate links are required to access each trading partner.

By having a single private network operated under a uniform protocol, interconnectivity between various trading partners is substantially simplified. In addition, ANX offers improved end-to-end service quality. For example, if an auto manufacturer needs to place with its parts supplier an order for car seats, the

Petitioner Apple Inc. - Exhibit 1026, p. 623

manufacturer may submit over the ANX system its confidential CAD drawings directly to the supplier. The manufacturer may also fill out the order form that the supplier may have for filling orders and timely submit over the ANX system due to its high reliability and performance.

The CSP and the CEPO must satisfy certain performance and security requirements in order to be certified under the ANX. The certification process is disclosed in ANX Release 1 Document Publication (TEL-2 02.00), which is incorporated herein by reference in its entirety.

The ANX VPN permits the use of a plurality of different IPSec devices. By virtue of the TEL-2 specification and the certification process all of the designated IPSec device are guaranteed to communicate with one another across the ANX VPN.

While the ANX was originated out of the need to interconnect automotive related companies, it is not limited to that industry. Any company/industry may become a TP, e.g. an aerospace company, a healthcare company, etc. ANX has become known as the Advanced Network eXchange.

With the advent of the Internet, global communication has become a reality. While the Internet works well for non-mission critical applications, such as transmitting and receiving e-mail and hosting websites, it has some drawbacks for business-to-business commerce and communication that require stringent end-to–end service quality. Quality concerns are in the area of end-to-end service quality as explained previously.

For example, when two companies want to communicate over the Internet, the lag between the systems at each company will be different virtually every time. The connection each has through their service provider, i.e. 14.4K, 28.8K, 56K, ISDN, DSL, T1, etc., plus the number of servers through which the connection is directed contribute to the resulting time lag between the two companies. Depending upon the type of information transmitted, the two parties may require a maximum acceptable time lag. Due to the nature of the Internet, it cannot guarantee such a maximum time lag. Furthermore, the two companies may desire that service assistance be available at certain times or 24 hours a day. The Internet has no such guarantees for help availability in a multi-provider environment. Such a lack of guaranteed bandwidth, latency and reliability are major impediments to business-to-business commerce and communication over the Internet.

Petitioner Apple Inc. - Exhibit 1026, p. 624

In recent years the number of electronic viruses and hacker attacks has increased dramatically. A company considering conducting business-to-business commerce over the Internet runs the risk of making their intranet vulnerable to such viruses and attacks with the potential related loss of data.

In order to address the security issue, some companies have developed virtual private networks (VPNs). Secure VPNs permit a company to communicate with any other entity on the network without the risk of increased vulnerability to viruses and hackers. However, while VPNs can connect to other VPNs over the Internet by providing authentication, access control, confidentiality and data integrity, there is still no way the end-to-end quality of the connection can be guaranteed to meet a required set of minimum standards in a multi-provider setting.

A secure VPN is a communication network that is secured with encryption and authentication. Secure VPNs are based on multiple technologies, for example IPSec, tunneling, certification and shared secret authentication. IPSec is the security standard established by the Internet Engineering task Force (IETF). Tunneling permits private networks to cross the Internet using unregistered IP addresses.

SUMMARY OF THE INVENTION

From the foregoing, it is desirable to provide a system and method for interconnecting multiple VPNs each using multiple service providers while offering a minimum standard of end-to-end service quality.

The system and method of the present invention utilizes an overseer that defines the service quality, continually qualifies service providers as meeting that service quality, and resolves end-to-end issues across multiple interconnected virtual private networks, such as the ANX. When connecting multiple virtual private networks according to the system and method of the present invention multiple interconnect providers are interconnected, and the manner in which these interconnect providers are interconnected so that the quality and reliability standards is met are another aspect of the present invention.

Certification of IPSec devices permits interoperability for encryption, integrity and authentication across the product of all IPSec vendors. When two subscriber companies both use certified IPSec equipment then they can provide each other with controlled access to each other's networks.

Petitioner Apple Inc. - Exhibit 1026, p. 625

Based on the foregoing, an object of the present invention is to provide a system and method of interconnecting multiple VPNs each using multiple service providers while offering a minimum standard of end-to-end connection quality and reliability.

Another object of the present invention is to provide a system and method of interconnecting multiple VPNs having an overseer that resolves end-to-end issues across multiple virtual private networks.

Still another object of the present invention is to provide a system and method of connecting multiple virtual private networks in which multiple interconnect providers are interconnected so that the end-to-end service quality is met.

DETAILED DESCRIPTION OF THE DRAWINGS

The foregoing and other attributes of the present invention will be described with respect to the following drawings in which:

Fig. 1 is a block diagram of two interconnected virtual private networks according to the present invention;

Fig. 2 is a configuration of governance and management of separate virtual private networks;

Fig. 3 is a configuration of governance and management of interconnected virtual private networks according to the present invention;

Fig. 4 is an interconnection configuration for governance of multiple interconnected virtual private networks according to the present invention;

Fig. 5 is a flow chart showing contractual obligations according to the present invention;

Fig. 6 is a diagram illustrating end-to-end latency in a virtual private network having multiple service providers;

Petitioner Apple Inc. - Exhibit 1026, p. 626

Fig. 7 is a diagram illustrating end-to-end availability in a virtual private network having multiple service providers;

Fig. 8 is a diagram illustrating trouble handling in a virtual private network having multiple service providers;

Fig. 9 is a diagram illustrating an accountability model for a single virtual private network having multiple service providers;

Fig. 10 is a diagram illustrating an accountability model for multiple virtual private networks having multiple service providers according to the present invention;

Fig. 11 is a diagram illustrating end-to-end interconnection of two virtual private networks according to the present invention;

Fig. 12 is a diagram illustrating a trouble escalation model for interconnection of two virtual private networks according to the present invention;

Fig. 13 is a diagram illustrating a multiple virtual private network fee model for interconnection of two virtual private networks according to the present invention; is a diagram illustrating interconnection of two virtual private networks using a multiple transit certified service providers according to the present invention;

Fig. 14 is a diagram illustrating interconnection of two virtual private networks using a single transit certified service provider according to the present invention;

Fig. 15 is a diagram illustrating interconnection of two virtual private networks using a multiple transit certified service providers according to the present invention;

Figs. 16 is a diagram illustrating interconnection of multiple virtual private networks using a multiple transit certified service providers, where no single transit

Petitioner Apple Inc. - Exhibit 1026, p. 627

certified service provider connects all of the virtual private networks according to the present invention; and

Figs. 17a - c are alternative configurations for interconnecting multiple virtual private networks according to the present invention.

Petitioner Apple Inc. - Exhibit 1026, p. 628

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 1 shows a block diagram of two interconnected virtual private networks 20 and 22. The present system and method of the interconnecting multiple virtual private networks is not intended to be limited to only these types of networks and has applicability to a wide variety of virtual private networks.

Each virtual private network 20 and 22 is shown having a trading partner (TP) 24 and 26, respectively. While Fig. 1 shows only one TP 24 and 26 for each virtual private network, there can in fact be hundred or thousands of such TPs for each virtual private network. Fig. 1 is intended to define the end-to-end service quality concept, and for such a purpose, only one TP 24 and 26 is need for each virtual private network 20 and 22.

The end-to-end service quality, provided by the present system and method of interconnecting multiple virtual private networks, cannot be achieved by simply interconnecting two virtual private networks, such as 20 and 22, with a wire. The end-to-end service quality incorporates a user-centric philosophy, where the user is the TP or subscriber. The user is guaranteed a minimum level of service encompassing factors that include: network services; interoperability; performance; reliability; disaster recovery and business continuity; security; customer care; and trouble handling. Simply connecting the two virtual private networks 20 and 22 with a wire will not achieve the minimum satisfactory levels for these factors.

To achieve such minimum levels of satisfactory performance for these factors the system and method must include a way to resolve disputes between the two virtual private networks. Referring to Fig. 2, each VPN 20 and 22 is shown as having its own governance, program management, coopetition policy, contracts, service assurance, and service description. While each virtual private network can operate with a successful level of end-to-end service quality when each VPN is not interconnected to another VPN, the governance, program management, coopetition policy, contracts, service assurance, and service description may need to be revised when interconnecting two or more VPNs in order to maintain the end-to-end service quality. It will be appreciated that at the very least the interconnection of at least two VPNs adds at least one additional level of complexity with regard to service between the VPNs.

Petitioner Apple Inc. - Exhibit 1026, p. 629

One resolution is shown in Fig. 3, in which each VPN 20 and 22 maintain their own governance, but the program management, coopetition policy, contracts, service assurance, and service description for the two VPNs 20 and 22 are unified. Such unification means that where the parameters for the program management, coopetition policy, contracts, service assurance, and service description of the two VPNs 20 and 22 are different, the parameter used in one of the networks is chosen as the acceptable minimum standard or a compromise parameter different from the parameter used in each or the VPNs is agreed upon. It is possible that the parameters for communication within each VPN need not change, while the new parameters are used only when communicating between VPNs. Fig. 3 further shows that the system and method contemplate connecting more than two VPNs.

One configuration for governance of multiple interconnected VPNs is shown in Fig. 4. In this scenario each VPN has its own program overseer (POVER) 30, and a global, or multiple virtual private network, overseer 32 is provided to resolve issues between the POVERs 30. Arrows are shown between the POVERs 30 indicating that the POVERs 30 are free to resolve their issues without requiring the GOVER 32. The GOVER is called on when direct POVER-to-POVER resolution fails. Each of the POVERs 30 governs one of the regional VPNs, while the GOVER 32 oversees the interconnection of the VPNs.

The GOVER is responsible for end-to-end quality assurance, and in particular acts as an inter-VPN interconnection certifier. The GOVER certifies interconnection facilities, and certifies a global CASP-CASP trust model. The GOVER also is an inter-VPN arbitrator that steps in when POVERs cannot resolve trouble between them.

Since the VPNs are used to running their networks in isolation, the interconnection of multiple VPNs has unique issues such as resolving trouble and conflicts between the VPNs and maintenance of minimum end-to-end service quality across the multiple programs. Since the system and method of the present invention are directed to providing specific end-to-end service quality, it must be possible for TPs to quantify the end-to-end service quality levels, and these service quality levels must be sufficient to allow applications to work across the multiple VPNs. Therefore, a high level of metric compatibility and measurement techniques are required.

Petitioner Apple Inc. - Exhibit 1026, p. 630

In the ANX type VPN each TP, CSP and CEP must meet specified criteria to become certified and to maintain that certification. The certification provides the TPs or subscribers with confidence that the level or transport and security will meet their business needs. The ANX type VPN utilizes multiple CSPs. On one level it is easier to run a VPN where all TPs are required to use a single CSP. The use of multiple CSPs in the ANX type VPN fosters competition between the CSPs and allows the VPN to reach TPs that may not be serviced by a single CSP. The implementation of multiple CSPs, however, brings with it the drawback of insuring that the CSPs can talk to one another. Whether the connection from one TP to another TP within the same VPN is through a single CSP of two CSPs should be invisible to the TPs. The TPs need never know when one or more CSPs are used for any particular connection. The certification process ensures that the TPs use one of the certified IPSec devices at their premises, and that the CSPs will utilize certified equipment and meet certain metrics so as to achieve the end-to-end service quality guaranteed to the TPs. In this manner, the multiple CSPs will be able to communicate with one another. The CSPs must meet business criteria, technical metrics, ongoing monitoring, trouble-handling criteria, routing registry criteria, and domain name registry criteria to achieve and maintain certification.

Fig. 5 shows the contractual obligations of the members of an ANX-type VPN. The TPs 40 contract with the VPN, as denoted in Fig. 5 by the arrows to the overseer 50, and contract with one of the multiple CSPs 42. The CSPs contract with the VPN and with the CEPO 44. The CEPO 44 contracts with the VPN. Each entity is responsible for the services that that entity provides.

The technical metrics for achieving end-to-end service quality in the ANX-type network include among other metrics, latency and availability. Fig. 6 illustrates the end-to-end latency within the ANX network. The TP1 router 60 is connected to ANX CSP_1 62, which in turn is connected to ANX CEPO 64. TP2 router 66 is connected to ANX CSP_2 68, which is connected to ANX CEPO 64. The packet latency from each router 60 and 66 through the corresponding CSP is 125 msec. The latency through the ANX CEPO is on the order of microseconds. The total packet latency through the network is therefore only slightly more than 250 msec.

Fig. 7 illustrates the end-to-end availability metric. The Access network between the TP1 router 60 and the ANX CSP_1 62 is permitted to be unavailable 43.80

Petitioner Apple Inc. - Exhibit 1026, p. 631

hours/year. The ANX CSP_1 62 may only be unavailable 2.63 hrs./year. The trunk 65 between the ANX CSP_1 62 and the ANX CEPO may only be unavailable 1.76 hrs./year. The ANX CEPO may only be unavailable 0.44 hours/year. The foregoing availabilities yield a total of 99.895% availability or 9.22 hours per year downtime.

The outline for how trouble is handled within the ANX-type VPN is shown in Fig. 8. There are effectively five layers of trouble handling. At the first level trouble between TPs is handled directly between the two TPs. Similarly, issues between the TPs and the CSPs are handled between the two parties. CSPs and the CEPOs also resolve their troubles between the troubled parties. A network overseer is provided to handle troubles that cannot be handled in the foregoing scenarios. The overseer can take complaints from the TPS, the CSPs, and the CEPOs.

A key to providing predictable end-to-end service quality is that the TPs must know the level of service they receive. To this end four service provider accountability levels exist. First, service providers, both interconnect providers and CSPs, must timely fix infrequent service provider troubles. Second, there must be end-to-end service provider cooperation to handle any troubles. Third, recourse must be provided to resolve disputes in the event of disagreement between CSPs and/or interconnect providers. Fourth, recourse must be provided to resolve continued non-compliance with the end-to-end service quality.

Referring to Figs. 9 and 10, charts for single VPN and interconnected VPNs are shown, respectively. In Fig. 9, the CSPs 70, CEPOs 72 and CASPs 74 are accountable to the POVER 76. The POVER 76 is accountable to the body 78 representing the TPs. The body 78 is accountable a regional/national arbitration body 80. Where multiple VPNs are interconnected in Fig. 10, the CSPs 70, the CEPOs 72, and CASPs 74 are accountable to the POVERs 76. The POVERs 76 are accountable to a GOVER 77, which in turn is accountable to the body 78. The body 78, instead of being accountable to the regional/national arbitration body 80, is accountable to an international arbitration body 82.

The GOVER/POVER model is but one way to oversee ensuring of the end-to-end service quality and metric compatibility. How the ANX-type networks are connected will be discussed below. In this context there must be five key types of end-to-end technology compatibility: 1 network interconnection that ensures a trading partner on one VPN can reach any trading partner on the other VPN; 2 routing

Petitioner Apple Inc. - Exhibit 1026, p. 632

compatibility that ensures any trading partner on one VPN can logically reach nay TP on the other VPN; 3 naming compatibility, e.g. so the web names or e-mail names of any trading partner on one VPN can be resolved to an address that is routable over the two VPNs; 4 IPSec compatibility; and 5 digital security certificate compatibility across multiple VPNs. While Figs. 9 and 10 refer to regional/national VPNs and international arbitration, the VPNs need not be limited to a specific country or geographical area. Any ANX-type VPN, regardless of the location of its subscribers could be interconnected.

While Fig. 1 illustrated the interconnection of two VPNs 20 and 22, a significant element is missing. Fig. 11 shows two VPNs, that have multiple service providers, which are connected through an inter-program service provider, also called an interconnect provider. The Tel-2 specification is still used as the basic guide in determining the end-to-end service quality, however regional or particular VPN peculiarities, referred to as deltas, must be considered when establishing the interconnected end-to-end service quality standards.

Returning to the GOVER/POVER model for overseeing interconnected VPNs; Fig. 12 illustrates an end-to-end trouble escalation model. It is expected that CSPs will work together to resolve trouble before contacting a POVER. Similarly, the POVERs and/or the POVERS and the interconnect provider are expected to work together to resolve trouble before contacting the GOVER.

When expanding from a single VPN to interconnected VPNs the inherent costs of running the system naturally increase. How such costs are distributed is an important part of the system. As shown in Fig. 13, the POVERs 100 pay fees to the GOVER to offset the costs of maintaining the GOVER. The VPNs having multiple service providers in turn pay fees to support the POVER. Furthermore the interconnect providers pay a certification fee to the GOVER for certification as a interconnect provider between VPNs.

There are multiple methods of interconnecting multiple VPNs with interconnect providers. As shown in Fig. 14, all the VPNs, having multiple service providers, can be interconnected using a single interconnect provider. Alternatively, all the VPNs can be interconnected by multiple interconnect providers, as shown in Fig. 15, thereby creating competition between the interconnect providers, just as there is competition between the CSPs in a single xNX-type VPN. Finally, as shown in

Petitioner Apple Inc. - Exhibit 1026, p. 633

Fig. 16, where no suitable interconnect provider is available to connect all he VPNs having multiple service providers, multiple interconnect providers are used. These interconnect providers service different combinations of VPNs. In Fig. 16, interconnect provider 120 interconnects VPNs having multiple service providers 122, 124, and 126. Interconnect provider 130 interconnects VPNs having multiple service providers 132 and 126. As a result, a TP of VPN 132 must connect through both Interconnect provider 130 and Interconnect provider 120 to reach TPs of either VPN 122 or 124.

How the multiple VPNs interconnect will directly affect the resulting end-to-end service quality. Figs. 17a-c illustrate potential configurations of multiple VPNs. In Fig. 17a a first TP 200 connects to a first CSP 210. The CSP210 connects to a first exchange point 220. The TP 200, CSP 210, and the exchange point 220 are within a first VPN 240. A second TP 250 connects to a second CSP 260, which connects to a second exchange point 270. The TP 250, CSP 260 and exchange point 270 are within a second VPN 280. The two VPNs 240 and 280 are interconnected by an Interconnect provider 300, which is connected to the exchange points 220 and 270.

In Fig. 17b TP 200, CSP 210, exchange point 220 and Interconnect provider 300 are connected in the same manner shown in Fig. 17a. While the second TP 250 is connected to the CSP 260, the exchange point 270 is not provided. Instead CSP 260 is shown as connecting directly to the Interconnect provider 300. This embodiment encompasses the situation where the Interconnect provider 300 and CSP 260 are the same entity or are directly wired. Fig. 17c is similar to Fig. 16b,
Except that the interconnect provider also acts as a CSP 320, and a third TP 310 is connected directly to the Interconnect provider 300/CSP 320.

As stated previously, while the end-to-end service quality is based upon the TEL-2 specification, the degree to which the TEL-2 specification needs to be modified to interconnect multiple VPNs depends upon the chosen complexity of the interconnection. An xNX-type VPN uses a maximum of two CSPs between any two TPS. A larger value, either three or four, is needed for multiple VPNs. The Interconnect provider will account for one additional CSP, and for configuration set forth in Fig. 16, two Interconnect providers are employed in addition to the two CSPs yielding four CSPs.

Petitioner Apple Inc. - Exhibit 1026, p. 634

Having described several embodiments of the system and method for interconnecting multiple virtual private networks in accordance with the present invention, it is believed that other modifications, variations and changes will be suggested to those skilled in the art in view of the description set forth above. It is therefore to be understood that all such variations, modifications and changes are believed to fall within the scope of the present invention as defined in the appended claims.

Petitioner Apple Inc. - Exhibit 1026, p. 635

What is claimed is:

1. A system of interconnecting multiple virtual private networks, each of said multiple private networks having multiple service providers, comprising:

at least one interconnect provider for connecting said multiple virtual private networks,

said multiple virtual private networks connected through said at least one interconnect provider having minimum standards for cross network services, virtual private network interoperability, inter–network performance, inter-network reliability, disaster recovery and business continuity, inter-network security, inter-network customer care, and inter-network trouble handling.

2. A system as recited in claim 1, further comprising a maximum acceptable latency between subscribers to different ones of said multiple virtual private networks.

3. A system as recited in claim 1, further comprising a maximum acceptable number of service providers between subscribers to different ones of said multiple virtual private networks.

4. A system as recited in claim 1, further comprising a minimum acceptable period of unavailability of interconnected multiple virtual private networks.

5. A system as recited in claim 1, wherein each of said multiple virtual private networks comprises a program overseer to ensure end-to-end service quality across each of said multiple virtual private networks.

6. A system as recited in claim 5, further comprising a global overseer to ensure end-to-end service quality across multiple ones of said multiple virtual private networks.

7. A system as recited in claim 6, wherein said global overseer resolves disputes between ones of said program overseers for said multiple virtual private networks or said program overseers and said at least one interconnect provider.

Petitioner Apple Inc. - Exhibit 1026, p. 636

8. A system as recited in claim 5, wherein said program overseer for each one of said multiple virtual private networks resolves disputes between service providers within said one of said multiple virtual private networks.

9. A system as recited in claim 6, wherein each of said program overseers and said multiple interconnect providers provides financial support to run said global overseer.

10. A system as recited in claim 1, wherein management of said multiple virtual private networks, contracts by between service providers and interconnect providers, service assurance, service description and how service providers and interconnect providers collaborate and compete are unified across said multiple virtual private networks to ensure end-to-end service quality.

11. A system as recited in claim 1, comprising multiple interconnect providers, wherein no one interconnect provider services all of said multiple virtual private networks.

12. A method of interconnecting multiple interconnection providers between multiple virtual private networks, each of said virtual private networks having multiple subscribers, multiple service providers and at least one exchange point interconnecting said multiple service providers, with guaranteed end-to-end service quality, comprising the steps of:

providing at least one interconnect provider disposed between a first set of said multiple service providers in one of said multiple virtual private networks and a second set of multiple service providers in a second one of said multiple virtual private networks.

13. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, wherein one of said at least one transit service providers is also one of said multiple service providers within at least one of said multiple virtual private networks.

Petitioner Apple Inc. - Exhibit 1026, p. 637

14. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, further comprising the step of certifying all of said multiple service providers in all of said multiple virtual private networks, said multiple transit service providers, and said exchange points to ensure minimum end-to-end quality and security levels are maintained.

15. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, comprising the further step of providing at least one exchange point between a first set of said multiple service providers in one of said multiple virtual private networks and said at least one interconnect service provider.

16. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, wherein a maximum number of service providers between two subscribers within one of said multiple virtual private networks is two, and the maximum number of said service providers and transit service providers between subscribers of different ones of said multiple virtual private networks is three.

17. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 15, further comprising the step of providing at least one second exchange point between a second set of said multiple service providers in another one of said multiple virtual private networks and said at least one transit service provider.

18. A system of interconnecting multiple virtual private networks, each of said multiple private networks having multiple service providers, comprising:

at least one interconnect provider for connecting said multiple virtual private networks,

each of said multiple virtual private networks comprising a program overseer to ensure end-to-end service quality across each of said multiple virtual private networks, and

Petitioner Apple Inc. - Exhibit 1026, p. 638

a global overseer to ensure end-to-end service quality across multiple ones of said multiple virtual private networks,

said multiple virtual private networks connected through said at least one interconnect provider have: minimum standards for cross network services; virtual private network interoperability; inter–network performance; inter-network reliability; disaster recovery and business continuity; inter-network security; inter-network customer care; and inter-network trouble handling.

19. A system as recited in claim 18, further comprising a maximum acceptable latency between subscribers to different ones of said multiple virtual private networks.

20. A system as recited in claim 18, further comprising a maximum acceptable number of service providers between subscribers to different ones of said multiple virtual private networks.

21. A system as recited in claim 18, further comprising a minimum acceptable period of unavailability of interconnected multiple virtual private networks.

22. A system as recited in claim 18, wherein said global overseer resolves disputes between ones of said program overseers for said multiple virtual private networks or said program overseers and said at least one interconnect provider.

23. A system as recited in claim 18, wherein said program overseer for each one of said multiple virtual private networks resolves disputes between service providers within said one of said multiple virtual private networks.

24. A system as recited in claim 18, wherein each of said program overseers and said multiple interconnect providers provides financial support to run said global overseer.

25. A system as recited in claim 18, wherein management of said multiple virtual private networks, contracts by between service providers and interconnect

Petitioner Apple Inc. - Exhibit 1026, p. 639

providers, service assurance, service description and how service providers and interconnect providers collaborate and compete are unified across said multiple virtual private networks to ensure end-to-end service quality.

26. A system as recited in claim 18, comprising multiple interconnect providers, wherein no one interconnect provider services all of said multiple virtual private networks.

Petitioner Apple Inc. - Exhibit 1026, p. 640

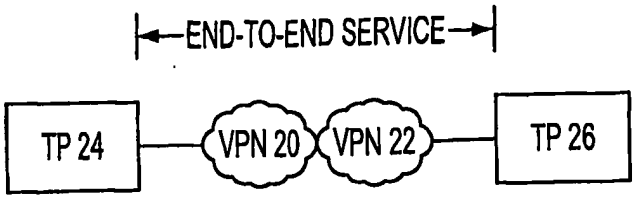


FIG. 1

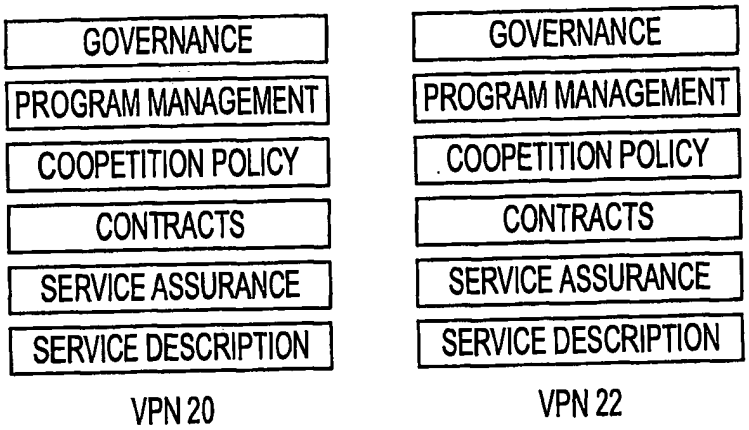


FIG. 2

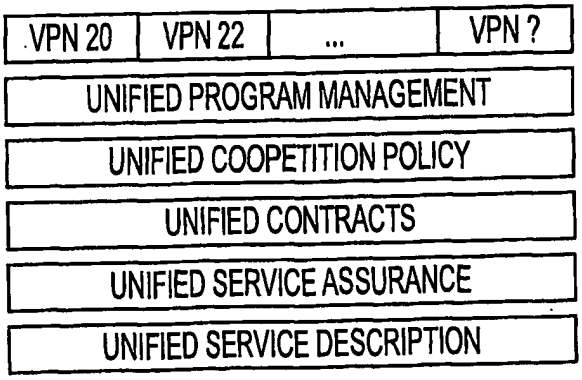


FIG. 3

Petitioner Apple Inc. - Exhibit 1026, p. 641

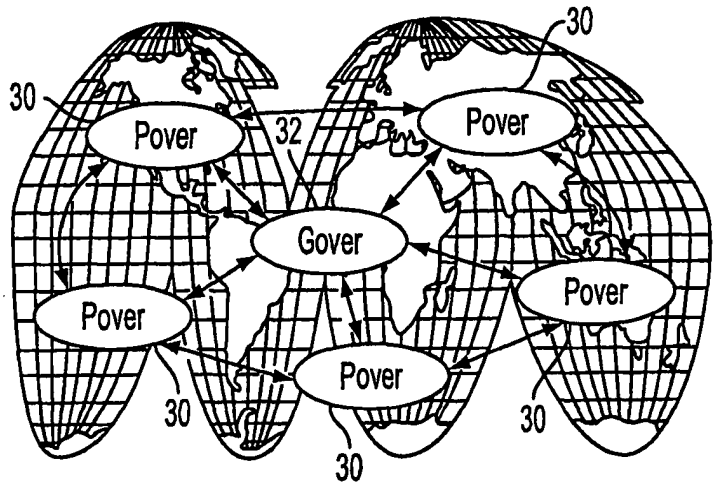


FIG. 4

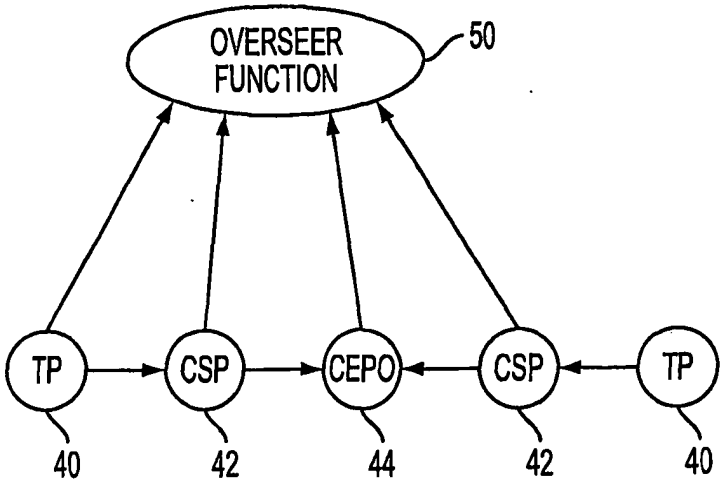


FIG. 5

Petitioner Apple Inc. - Exhibit 1026, p. 642

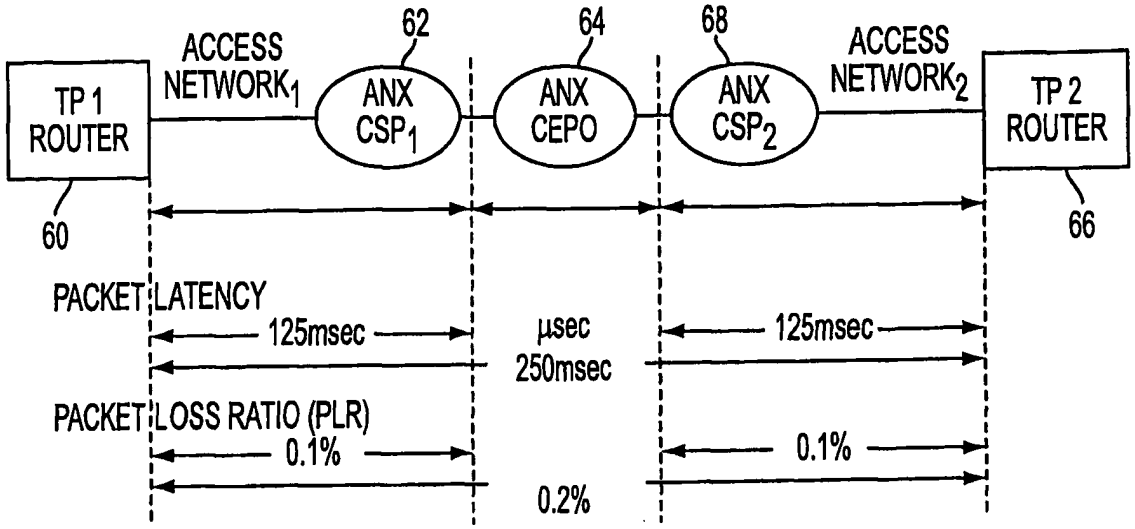


FIG. 6

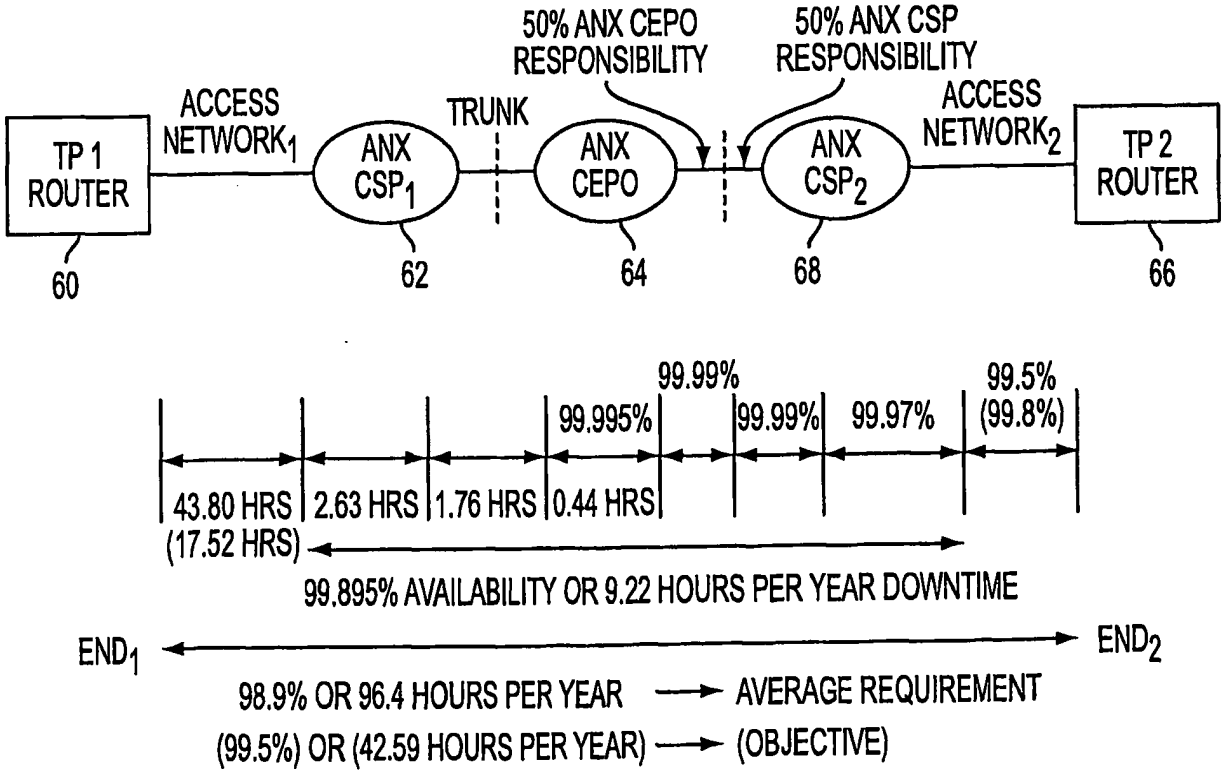


FIG. 7

Petitioner Apple Inc. - Exhibit 1026, p. 643

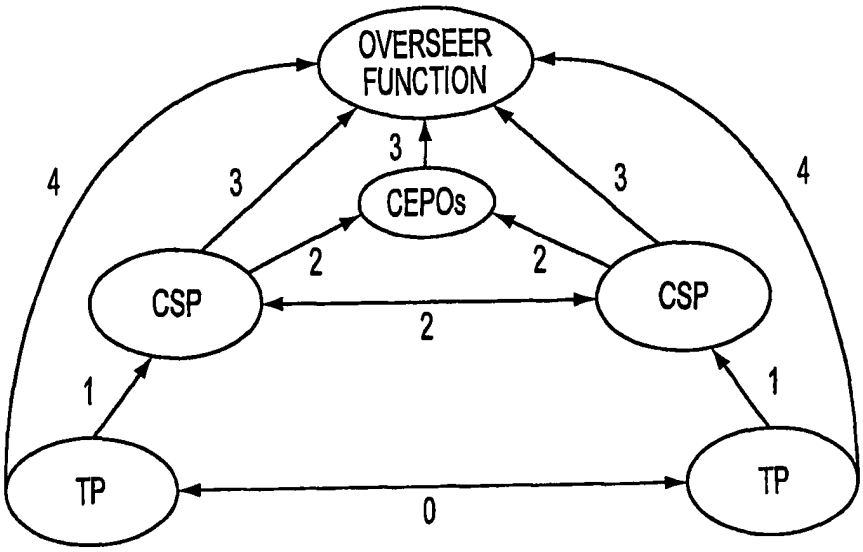

OVERSEER FUNCTION
CEPOs
CSP
CSP
TP
TP
4
3
3
4
3
2
2
2
1
1
0

FIG. 8

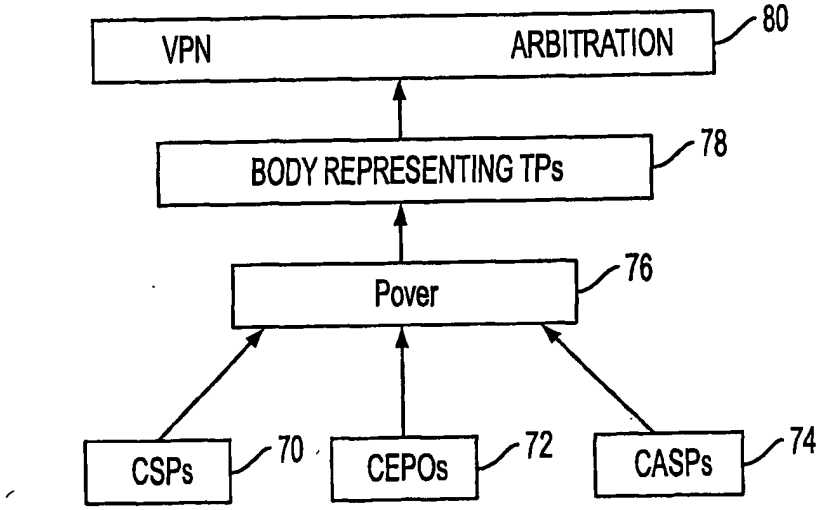

VPN
ARBITRATION
80
BODY REPRESENTING TPs
78
Pover
76
CSPs
70
CEPOs
72
CASPs
74

FIG. 9

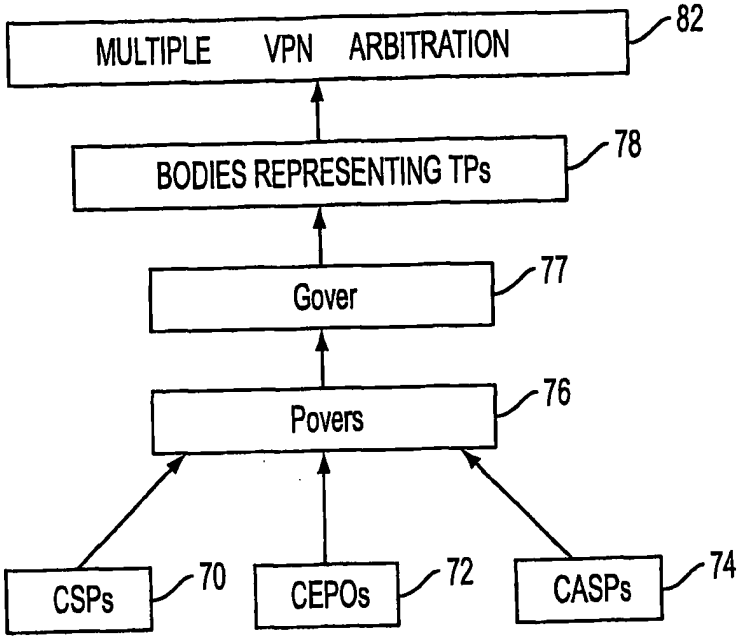


FIG. 10

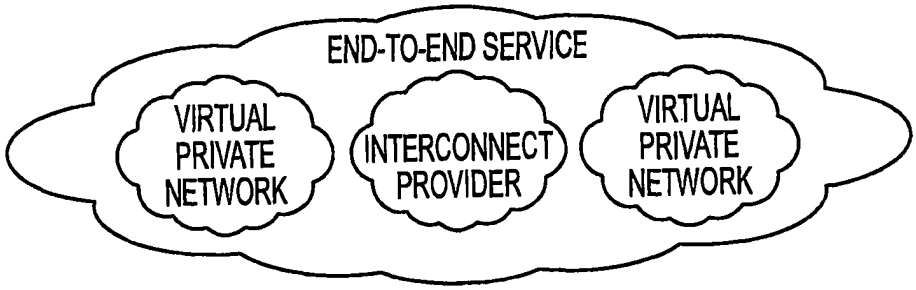


FIG. 11

Petitioner Apple Inc. - Exhibit 1026, p. 645

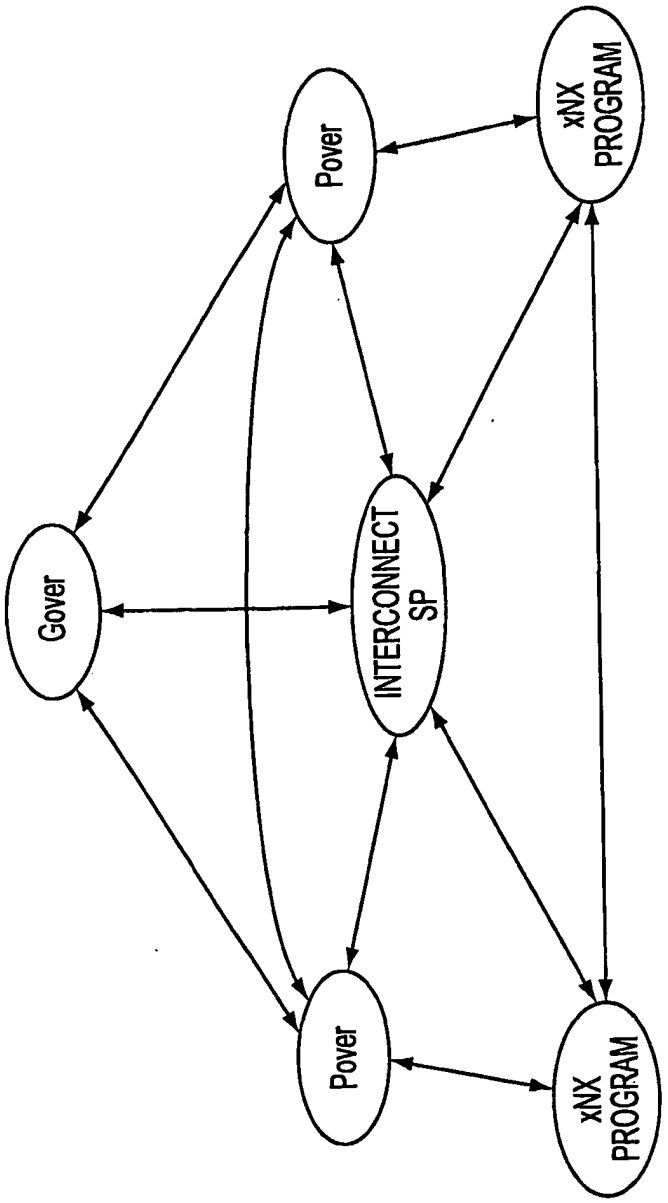


FIG. 12

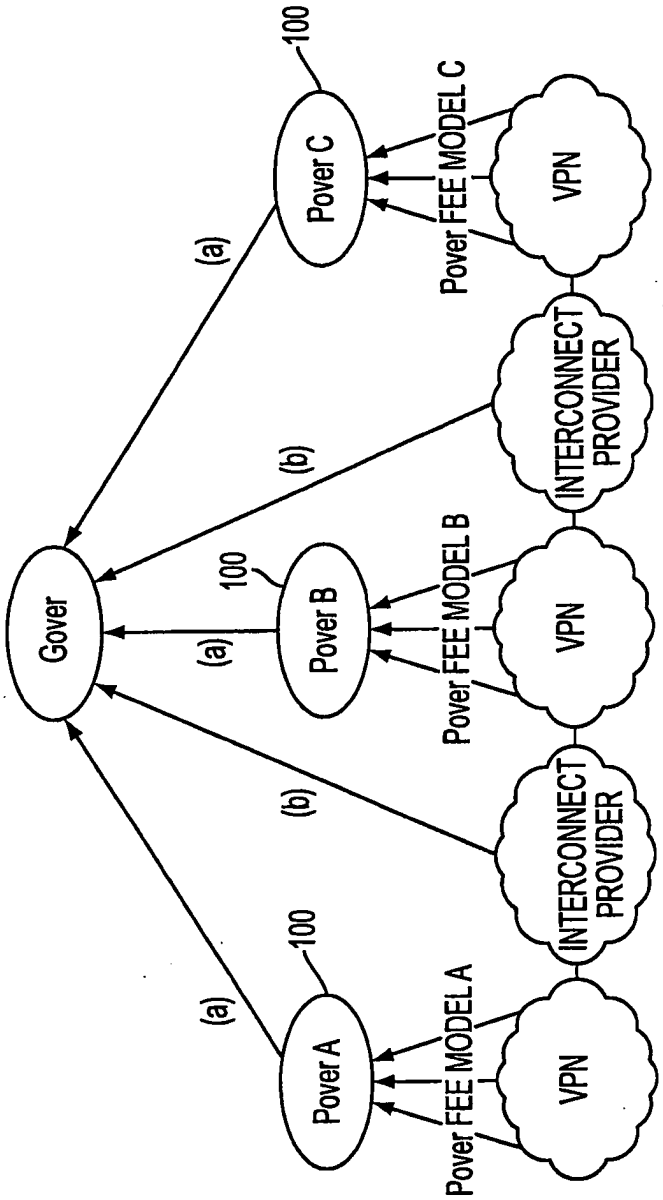

Gover
(a)
(b)
Pover A
Pover B
Pover C
100
Pover FEE MODEL A
Pover FEE MODEL B
Pover FEE MODEL C
VPN
INTERCONNECT PROVIDER

FIG. 13

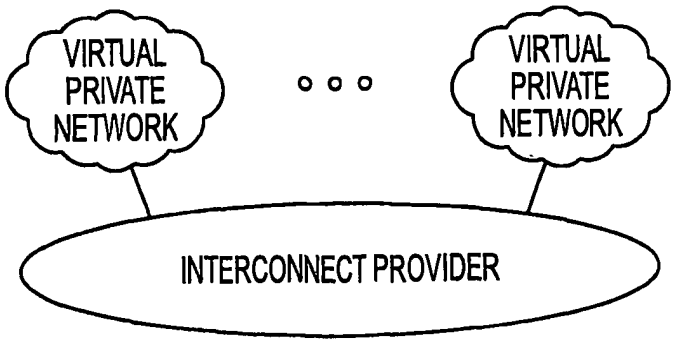

VIRTUAL PRIVATE NETWORK
VIRTUAL PRIVATE NETWORK
INTERCONNECT PROVIDER

FIG. 14

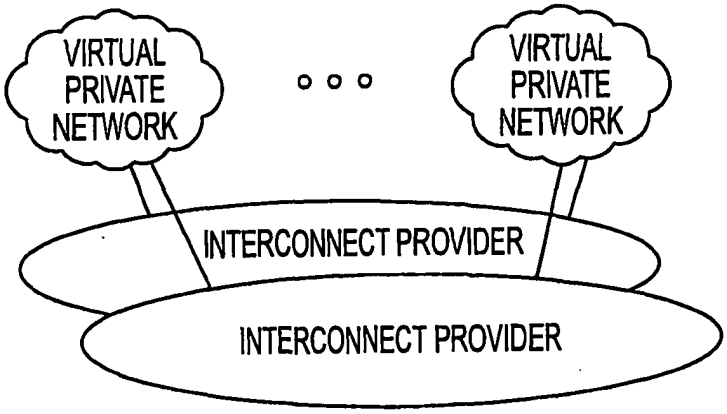

VIRTUAL PRIVATE NETWORK
VIRTUAL PRIVATE NETWORK
INTERCONNECT PROVIDER
INTERCONNECT PROVIDER

FIG. 15

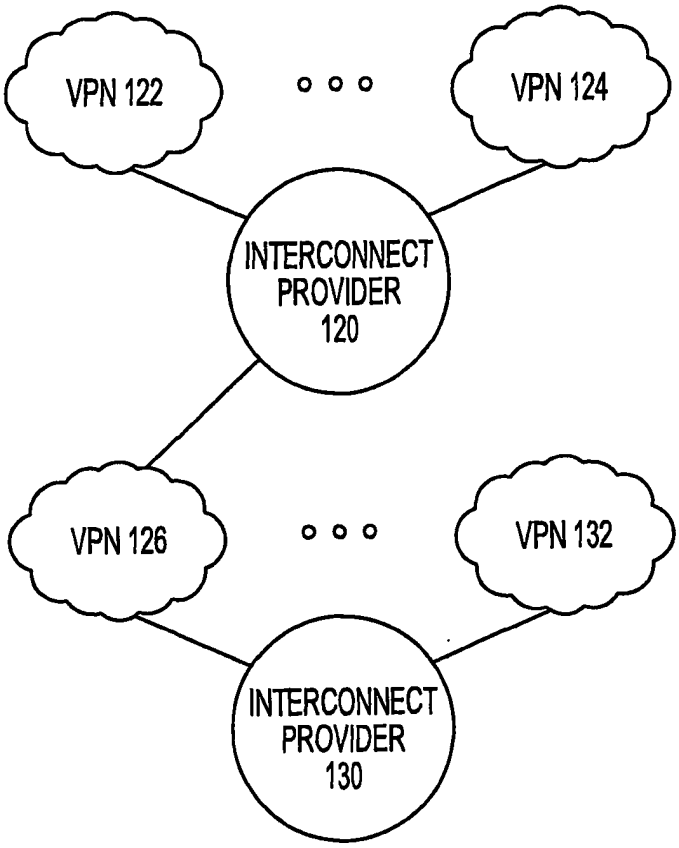


FIG. 16

Petitioner Apple Inc. - Exhibit 1026, p. 649

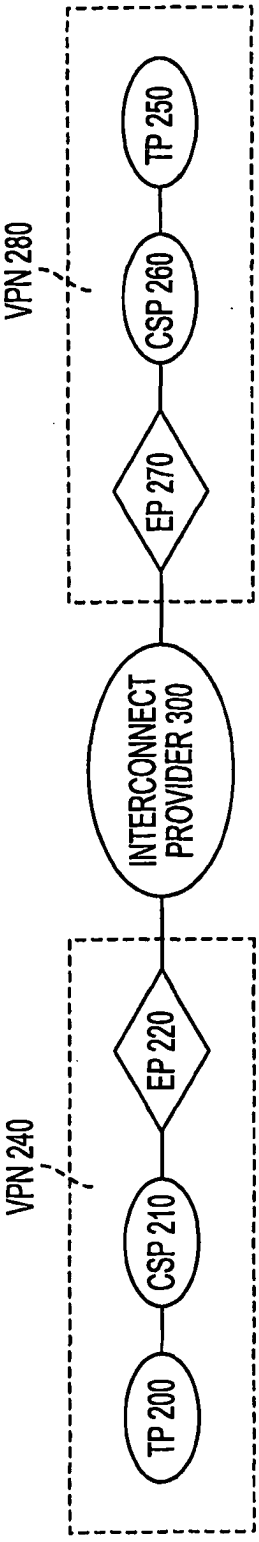


FIG. 17A

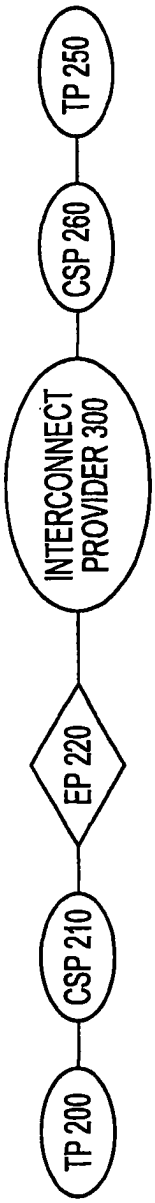


FIG. 17B

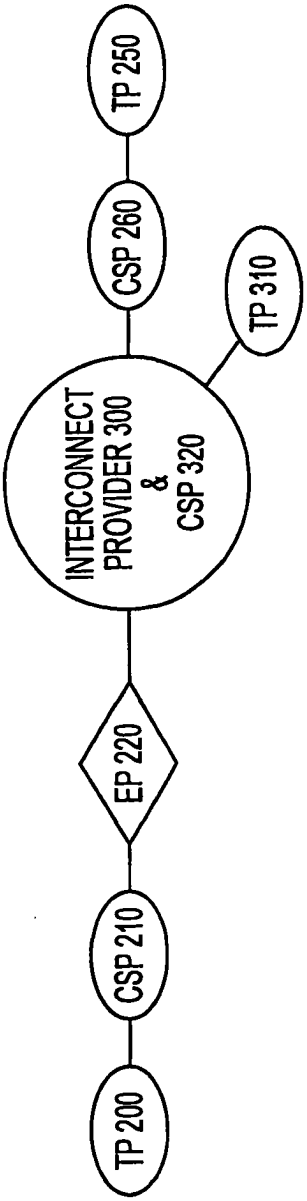


FIG. 17C

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/23774

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 13/00
US CL : 709/201, 220, 221, 223, 227, 228, 236, 238
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/201, 220, 221, 223, 227, 228, 236, 238

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CAS ONLINE
service(1w)providers, private(1w)(networks or lans), interconnection(1w)provider

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US 6,104,701 A (AVARGUES et al) 15 August 2000, Figs 1-3, col 1, lines 60-67, col 2, lines 1-6, lines 22-67, col 3, lines 1-6, col 6, lines 20-67, col 7, lines 1-26.	1-26

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 10 OCTOBER 2000	Date of mailing of the international search report 26 OCT 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Peggy Harod MOUSTAFA M. MEKY Telephone No. (703) 305-9697

Form PCT/ISA/210 (second sheet) (July 1998)★

MAY 04 2009
PATENT & TRADEMARK OFFICE

5-5-09 IDS

Docket No.: 077580-0015

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Victor Larson, et al.
Appl. No.:	11/679,416
Filed:	February 27, 2007
Title:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
Grp./A.U.	2157
Examiner:	Not yet assigned

Customer No.: 23630
Confirmation No.: 3528

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail under 37 CFR 1.8(a) in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on May 4, 2009

Jacqueline Andreu

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Enclosed for filing in connection with the above-referenced patent application are the following documents:

1) Information Disclosure Statement (2 pages)
2) Information Disclosure Statement by Applicant (Form 1449) (17 pages);
3) 6 Boxes of cited references B1000-B1002 and C998-C1226;
   - (Please note that references are arranged in order starting from Box 1)
4) Return receipt postcard.

There are no fees due with the filing of this Information Disclosure Statement. However, the Commissioner is hereby authorized to charge any additional fees that may be required, or credit any overpayment, to our Deposit Account No. 50-1133.

Respectfully submitted,

Date: May 4, 2009

Toby H. Kusmer, Reg. No.: 26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4065
Facsimile: (617) 535-3800

BST99 1618793-1.077580.0015

MAY 0 4 2009
PATENT & TRADEMARK OFFICE

Docket No.: 077580-0015 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Victor Larson, et al.
Appl. No.:	11/679,416
Filed:	February 27, 2007
Title:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
Grp./A.U.	2157
Examiner:	Not yet assigned

Customer No.: 23630
Confirmation No.: 3528

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail under 37 CFR 1.8(a) in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on May 4, 2009.

Jacqueline Andreu

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Dear Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached form PTO-1449. It is respectfully requested that the documents be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is being filed before the receipt of a First Office Action on the merits for above-referenced application; therefore, no fees are believed to be due with the filing of this paper.

All of the documents herein submitted have been produced by Microsoft Corp. in VirnetX Inc. and Science Applications International Corp. v. Microsoft Corp. civil action currently pending before the U.S. District Court for the Eastern District of Texas. Although the undersigned attorney has not reviewed these documents to assess their materiality, these documents are submitted under the assumption that they may be material to the patentability of the claims pending in this application. As indicated in form 1449 enclosed herewith, the hard copies of some of the documents listed have not been located and therefore are not included with

Petitioner Apple Inc. - Exhibit 1026, p. 653

this IDS submission. The undersigned attorney will file the missing documents with the U.S. Patent Office if or as soon as they become available. The Examiner is invited to call the undersigned attorney for any questions regarding the missing documents.

This Statement is not to be interpreted as a representation that the cited publications are material, or that no other relevant information exists. Nor shall the citation of any publication herein be construed *per se* as a representation that such publication is prior art. Moreover, the Applicant understands that the Examiner will make an independent evaluation of the cited publications.

If the Examiner applies any of the documents as prior art against any claim in the application and applicants determine that the cited document does not constitute "prior art" under United States law, applicant reserves the right to present to the office the relevant facts and law regarding the appropriate status of such documents. Applicants further reserve the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Toby H. Kusmer
Registration No. 26,418
28 State Street
Boston, MA 02109
Phone: 617-535-4065
Facsimile: 617-535-3800
Date: May 4, 2009

Please recognize our Customer No. 23630 as our correspondence address.

Petitioner Apple Inc. - Exhibit 1026, p. 654

PTO/SB/08a (04-09)
Approved for use through 05/31/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11679416
Filing Date	2007-02-27
First Named Inventor	Larson, et al.
Art Unit	2157
Examiner Name	
Attorney Docket Number	77580-015(VRNK-1CP2DVCN)

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6246670		2001-06-00	Karlsson, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	2157
	Examiner Name	
	Attorney Docket Number	77580-015(VRNK-1CP2DVCN)

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	2157
	Examiner Name	
	Attorney Docket Number	77580-015(VRNK-1CP2DVCN)

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/ARR/	Date (YYYY-MM-DD)	2009-05-29
Name/Print	Atabak R. Royaee	Registration Number	59037

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	5426736
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royaee/Erin Shea
Filer Authorized By:	Atabak R Royaee
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)
Receipt Date:	01-JUN-2009
Filing Date:	27-FEB-2007
Time Stamp:	11:01:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	VRNK_1CP2DVCN_US_IDS_Form__SB_08a.pdf	608426 fd09e0b59d903b297eae473732a7753c9eb4bdc7	no	4

Warnings:	
Information:	

Total Files Size (in bytes):	608426

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11679416	LARSON ET AL.
	Examiner	Art Unit
	Krisna Lim	2453

SEARCHED

Class	Subclass	Date	Examiner
709	225-229, 245	6/6/09	kl

SEARCH NOTES

Search Notes	Date	Examiner
Inventors, EAST	6/6/09	kl

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11679416	LARSON ET AL.
	Examiner	**Art Unit**
	Krisna Lim	2453

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/05/2009								
	1	✓								

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	49	((VICTOR) near2 (LARSON)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
L2	164	((ROBERT) near2 (SHORT)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
L3	27	((EDMUND) near2 (MUNGER)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
L4	72	((MICHAEL) near2 (WILLIAMSON)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
L5	242	l1 or l2 or l3 or l4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:07
L6	242	l5 and ad@ad<"02152000"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:07
L7	43745710	l5 adn ad@ad<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:07
L8	242	l5 and ad@<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:08
L9	242	l5 and ad@<="02152000"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:09
L10	49	l8 and (secure network address).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:09
L11	24	l8 and domain.ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:09
L12	15	l11 and (secure adj5 domain).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:10

Petitioner Apple Inc. - Exhibit 1026, p. 663

L13	3938	(secure same computer same network).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:11
L14	0	l13 and (secure same domanin same name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:11
L15	110	l13 and (secure same domain same name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:12
L16	70	l15 and (secure same domain same service)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:14
L17	70	l16 and ad@<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:14
L18	70	l17 and (query message secure domain name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:16

6/5/09 11:17:00 AM
C:\Program Files\USPTO\EAST\Bin\default.wsp

Petitioner Apple Inc. - Exhibit 1026, p. 664

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	3938	(secure same computer same network).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:30
L2	110	L1 and (secure same domain same name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:30
L3	70	L2 and (secure same domain same service)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:30
L4	70	L3 and ad@<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:30
L5	70	L4 and (query message secure domain name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:30
L6	27	(secure adj4 computer adj5 network adj5 address)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:39
L7	131	(secure adj4 domain adj5 name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:40
L8	131	l7 and ad@<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:40
L9	4	l7 and @ad<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 13:41
L10	16	(secure adj5 computer adj5 network adj5 address).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 14:08

Petitioner Apple Inc. - Exhibit 1026, p. 665

L11	670	(secure adj6 communication adj6 link).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 14:27
L12	11	l11 and (secure adj6 domain).ti, ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 14:30
S1	49	((VICTOR) near2 (LARSON)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
S2	164	((ROBERT) near2 (SHORT)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
S3	27	((EDMUND) near2 (MUNGER)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
S4	72	((MICHAEL) near2 (WILLIAMSON)).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2009/06/05 11:06
S5	242	S1 or S2 or S3 or S4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:07
S6	242	S5 and ad@ad<"02152000"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:07
S7	43745710	S5 adn ad@ad<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:07
S8	242	S5 and ad@<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:08
S9	242	S5 and ad@<="02152000"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:09
S10	49	S8 and (secure network address).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:09
S11	24	S8 and domain.ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:09

Petitioner Apple Inc. - Exhibit 1026, p. 666

S12	15	S11 and (secure adj5 domain).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:10
S13	3938	(secure same computer same network).ti,ab,clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:11
S14	0	S13 and (secure same domanin same name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:11
S15	110	S13 and (secure same domain same name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:12
S16	70	S15 and (secure same domain same service)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:14
S17	70	S16 and ad@<="19981030"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:14
S18	70	S17 and (query message secure domain name)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/05 11:16

6/ 5/ 09 2:37:10 PM
C:\ Documents and Settings\ klim\ My Documents\ EAST\ Workspaces\ 11679416.wsp

Petitioner Apple Inc. - Exhibit 1026, p. 667

PTO/SB/08a (01-09)
Approved for use through 05/31/2009. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11679416
Filing Date	2007-02-27
First Named Inventor	Larson, et al.
Art Unit	2157
Examiner Name	
Attorney Docket Number	77580-015(VRNK-1CP2DVCN)

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6246670		2001-06-00	Karlsson, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416 11679416 - GAU: 2453
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	2157
	Examiner Name	
	Attorney Docket Number	77580-015(VRNK-1CP2DVCN)

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	06/04/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

PTO/SB/08a (11-08)
Approved for use through 12/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11679416
Filing Date	2007-02-27
First Named Inventor	Larson, et al.
Art Unit	
Examiner Name	
Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5384848		1995-01-00	Kikuchi	
	2	6223287		2001-04-00	Douglas, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416 11679416 - GAU: 2453
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	06/04/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416 11679416 - GAU: 2453
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/THK/	Date (YYYY-MM-DD)	2008-12-16
Name/Print	Toby H. Kusmer	Registration Number	26,418

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

PTO/SB/08a (11-08)
Approved for use through 12/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11679416
Filing Date	2007-02-27
First Named Inventor	Larson, et al.
Art Unit	
Examiner Name	
Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5303302		1994-04-12	Burrows	
	2	5629984		1997-05-13	McManis	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416 11679416 - GAU: 2453
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	06/04/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

PTO/SB/08a (11-08)
Approved for use through 12/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11679416
Filing Date	2007-02-27
First Named Inventor	Larson, et al.
Art Unit	
Examiner Name	
Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5771239		1998-06-23	Moroney, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11679416 11679416 - GAU: 2453
	Filing Date	2007-02-27
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-015(VRNK-1CP2DVCN)

	1	FASBENDER, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Krisna Lim/	Date Considered	06/04/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/679,416	02/27/2007	Victor Larson	77580-015 (VRNK-1CP2DVCN)	3528

23630 7590 06/08/2009

MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775

EXAMINER	
LIM, KRISNA	

ART UNIT	PAPER NUMBER
2453	

MAIL DATE	DELIVERY MODE
06/08/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/679,416	LARSON ET AL.	
	Examiner	Art Unit	
	Krisna Lim	2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

1. Claim 1 is presented for examination.

2. The disclosure is objected to because of the following informalities:

(a) On page 1, the text of the first paragraph should be updated with the current status of the cited applications such as U.S. Patent Application Serial No., a filing date, U.S. Patent No., and the issued date. Appropriate correction is required.

3. The information disclosure statement filed 5/04/09 (there is at least **102 pages** of just a list of the references), 11/13/07 and 12/16/08 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information. It has been placed in the application file, but the information referred to therein has not been considered.

4. The information disclosure statement filed 05/04/09 (there is at least 102 pages of just a list of the references) fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

5. Claim 1 is rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

At line 3, it is unclear from where a query message is sent. At line 4, it is unclear from where the query message is requesting a secure computer network address. At line 5, it is unclear where the response message is received and from where the response message is received. At line 7, it is unclear from where an access request is sent.

6. .A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

7. Claim 1 provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claim 1 of copending Application No. 11/839,987. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

8. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140

F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

9. Claim 1 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 7,188,180. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a method of accessing a secure computer network address, comprising steps of: a) receiving a secure domain ...; b) sending a query message to a secure domain …; c) receiving from the secure domain name center ...; and d) sending an access request message to the secure computer network address using a virtual private network communication link. The different is the clarity language of the claim of the parent while the language of the claim of the present application does not.

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The references are cited in the Form PTO-892 for the applicant's review.

A shortened statutory period for response to this action is set to expire 3 (three) months and 0 (zero) days from the mail date of this letter. Failure to respond within the period for response will result in **ABANDONMENT** of the application (see 35 U.S.C 133, M.P.E.P 710.02, 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Krisna Lim whose telephone number is 571-272-3956 The examiner can normally be reached on Monday to Friday from 9:30 AM to 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne, can be reached on 571-272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kl

June 06, 2009

/Krisna Lim/

Primary Examiner, Art Unit 2453

OIPE
SEP 08 2009
PATENT & TRADEMARK OFFICE

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1	of	2

Complete if Known	
Application Number	**11/679,416**
Filing Date	**February 27, 2007**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Lim, Krisna**
Docket Number	**77580-015 (VRNK-1CP2DVCN)**

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes3-Number 4-Kind Codes *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)	
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1)	
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)	
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/soc kswp.html (1997). (Socks, Aventail)	
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)	
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3)	
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4)	
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5)	
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6)	
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7)	
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8)	
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Petitioner Apple Inc. - Exhibit 1026, p. 684

Subst. for form 1449/PTO	Complete if Known	
SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/679,416**
	Filing Date	**February 27, 2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
Sheet 2 of 2	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10)	
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11)	
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail)	
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail)	
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail)	
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW)	
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12)	
	C1081	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	C1090	Assured Digital Products. (Assured Digital)	
	C1146	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3)	
	C1155	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)	
	C1163	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4)	
	C1164	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview)	
	C1168	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager)	
	C1201	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

BST99 1628591-1.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 685

OIPE
SEP 0 8 2009
PATENT & TRADEMARK OFFICE

09-09-09

Docket No.: 077580-0015

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Victor Larson, et al.

Customer No.: 23630

Appl. No.: 11/679,416

Confirmation No.: 3528

Filed: February 27, 2007

Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Grp./A.U. 2453

Examiner: LIM, Krisna

CERTIFICATE OF MAILING (37 CFR § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail No. EV643770342 under 37 CFR 1.8(a) in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on September 8, 2009.

Jacqueline Andreu

Jacqueline Andreu

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Enclosed for filing in connection with the above-referenced patent application are the following documents:

1) Supplemental Information Disclosure Statement (2 pages)
2) Supplemental Information Disclosure Statement by Applicant (Form 1449) (2 pages);
3) Copies of twenty-seven (27) references listed in form 1449; and
4) Return receipt postcard.

The commissioner is hereby authorized to charge $180.00, and any additional fees that may be required, or credit any overpayment, to our Deposit Account No. 50-1133.

Respectfully submitted,

Date: September 8, 2009

Atabak R. Royaee, Reg. No.: 59,037
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4108
Facsimile: (617) 535-3800

BST99 1628592-1.077580.0015

OIPE
SEP 08 2009
PATENT & TRADEMARK OFFICE

Docket No.: 077580-0015 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Victor Larson, et al.	Customer No.:	23630
Appl. No.:	11/679,416	Confirmation No.:	3528
Filed:	February 27, 2007		
Title:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK		
Grp./A.U.	2453		
Examiner:	LIM, Krisna		

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail No. EV643770342 under 37 CFR 1.8(a) in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on September 8, 2009.

Jacqueline Andreu

Jacqueline Andreu

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Dear Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached form PTO-1449. It is respectfully requested that the documents be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is being filed before the receipt of a Final Office Action on the merits for above-referenced application; therefore, a fee in the amount of $180.00 is believed to be due with the filing of this paper.

09/10/2009 CCHAU1 00000002 501133 11679416
01 FC:1806 180.00 DA

Petitioner Apple Inc. - Exhibit 1026, p. 687

The twenty-seven (27) documents submitted herein are those previously listed in the IDS filed on 05/4/09, but whose copies were not available at the time. This Statement is not to be interpreted as a representation that the cited publications are material, or that no other relevant information exists. Nor shall the citation of any publication herein be construed *per se* as a representation that such publication is prior art. Moreover, the Applicant understands that the Examiner will make an independent evaluation of the cited publications.

If the Examiner applies any of the documents as prior art against any claim in the application and applicants determine that the cited document does not constitute "prior art" under United States law, applicant reserves the right to present to the office the relevant facts and law regarding the appropriate status of such documents. Applicants further reserve the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Atabak R. Royaee
Registration No. 59,037
28 State Street
Boston, MA 02109
Phone: 617-535-4108
Facsimile: 617-535-3800
Date: September 8, 2009

Please recognize our Customer No. 23630 as our correspondence address.

Petitioner Apple Inc. - Exhibit 1026, p. 688

OIPE IAP99
OCT 06 2009
PATENT & TRADEMARK OFFICE

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	**11/679,416**
Filing Date	**February 27, 2007**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Lim, Krisna**
Docket Number	**77580-015 (VRNK-1CP2DVCN)**

Sheet 1 of 1

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes3-Number 4-Kind Codes (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1177	WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000)	
	C1178	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999)	
	C1179	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000)	
	C1180	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000)	
	C1181	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000) **(resubmitted)**	
	C1182	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes* (July 21, 2000)	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

BST99 1630399-1.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 689

OIPE
OCT 06 2009
PATENT & TRADEMARK OFFICE

10-07-09

(FW)

Docket No.: 077580-0015 (VRNK-1CP2DVCN) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Victor Larson, et al.

Customer No.: 23630

Appl. No.: 11/679,416

Confirmation No.: 3528

Filed: February 27, 2007

Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Grp./A.U. 2453

Examiner: LIM, Krisna

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail No. EV643770435 under 37 CFR 1.8(a) in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on October 6, 2009.

Jacqueline Andreu

Jacqueline Andreu

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Enclosed for filing in connection with the above-referenced patent application are the following documents:

1) Supplemental Information Disclosure Statement (2 pages)
2) Supplemental Information Disclosure Statement by Applicant (Form 1449) (1 page);
3) Copies of six (6) references listed in form 1449 (C1177 to C1182); and
4) Return receipt postcard.

The commissioner is hereby authorized to charge $180.00, and any additional fees that may be required, or credit any overpayment, to our Deposit Account No. 50-1133.

Respectfully submitted,

Date: October 6, 2009

Atabak R. Royaee, Reg. No.: 59,037
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4108
Facsimile: (617) 535-3800

BST99 1628592-1.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 690

Docket No.: 077580-0015 (VRNK-1CP2DVCN)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Victor Larson, et al.	Customer No.:	23630
Appl. No.:	11/679,416	Confirmation No.:	3528
Filed:	February 27, 2007		
Title:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK		
Grp./A.U.	2453		
Examiner:	LIM, Krisna		

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail No. EV643770435 under 37 CFR 1.8(a) in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on October 6, 2009.

Jacqueline Andreu

Jacqueline Andreu

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Dear Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached form PTO-1449. It is respectfully requested that the documents be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is being filed before the receipt of a Final Office Action on the merits for above-referenced application; therefore, a fee in the amount of $180.00 is believed to be due with the filing of this paper.

10/07/2009 RMEBRAH1 00000107 501133 11679416

01 FC:1806 180.00 DA

Petitioner Apple Inc. - Exhibit 1026, p. 691

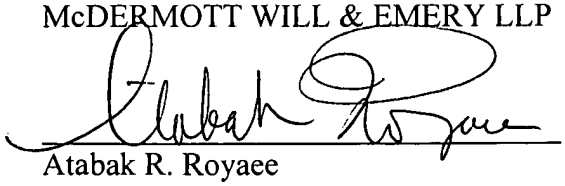
References Nos. C1177-C1180 and C1182 submitted herewith are those previously listed in the IDS filed on 5/4/09 but whose copies were not available at that time. Also, reference C1181 is being resubmitted because it has been supplemented with additional pages.. This Statement is not to be interpreted as a representation that the cited publications are material, or that no other relevant information exists. Nor shall the citation of any publication herein be construed *per se* as a representation that such publication is prior art. Moreover, the Applicant understands that the Examiner will make an independent evaluation of the cited publications.

If the Examiner applies any of the documents as prior art against any claim in the application and applicants determine that the cited document does not constitute "prior art" under United States law, applicant reserves the right to present to the office the relevant facts and law regarding the appropriate status of such documents. Applicants further reserve the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Atabak R. Royaee
Registration No. 59,037
28 State Street
Boston, MA 02109
Phone: 617-535-4108
Facsimile: 617-535-3800
Date: October 6, 2009

Please recognize our Customer No. 23630 as our correspondence address.

Petitioner Apple Inc. - Exhibit 1026, p. 692

OIPE IAP9 NOV 06 2009 PATENT & TRADEMARK OFFICE

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**11/679,416**
Filing Date	**February 27, 2007**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**LIM, Krisna**
Docket Number	**077580-0015 (VRNK-1CP2DVCN)**

Sheet 1 of 2

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1227	Microsoft Corporation's Fifth Amended Invalidity Contentions dated September 18, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation and invalidity claim charts for U.S. Patent Nos. 7,188,180 and 6,839,759	
	C1228	The IPSEC Protocol as described in Atkinson, et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401"); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1229	S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1230	C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1231	C. Madson and R. Glenn, "The Use HMAC-SHA-1-96 within ESP and AH," RFC 2404 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2453**
				Examiner Name	**LIM, Krisna**
Sheet	2	of	2	Docket Number	**077580-0015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
	C1232	C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1233	S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1234	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1235	Douglas Maughan, et al, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1236	D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1237	R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1238	R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1239	Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (November 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (July 1996) ("Galvin")	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

BST99 1632946-1.077580.0015

11-9-07

OIPE
IAP9
NOV 0 6 2009
PATENT & TRADEMARK OFFICE

Docket No.: 077580-0015 (VRNK-1CP2DVCN) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Victor Larson, et al.	Customer No.:	23630
Appl. No.:	11/679,416	Confirmation No.:	3528
Filed:	February 27, 2007		
Title:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK		
Grp./A.U.	2453		
Examiner:	LIM, Krisna		

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail No. EV643770532US under 37 CFR 1.8(a) in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on October 6, 2009.

Jacqueline Andreu

Jacqueline Andreu

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Enclosed for filing in connection with the above-referenced patent application are the following documents:

1) Supplemental Information Disclosure Statement (2 pages)
2) Supplemental Information Disclosure Statement by Applicant (Form 1449) (2 pages);
3) Copies of references listed in form 1449 (C1227 to C1239); and
4) Return receipt postcard.

The commissioner is hereby authorized to charge $180.00, and any additional fees that may be required, or credit any overpayment, to our Deposit Account No. 50-1133.

Respectfully submitted,

Date: November 6, 2009

Atabak R. Royaee, Reg. No.: 59,037
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4108
Facsimile: (617) 535-3800

BST99 1628592-1.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 695

NOV 06 2009
PATENT & TRADEMARK OFFICE

Docket No.: 077580-0015 (VRNK-1CP2DVCN) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Victor Larson, et al.	Customer No.:	23,630
Appl. No.:	11/679,416	Confirmation No.:	9623
Filed:	February 27, 2007		
Title:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK		
Grp./A.U.	2453		
Examiner:	LIM, Krisna		

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail No. EV643770532US under 37 CFR 1.8(a) in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on November 6, 2009.

Jacqueline Andreu

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Dear Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached form PTO-1449. It is respectfully requested that the documents be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is being filed before the receipt of a Final Office Action on the merits for above-referenced application; therefore, a fee in the amount of $180.00 is believed to be due with the filing of this paper.

11/10/2009 HALI33 00000016 501133 11679416
01 FC:1806 180.00 DA

Petitioner Apple Inc. - Exhibit 1026, p. 696

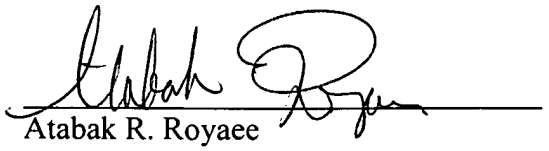
References Nos. C1227-C1239 submitted herewith are those produced by Microsoft Corp. in VirnetX Inc. and Science Applications International Corp. v. Microsoft Corp. civil action currently pending before the U.S. District Court for the Eastern District of Texas. Although the undersigned agent has not reviewed these documents to assess their materiality, these documents are submitted under the assumption that they may be material to the patentability of the claims pending in this application. This Statement is not to be interpreted as a representation that the cited publications are material, or that no other relevant information exists. Nor shall the citation of any publication herein be construed *per se* as a representation that such publication is prior art. Moreover, the Applicant understands that the Examiner will make an independent evaluation of the cited publications.

If the Examiner applies any of the documents as prior art against any claim in the application and applicants determine that the cited document does not constitute "prior art" under United States law, applicant reserves the right to present to the office the relevant facts and law regarding the appropriate status of such documents. Applicant further reserves the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

The Examiner is invited to call the undersigned agent for any questions regarding the IDS. The Commissioner is hereby authorized to charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Atabak R. Royaee
Registration No. 59,037
28 State Street
Boston, MA 02109
Phone: 617-535-4108
Facsimile: 617-535-3800
Date: November 6, 2009

Please recognize our Customer No. 23630 as our correspondence address.

Petitioner Apple Inc. - Exhibit 1026, p. 697

Docket No.: 077580-0015 (1CP2DVCN)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Victor Larson, et al.	Customer No.:	23,630
Appl. No.:	11/679,416	Confirmation No.:	3528
Filed:	February 27, 2007		
Title:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK		
Grp./A.U.	2453		
Examiner:	LIM, Krisna		

CERTIFICATE OF MAILING (37 CFR § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail No. EV643770532US under 37 CFR 1.8(a) in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on November 6, 2009.

Jacqueline Andrew

Jacqueline Andrew

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Dear Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached form PTO-1449. It is respectfully requested that the documents be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is being filed before the receipt of a Final Office Action on the merits for above-referenced application; therefore, a fee in the amount of $180.00 is believed to be due with the filing of this paper.

11/10/2009 HALI33 00000003 501133 11924460
01 FC:1806 180.00 DA

Copied from 11924460 on 01/10/2010
Petitioner Apple Inc. - Exhibit 1026, p. 698

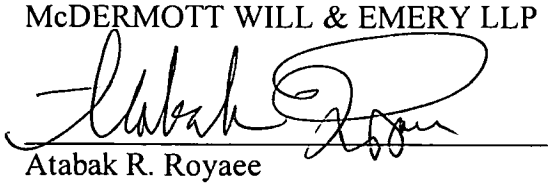
References Nos. C1227-C1239 submitted herewith are those produced by Microsoft Corp. in VirnetX Inc. and Science Applications International Corp. v. Microsoft Corp. civil action currently pending before the U.S. District Court for the Eastern District of Texas. Although the undersigned agent has not reviewed these documents to assess their materiality, these documents are submitted under the assumption that they may be material to the patentability of the claims pending in this application. This Statement is not to be interpreted as a representation that the cited publications are material, or that no other relevant information exists. Nor shall the citation of any publication herein be construed *per se* as a representation that such publication is prior art. Moreover, the Applicant understands that the Examiner will make an independent evaluation of the cited publications.

If the Examiner applies any of the documents as prior art against any claim in the application and applicants determine that the cited document does not constitute "prior art" under United States law, applicant reserves the right to present to the office the relevant facts and law regarding the appropriate status of such documents. Applicant further reserves the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

The Examiner is invited to call the undersigned agent for any questions regarding the IDS. The Commissioner is hereby authorized to charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Atabak R. Royaee
Registration No. 59,037
28 State Street
Boston, MA 02109
Phone: 617-535-4108
Facsimile: 617-535-3800
Date: November 6, 2009

Please recognize our Customer No. 23630 as our correspondence address.

Copied from 11924460 on 01/10/2010
Petitioner Apple Inc. - Exhibit 1026, p. 699

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Larson et al.
Application Serial No.:	11/679,416
Filing Date:	February 27, 2007
Title:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
Examiner:	Lim, Krisna
Art Unit:	2453
Confirmation No.:	3528
Atty. Docket No.:	077580-0015 (VRNK-1CP2DVCN)

I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office via ESF-WEB on December 8, 2009.

/Kelly Ciarmataro/
Kelly Ciarmataro

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT "A"

In response to the non-final Office Action mailed June 8, 2009 ("the Office Action"), for the above-identified application, please enter the following amendments and remarks.

Amendments to the Specification, beginning on page 2 of this paper;

Amendments to the Claims, beginning on page 3 of this paper, and

Remarks, beginning on page 8 of this paper.

Petitioner Apple Inc. - Exhibit 1026, p. 700

1. Amendments to the Specification

Please amend the **Description** of the specification to read:

Please amend paragraph [0001] as follows:

[0001] This application claims priority from and is a divisional patent application of co-pending U.S. application Ser. No. 09/558,209, filed Apr. 26, 2000 and now abandoned, which is in turn a continuation-in-part patent application of previously-filed U.S. application Ser. No. 09/504,783, filed on Feb. 15, 2000[[,]] and now U.S. Pat. No. 6,502,135, issued Dec. 31, 2002, which in turn claims priority from and is a continuation-in-part patent application of previously-filed U.S. application Ser. No. 09/429,643, filed on Oct. 29, 1999, now U.S. Pat. No. 7,010,604, issued Mar. 7, 2006. The subject matter of U.S. application Ser. No. 09/429,643, which is bodily incorporated herein, derives from provisional U.S. application Nos. 60/106,261 (filed Oct. 30, 1998) and 60/137,704 (filed Jun. 7, 1999). The present application is also related to U.S. application Ser. No. 09/558,210, filed Apr. 26, 2000 and now abandoned, ~~and~~ which is incorporated by reference herein.

Petitioner Apple Inc. - Exhibit 1026, p. 701

Amendments to the Claims

The listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Cancelled)

2. (New) A method of communicating with a device having a secure name, the method comprising:

sending a message to a name service, the message requesting an address associated with the secure name of the device;

receiving a message containing the address associated with the secure name of the device; and

sending a message to the address associated with the secure name of the device using a secure communication link.

3. (New) The method according to claim 2, further including supporting a plurality of services through the secure communication link.

4. (New) The method according to claim 2, wherein the secure name indicates security.

5. (New) The method according to claim 2, wherein receiving the message containing the address associated with the secure name of the device includes receiving the message in encrypted form.

6. (New) The method according to claim 5, further including decrypting the message.

7. (New) The method according to claim 2, wherein the device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link when needed..

Petitioner Apple Inc. - Exhibit 1026, p. 702

8. (New) The method according to claim 2, wherein receiving a message containing the address associated with the secure name of the device includes receiving the address as an IP address associated with the secure name of the device.

9. (New) The method according to claim 2, further including automatically initiating the secure communication link after it is enabled.

10. (New) The method according to claim 2, wherein receiving a message containing the address associated with the secure name of the device includes receiving the message through tunneling within the secure communication link.

11. (New) The method according to claim 2, wherein receiving a message containing the address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet.

12. (New) The method according to claim 2, wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols.

13. (New) The method according to claim 2, wherein the receiving an sending of messages through the secure communication link includes multiple sessions.

14. (New) The method according to claim 2, further including supporting a plurality of services over the secure communication link.

15. (New) The method according to claim 14, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

16. (New) The method according to claim15, wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof.

17. (New) The method according to claim 15, wherein the plurality of services comprises audio, video or a combination thereof.

Petitioner Apple Inc. - Exhibit 1026, p. 703

18. (New) The method according to claim 2, wherein the secure communication link is an authenticated link.

19. (New) The method according to claim 2, wherein the device is a computer, and the steps are performed on the computer.

20. (New) The method according to claim 2, wherein the device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network.

21. (New) The method according to claim 2, further including providing an unsecure name associated with the device.

22. (New) The method according to claim 2, wherein the secure name is registered prior to the step of sending a message to a name service.

23. (New) The method according to claim 2,

wherein sending a message to a name service comprises sending a first message from a first device to the name service, the first message requesting from the name service the address associated with the secure name of the device,

wherein receiving a message comprises receiving at the first device a second message from the name service, the second message containing the address associated with the secure name of the device, and

wherein sending a message to the address comprises sending a third message from the first device to the address associated with the secure name of the device using the secure communication link.

24. (New) A method for communicating with a device in a communication network, the device having a secure name, the method comprising:

requesting registration of a secure name of a first device, the secure name associated with an address;

receiving at the address associated with the secure name of the first device a message from a second device to communicate with the first device; and

sending a message securely from the first device to the second device.

Petitioner Apple Inc. - Exhibit 1026, p. 704

25. (New) The method according to claim 24, wherein requesting registration of a secure name of a first device comprises requesting from the first device registration of the secure name of the first device, and

wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link.

26. (New) A method for communicating with a device in a communication network, the device associated with a secure name and an unsecured name, the method comprising:

requesting registration of an unsecured name associated with a first device;

requesting registration of a secure name associated with the first device, wherein an address corresponds to the secure name associated with the first device;

receiving at the address associated with the secure name a message from a second device to communicate with the first device; and

sending a message securely from the first device to the second device.

27. (New) The method according to claim 26,

wherein requesting registration of an unsecured name associated with a first device comprises requesting from the first device registration of the unsecured name associated with the first device, and

wherein requesting registration of a secure name associated with the first device comprises requesting from the first device registration of the secure name associated with the first device.

28. (New) A machine-readable medium comprising instructions for:

sending a message to a name service, the message requesting an address associated with a secure name of a device;

receiving a message containing the address associated with the secure name of the device; and

sending a message to the address associated with the secure name of the device using a secure communication link.

29. (New) A machine-readable medium comprising instructions for a method for communicating with a device having a secure name, the method comprising:

Petitioner Apple Inc. - Exhibit 1026, p. 705

receiving at an address associated with a secure name of a first device a message from a second device to communicate with the first device, wherein the secure name of the first device is registered; and

sending a message securely from the first device to the second device.

30. (New) A machine-readable medium comprising instructions for a method for communicating with a device associated with a secure name and an unsecured name, the method comprising:

receiving, at an address corresponding to a secure name associated with a first device, a message from a second device to communicate with the first device, wherein an unsecured name is associated with the first device, and the secure name and the unsecured name are registered; and

sending a message securely from the first device to the second device.

Petitioner Apple Inc. - Exhibit 1026, p. 706

Remarks

Claims 2-30 remain in the application. Applicant appreciates the Examiner's examination of the subject application. In the specification, the CROSS-REFERENCE TO RELATED APPLICATIONS is amended to update the current status of the cited applications. In the claims, claim 1 has been cancelled and claims 2-30 have been added.

Applicant respectfully traverses the rejection of claim 1, and requests consideration of the subject application in light of the foregoing amendments and the following remarks.

Information Disclosure Statements and 37 C.F.R. § 1.98(a)(3)

In the Office Action, the Examiner states that the Applicant's May 4, 2009, November 13, 2007, and December 16, 2008 Information Disclosure Statements fail to comply with 37 C.F.R. § 1.98(a)(3), which states:

> Any information disclosure statement filed under § 1.97 shall include . . . (i) A concise explanation of the relevance, as it is presently understood by the individual designated in § 1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language. The concise explanation may be either separate from applicant's specification or incorporated therein. (ii) A copy of the translation if a written English-language translation of a non-English-language document, or portion thereof, is within the possession, custody, or control of, or is readily available to any individual designated in § 1.56(c).

The Applicant respectfully submits that, to the best of the Applicant's knowledge, these Information Disclosure Statements list references written in the English language which are outside the purview of § 1.98(a)(3). Accordingly, because the references are in the English language, the Applicant respectfully requests consideration of these references in the Examiner's review of the subject application.

Information Disclosure Statements and 37 C.F.R. § 1.98(a)(2)

In the Office Action, the Examiner states that the Applicant's May 4, 2009 Information Disclosure Statement fails to comply with 37 C.F.R. § 1.98(a)(2), which states:

> Any information disclosure statement filed under § 1.97 shall include . . . A legible copy of: (i) Each foreign patent; (ii) Each publication or that portion which caused it to be listed, other than U.S. patents and U.S. patent application publications unless required by the Office; (iii) For each cited pending

Petitioner Apple Inc. - Exhibit 1026, p. 707

> unpublished U.S. application, the application specification including the claims, and any drawing of the application, or that portion of the application which caused it to be listed including any claims directed to that portion; and (iv) All other information or that portion which caused it to be listed.

As stated in the May 4, 2009 Information Disclosure Statement and those filed thereafter, the references cited therein were produced by the Defendant Microsoft Corp. in the VirnetX, Inc. and Science Applications Int'l Corp. v. Microsoft Corp. litigation in the Eastern District of Texas. While copies of various of the listed references were unavailable at the time the Information Disclosure Statement was filed, the Applicant has since submitted copies of those unavailable references in accordance with 37 C.F.R. § 198(a)(2) in Information Disclosure Statements filed on September 8, 2009 and October 6, 2009. Accordingly, the provisions of 37 C.F.R. § 1.98(a)(2) are satisfied for all references listed in the May 4, 2009 Information Disclosure Statement. The Applicant thus respectfully requests consideration of these references in the Examiner's review of the subject application.

Rejection of Claim 1 under 35 U.S.C. §112. Second Paragraph

In the Office Action, the Examiner rejected Claim 1 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicant regards as the invention. Because Claim 1 has been cancelled, the Applicant respectfully submits that this rejection is moot and requests consideration of pending claims 2-30.

Statutory Type Double Patenting Rejection

The Examiner rejected claim 1 under 35 U.S.C. § 101 as claiming the same invention as that of claim 1 of copending Application No. 11/839,987. Because claim 1 has been cancelled, the Applicant respectfully submits that this rejection is rendered moot.

Non-statutory Double Patenting Rejection

The Examiner rejected claim 1 on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 7,188,180. Because claim 1 has been cancelled, the Applicant respectfully submits that this rejection is rendered moot.

Petitioner Apple Inc. - Exhibit 1026, p. 708

CONCLUSION

In light of the Amendments and Remarks herein, the Applicant submits that the claims are in condition for allowance and respectfully requests a notice to this effect. Should the Examiner have any questions, please call the undersigned at the phone number listed below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 501133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: 8 December 2009

/Toby H. Kusmer/

Toby Kusmer, Reg. No.: 26,418
McDERMOTT WILL & EMERY LLP
28 State Street
Boston, Massachusetts 02109
Telephone: (617) 535-4065
Facsimile: (617) 535-3800

BST99 1638055-1.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 709

Electronic Patent Application Fee Transmittal

Application Number:	11679416
Filing Date:	27-Feb-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	1202	9	52	468
Independent claims in excess of 3	1201	3	220	660
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 3 months with $0 paid	1253	1	1110	1110
Miscellaneous:				
			Total in USD ($)	**2238**

Electronic Acknowledgement Receipt

EFS ID:	6596629
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)
Receipt Date:	08-DEC-2009
Filing Date:	27-FEB-2007
Time Stamp:	17:11:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2238
RAM confirmation Number	3991
Deposit Account	501133
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	Amendment_A.pdf	406211 c5febe259ab08473edd584e30bdd7b45b15c9d02	no	10

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

2	Fee Worksheet (PTO-875)	fee-info.pdf	34257 1695d943ef3e389ea253c4b14287016b40806760	no	2

Warnings:

Information:

Total Files Size (in bytes):	440468

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/679,416	02/27/2007	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	12/08/2009	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 29	Minus	** 30	= 0	X $ =		OR	X $52=	0
	Independent (37 CFR 1.16(h))	* 6	Minus	***3	= 3	X $ =		OR	X $220=	660
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	660

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/Wanda Meredith/

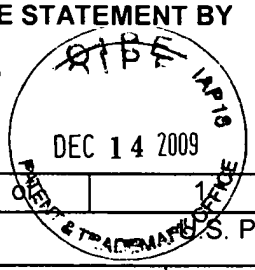
This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)



Complete if Known	
Application Number	11/679,416
Filing Date	February 27, 2007
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	LIM, Krisna
Sheet 1 of 1	
Docket Number	077580-0015 (VRNK-1CP2DVCN)

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1019	US	7,461,334	12/02/08	Lu, et al.	
	A1020	US	7,353,841	04/08/08	Kono, et al.	
	A1021	US	7,188,175	03/06/07	McKeeth, James A.	
	A1022	US	7,167,904	01/23/07	Devarajan, et al.	
	A1023	US	7,039,713	05/02/06	Van Gunter, et al.	
	A1024	US	6,757,740	06/29/04	Parekh, et al.	
	A1025	US	6,752,166	06/22/04	Lull, et al.	
	A1026	US	6,687,746	02/03/04	Shuster, et al.	
	A1027	US	6,338,082	01/08/02	Schneider, Eric	
	A1028	US	6,333,272	12/25/01	McMillin, et al.	
	A1029	US	6,314,463	11/06/01	Abbott, et al.	
	A1030	US	6,298,341	10/02/01	Mann, et al.	
	A1031	US	6,262,987	07/17/01	Mogul, Jeffrey C.	
	A1032	US	6,199,112	03/06/04	Wilson, Stephen K.	
	A1033	US	2,895,502	07/21/59	Garland Roper Charles, et al.	
	A1034	US	2001/0049741	12/06/01	Skene, et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1240	David Kosiur, "Building and Managing Virtual Private Networks" (1998)	
	C1241	P. Mockapetris, "Domain Names – Implementation and Specification," Network Working Group, RFC 1035 (November 1987)	
	C1242	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.	
	C1243	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

12-15-09

Docket No.: 077580-0015 (VRNK-1CP2DVCN) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

USPTO JAP18 DEC 14 2009 PATENT & TRADEMARK OFFICE

Applicant: Victor Larson, et al.

Appl. No.: 11/679,416

Filed: February 27, 2007

Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

Grp./A.U. 2453

Examiner: LIM, Krisna

Customer No.: 23630

Confirmation No.: 3528

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail No. EV643770515US under 37 CFR 1.8(a) in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on December 14, 2009.

Jacqueline Andrew

Jacqueline Andrew

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Enclosed for filing in connection with the above-referenced patent application are the following documents:

1) Supplemental Information Disclosure Statement (2 pages)
2) Supplemental Information Disclosure Statement by Applicant (Form 1449) (1 page);
3) Copies of references listed in form 1449 (C1240 to C1243); and
4) Return receipt postcard.

The commissioner is hereby authorized to charge $180.00, and any additional fees that may be required, or credit any overpayment, to our Deposit Account No. 50-1133.

Respectfully submitted,

Date: December 14, 2009

Atabak R. Royaee, Reg. No.: 59,037
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4108
Facsimile: (617) 535-3800

BST99 1628592-1.077580.0015

OIPE IAP19
DEC 14 2009
PATENT & TRADEMARK OFFICE

Docket No.: 077580-0015 (VRNK-1CP2DVCN) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Victor Larson, et al.	Customer No.:	23,630
Appl. No.:	11/679,416	Confirmation No.:	9623
Filed:	February 27, 2007		
Title:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF A VIRTUAL PRIVATE NETWORK		
Grp./A.U.	2453		
Examiner:	LIM, Krisna		

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail No. EV643770515US under 37 CFR 1.8(a) in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on December 14, 2009.

Jacqueline Andrieu

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Dear Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached form PTO-1449. It is respectfully requested that the documents be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is being filed before the receipt of a Final Office Action on the merits for above-referenced application; therefore, a fee in the amount of $180.00 is believed to be due with the filing of this paper.

12/15/2009 SDENBOB3 00000027 501133 11679416
01 FC:1806 180.00 DA

References Nos. C1240-C1243 submitted herewith were cited in the Request for *Inter Partes* Reexamination of Patent filed for U.S. Patent Nos. 6,502,135 and 7,188,180. Although the undersigned agent has not reviewed these documents to assess their materiality, these documents are submitted under the assumption that they may be material to the patentability of the claims pending in this application. This Statement is not to be interpreted as a representation that the cited publications are material, or that no other relevant information exists. Nor shall the citation of any publication herein be construed per se as a representation that such publication is prior art. Moreover, the Applicant understands that the Examiner will make an independent evaluation of the cited publications.

If the Examiner applies any of the documents as prior art against any claim in the application and applicants determine that the cited document does not constitute "prior art" under United States law, applicant reserves the right to present to the office the relevant facts and law regarding the appropriate status of such documents. Applicant further reserves the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

The Examiner is invited to call the undersigned agent for any questions regarding the IDS. The Commissioner is hereby authorized to charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Atabak R. Royaee
Registration No. 59,037
28 State Street
Boston, MA 02109
Phone: 617-535-4108
Facsimile: 617-535-3800
Date: December 14, 2009

Please recognize our Customer No. 23630 as our correspondence address.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	11/679,416
	Filing Date	02-27-2007
	First Named Inventor	Victor Larson
	Art Unit	2453
	Examiner Name	Krisna Lim
	Docket Number	077580-0015

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed before the receipt of a first office action.

[ ] Items contained in this Information Disclosure Statement were first cited in any communication from a foreign patent office in a counterpart foreign application.

[ ] No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned, after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of this Information Disclosure Statement

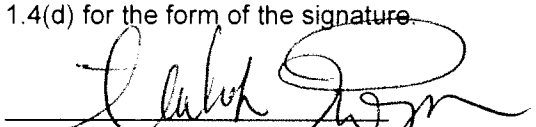
[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[X] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.



Date: April 2, 2010

Atabak R. Royaee, Reg. No.: 59,037
McDermott Will & Emery LLP
28 State Street
Boston, MA 02108
Tel. (617) 535-4000
Fax (617) 535-3800

BST99 1646790-1.077580.0015

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	11/679,416
Filing Date	02-27-2007
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	077580-0015

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	5,764,906	06/1998	Edelstein et al.	
	A2	5,864,666	01/1999	Shrader, Theodore Jack London	
	A3	5,898,830	04/1999	Wesinger et al.	
	A4	6,052,788	04/2000	Wesinger et al.	
	A5	6,061,346	05/2000	Nordman, Mikael	
	A6	6,081,900	06/2000	Subramaniam et al.	
	A7	6,101,182	08/2000	Sistanizadeh et al.	
	A8	6,199,112	03/2001	Wilson, Stephen K.	
	A9	6,202,081	03/2001	Naudus, Stanley **T**.	
	A10	6,298,341	10/2001	Mann et al.	
	A11	6,262,987	07/2001	Mogul, Jeffrey C.	
	A12	6,314,463	11/2001	Abbott et al.	
	A13	6,338,082	01/2002	Schneider, Eric	
	A14	6,502,135	12/2002	Munger et al.	
	A15	6,557,037	04/2003	Provino, Joseph E.	
	A16	6,687,746	02/2004	Shuster et al.	
	A17	6,757,740	06/2004	Parkh et al.	
	A18	7,039,713	05/2006	Van Gunter et al.	
	A19	7,167,904	01/2007	Devarajan et al.	
	A20	7,188,175	03/2007	McKeeth, James A.	
	A21	7,461,334	12/2008	Lu et al.	
	A22	7,490,151	02/2009	Munger et al.	
	A23	7,493,403	02/2009	Shull et al.	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B1	US2001/0049741	12/2001	Skene et al.	
	B2	US2004/0199493	10/2004	Ruiz et al.	
	B3	US2004/0199520	10/2004	Ruiz et al.	
	B4	US2004/0199608	10/2004	Rechterman et al.	
	B5	US2004/0199620	10/2004	Ruiz et al.	
	B6	US2007/0208869	09/2007	Adelman et al.	
	B7	US2007/0214284	09/2007	King et al.	
	B8	US2007/0266141	11/2007	Norton, Michael Anthony	

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	11/679,416
Filing Date	02-27-2007
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	077580-0015

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B9	US2008/0235507	09/2008	Ishikawa et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code[3]-Number[4]-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C1	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp		English Abstract	
	C2	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp		English Abstract	
	C3	JP10-070531	03/10/1998	Brother Ind Ltd.		English Abstract	
	C4	JP62-214744	9/21/1987	Hitachi Ltd.		English Abstract	

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1	Yuan Dong Feng, "A novel scheme combining interleaving technique with cipher in Rayleigh fading channels," Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998)	
	D2	D.W. Davies and W.L. Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **62-214744**

(43)Date of publication of application : **21.09.1987**

(51)Int.Cl. **H04L 9/00**
H04L 11/20
H04L 11/26

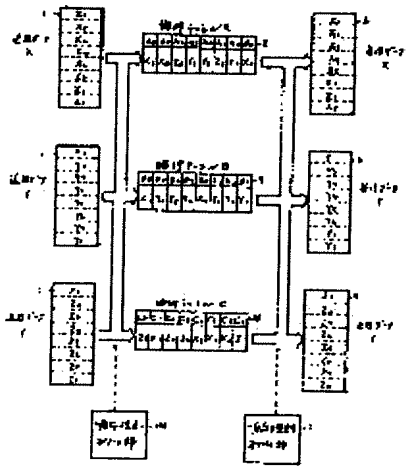
(21)Application number : **61-056812**

(22)Date of filing : **17.03.1986**

(71)Applicant : **HITACHI LTD**

(72)Inventor : **OOYA KAZUAKI**
HIRAGA KATSUHISA

(54) PACKET TRANSMISSION SYSTEM



(57)Abstract:

PURPOSE: To prevent the leakage of data by providing a means controlling the order of packet by a prescribed definition to the reception and transmission side, deciding the logical channel of each packet in the order of sending at the transmission side and restoring the data string of the packet received from each logical channel at the reception side.

CONSTITUTION: Data X, Y, Z to be sent of data 1, 4, 7 are split at each packet, a transmisson order rule control section 10 is used to share the packets into logical channels A, B, C of data 2, 5, 8. In this case, the sent order is changed according to the sequence restriction of the control section 10. Thus, the packet data are sent in the entirely difference order from that of the packet data constituting the original data 1, 4, 7 to be sent. At the reception side, the packet data received from each logical channel (2, 5, 8) is rearranged by a reception side order rule control section 11 to obtain reception data X, Y, Z of data 3, 6, 7. Thus, the leakage of the data from the transmission line and the decoding are prevented.

Cited Document 1 (JP-A (Kokai) S62-214744)

The order of packet data in each logical channel of the present invention is different from those in logical channels 2, 5, and 8 of the conventional packet transmission system as shown in Fig. 5 in that correct information cannot be obtained at the receiver even if the data in one logical channel are aligned sequentially, as indicated by 2, 5, and 8 in Fig. 1. Therefore, at the receiver, it is necessary to realign the data received from each logical channel with reference to the same order rule as that used at the transmitter.

Fig. 2 shows an example of the order rule. When arranged in a table indicated by 12, this order rule forms a matrix in which 24 types of numerals from A1 to C8, configured by the combination of the logical channel numbers of A, B, and C, and the sequence numbers from 1 to 8, correspond to the packet data from X1 to Z8 obtained by dividing the corresponding transmission data X, Y, and Z.

Fig. 3 shows an example of processing at the transmitter. When the data to be transmitted via the logical channel A of 2 are selected from the transmission data X, Y, and Z of 1, 4, and 7, the order rule shown in the table 12 in Fig. 3 is used to send out the packets in the order of X_1, Y_2, Z_2, Y_6, Y_7, and Z_6 to the logical channel A. The same applies to the data to be transmitted via the logical channels B and C of 5 and 8.

Fig. 4 shows an example of processing at the receiver. For example, the data X_1, Y_2, Z_2, Y_6, Y_7, and Z_6 received from the logical channel A indicated by 2 are aligned in each position of the received data X, Y, and Z indicated by 3, 6, and 9 according to the order rule of the logical channel A as shown in table 12 of Fig. 3. The same processing is executed for the other logical channels to restore the received data X, Y, and Z.

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭62－214744

⑤1Int.Cl.⁴	識別記号	庁内整理番号	④3公開　昭和62年(1987)9月21日
H 04 L 9/00		B－7240－5K	
11/20	102	A－7117－5K	
11/26		7117－5K	審査請求　未請求　発明の数 1　（全4頁）

⑤4発明の名称　パケット伝送方式

⑳特　願　昭61－56812
㉒出　願　昭61(1986)3月17日

⑦2発明者　大家　万明　秦野市堀山下1番地　株式会社日立製作所神奈川工場内
⑦2発明者　平賀　勝久　秦野市堀山下1番地　株式会社日立製作所神奈川工場内
⑦1出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
⑦4代理人　弁理士　小川　勝男　外1名

明　細　書

1．発明の名称

パケット伝送方式

2．特許請求の範囲

(1) 送信側と受信側において複数の論理チャネルを使用しデータをパケット分割して伝送するパケット伝送方式において、送信側と受信側にパケットの送信及び受信の順序を予め定めた定義に従って制御する順序規則制御手段を持ち、この順序規則制御手段により、送信側では受信する各パケットの論理チャネル及び送出順序を決定し、受信側では各論理チャネルから受信したパケットのデータ列の復元を行うことを特徴としたパケット伝送方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明はパケット伝送方式に係り、特に伝送内容の秘密を守るため、伝送路上でデータが第3者に漏れ、これが容易に解析されることを防ぐのに好適なパケット伝送方式に関する。

〔従来の技術〕

パケット伝送方式の一つに、送信側と受信側において複数の論理チャネルを使用し、データをパケット分割して伝送する方式がある（ＣＣＩＴＴ，Ｘ．２５勧告）。

第５図に従来のこの種パケット伝送方式を示す。１，４，７は送信しようとするデータＸ，Ｙ，Ｚであり、これをそれぞれパケット分割し、２，５，８の論理チャネルＡ，Ｂ，Ｃを経由して各々のパケットデータを受信側へ送信する。受信側では、各論理チャネルごとに受信したパケットデータをシーケンス番号順に整列させ、３，６，９の受信データＸ，Ｙ，Ｚを得る。

なお、秘密データ伝送に関連する公知文献としては、例えば特開昭６０－５４５４４号公報が挙げられる。

〔発明が解決しようとする問題点〕

従来技術においては、受信側において論理チャネル番号とパケットシーケンス番号により、パケットデータの識別を行うため、データを受信した

Petitioner Apple Inc. - Exhibit 1026, p. 724

側では容易にパケットの解読ができ、データが第3者へ漏洩するという問題があった。

本発明の目的は、伝送しようとするデータの形式を加工することなく、データを構成するパケットをそれぞれ異った仮想的通信路を通して伝送することにより、伝送しようとするデータが伝送路上から漏れ容易に解読されることを防ぐためのパケット伝送方式を提供することにある。

〔問題点を解決するための手段〕

本発明は、伝送しようとするデータを、同一の論理チャネルを通さずに、データを構成する複数のパケットをあらかじめ定めた規則により、いくつかの異った論理チャネルを使用して分割伝送する。あらかじめ定めた規則とは伝送しようとする一定順序のパケットをどの順序でどの仮想的通信路に送出するかを決めた通信路ごとの順序規則を言う。パケットを送信する側では、伝送しようとするデータを構成する一連のパケットを上記規則に従って仮想的通信路に順次送出する。パケットを受信する側では、同様に上記規則に従い、各仮想的通信路より受信したパケットを整列させ元のデータ列を復元する。

〔作　用〕

本発明は、データの漏洩を防止することを目的とし、伝送しようとするパケット列の順序及び伝送路に関してスクランブリングしようとするものである。従来のパケット伝送では、各パケットごとに持つ論理チャネル番号及びシーケンス番号を用いて、送信側と受信側のデータ側の順序制御を行っているため、受信側では受信したパケットデータ列から得られる情報のみで容易に元のデータ列を復元させることが容易である。

本発明においては、送信側と受信側にあらかじめ定義した論理チャネルとシーケンス番号から成る送信及び受信パケットの順序を変換するための順序規則を持ち、この順序情報と各パケットに持つ論理チャネル番号とパケットシーケンス番号を用いて、元のデータ列を復元させる。従って順序規則を持たないものが受信しても解読はできない。

〔実施例〕

以下、本発明の一実施例について図面により説明する。

第1図に本発明のパケット伝送方式を示す。1，4，7の送信しようとするデータX，Y，Zをそれぞれパケット分割し、10の送信側順序規則制御部を用いて、それぞれのパケットを2，5，8の各論理チャネルA，B，Cに振り分ける。この際、送出する順序も制御部10の順序規則に従って変化させる。従って、各論理チャネル2，5，8上には、図示の如く、送出しようとする元のデータ1，4，7を構成するパケットデータとはまったく異った順序で、パケットデータが伝送されることになる。受信側では、2，5，8の各論理チャネルより受信したパケットデータを、11の受信側順序規則制御部により整列し直し、3，6，7の受信データX，Y，Zを得る。

本発明における各論理チャネル上のパケットデータの順序は、第5図に示す従来のパケット伝送方式の論理チャネル2，5，8と異なり、第1図の2，5，8に示す様に1つの論理チャネル内のデータを順に整列させても受信側では正しい情報を得ることができない。従って、受信側では、送信側と同じ順序規則を参照して、各論理チャネルから受信したデータを再度整列させる必要がある。

第2図に順序規則の1例を示す。この順序規則例は、12に示すテーブル形式とした場合、A，B，Cの論理チャネル番号と1から8のシーケンス番号との組み合せによって構成されるA1からC8までの24種類の番号と、これに対応する送信データX，Y，Zを分割したX1からZ8のパケットデータを対応させたマトリックスとなる。

第3図に送信側の処理例を示す。1，4，7の送信データX，Y，Zより、2の論理チャネルA経由で送信するデータを選択する場合、第3図のテーブル12に示した順序規則を用いて、論理チャネルAに対して、X_1，Y_2，Z_3，Y_4，Y_5，Z_6の順序でパケットを送出する。5と8の論理チャネルB、C経由で送信するデータも同様である。

第4図に受信側の処理例を示す。例えば、2に

Petitioner Apple Inc. - Exhibit 1026, p. 725

示す論理チャネルAより受信したデータ、X_1, Y_2, Z_3, Y_6, Y_7, Z_8は、第3図のテーブル12で示した論理チャネルAの順序規則に従い、3，6，9に示される受信データX，Y，Zのそれぞれの位置に整列される。他の論理チャネルについても同様の処理を行い、受信データX，Y，Zを復元させる。

なお、順序規則は、テーブル形式で定義する方式のほかに、計算式で定義する方式が考えられる。

〔発明の効果〕

本発明によれば、あらかじめ定められた順序規則を知っている場合のみ、パケットデータの正しい送受信が行える。従って、順序規則を知らされていない第三者は正しい受信を行うことが出来ず、データの機密を守る上で効果がある。また、本発明においては、複数の論理チャネルを使用するため、各論理チャネルを物理的に別々の回線に分割して配置することが出来、この時には物理的に別々の回線を同時に接続して受信する必要があるため、データの漏洩防止にさらに効果がある。

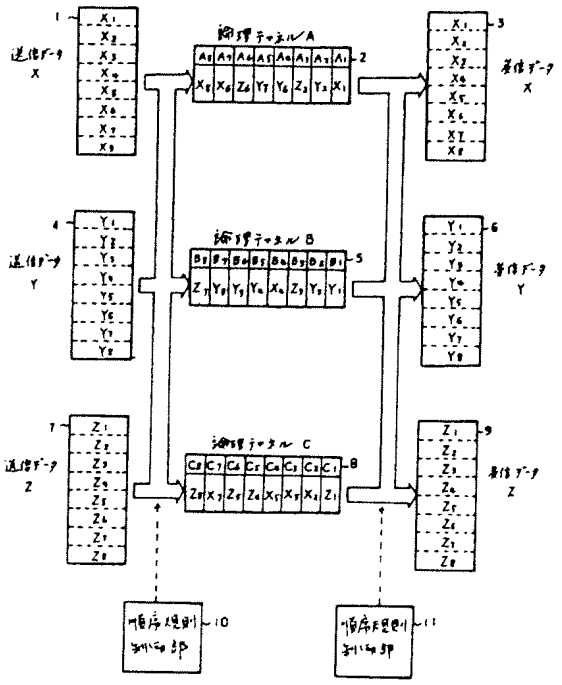
4．図面の簡単な説明

第1図は本発明のパケット伝送方式を説明する図、第2図は本発明で用いる順序規則の一例を示す図、第3図は本発明による送信側の処理例を示す図、第4図は本発明による受信側の処理例を示す図、第5図は従来のパケット伝送方式を説明する図である。

1，4，7…送信データ、
3，6，9…受信データ、
2，5，8…論理チャネル、
10…送信側順序規則制御部、
11…受信側順序規則制御部。

代理人弁理士　小川勝男

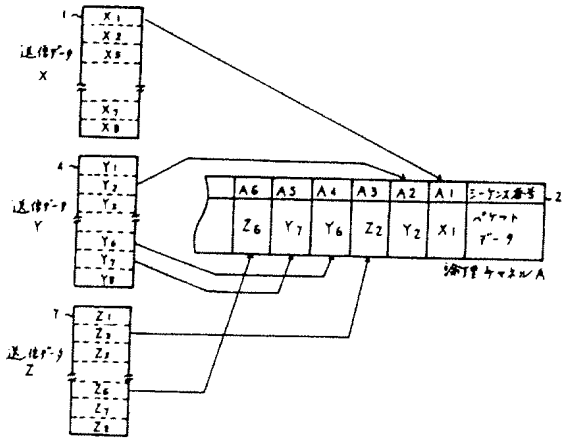
第1図



第2図

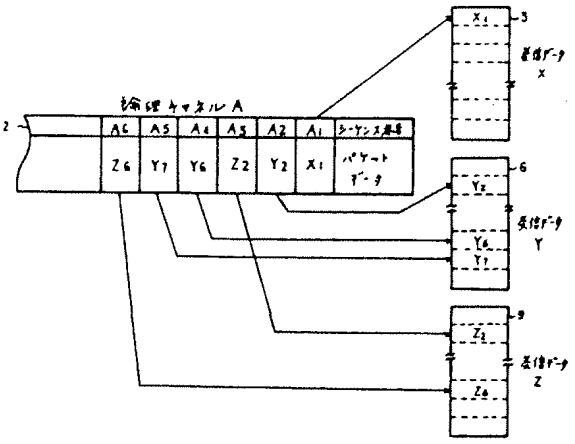
シーケンス番号	1	2	3	4	5	6	7	8
A	X_1	Y_2	Z_3	Y_6	Y_7	Z_8	X_6	X_8
B	Y_1	Y_3	Z_3	X_4	Y_4	Y_5	Y_8	Z_7
C	Z_1	X_2	X_3	X_5	Z_4	Z_5	X_7	Z_8

第3図

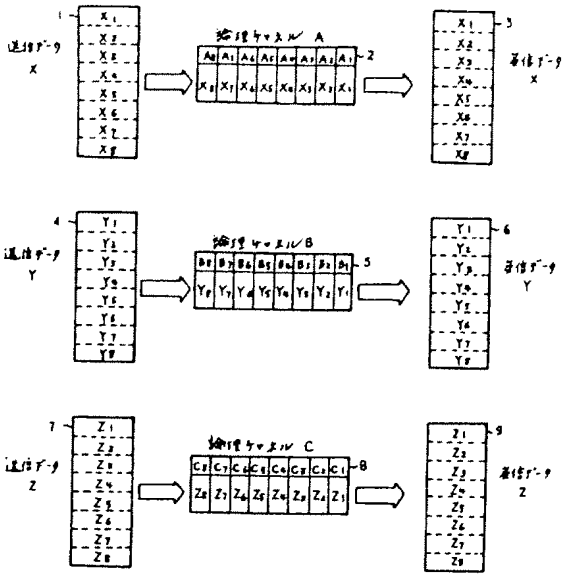


Petitioner Apple Inc. - Exhibit 1026, p. 726

第 4 図



第 5 図



Petitioner Apple Inc. - Exhibit 1026, p. 727

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-070531**

(43)Date of publication of application : **10.03.1998**

(51)Int.Cl. **H04L 12/22**
G06F 13/00
H04K 1/00

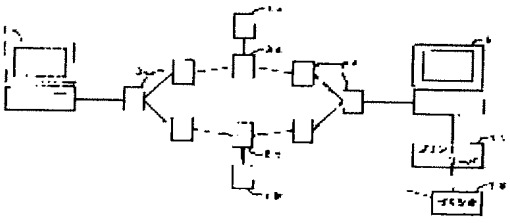
(21)Application number : **08-223898**

(22)Date of filing : **26.08.1996**

(71)Applicant : **BROTHER IND LTD**

(72)Inventor : **SUZUKI MASASHI**
MATSUDA KAZUHIKO
SAGOU AKIRA
KONDO HIROMOTO
YASUI TSUNEO

(54) DATA COMMUNICATION SYSTEM AND RECEIVER



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data communication system capable of satisfactorily preventing the leakage of data to be communicated.

SOLUTION: A personal computer 1 bi-sects data to be transmitted, adds transmission source data and transmission time data to the respective bisected data and transmits respective data to different servers 7a and 7b through different communication routes. Then the respective servers 7a and 7b transmit each received data to a server 5 through the communication route. The server 5 judges whether or not the transmission source data and transmission time data of the received data is matched with those of the already received data, and at the time they are matched, the received data is combined with the already received to obtain data before bisecting.

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]A data communication system provided with a sending set characterized by comprising the following which transmits data, and a receiving set which receives the above-mentioned data transmitted from this sending set.

A data dividing means into which it has two or more repeating installation which relays separately the above-mentioned data transmitted to the above-mentioned receiving set via a different communication path from the above-mentioned sending set, and the above-mentioned sending set divides the above-mentioned data at plurality.

An identification data grant means to give identification data which matches the data with each data divided in this data dividing means mutually.

A data sending means which transmits each data in which the above-mentioned identification data was given to the mutually different above-mentioned repeating installation.

A data-coupling means to combine the data which have and have identification data in which the above-mentioned receiving set corresponds mutually among each data received in a data receiving means which receives data separately from each above-mentioned repeating installation, and this data receiving means.

[Claim 2]The data communication system according to claim 1, wherein the above-mentioned identification data contains transmission source data showing common transmitting origin, and transmission time data showing having been mostly transmitted to identical time.

[Claim 3]The data communication system according to claim 1 or 2, wherein the above-mentioned identification data contains a serial number which has numerals common to at least a part.

[Claim 4]A receiving set comprising:

A data receiving means which receives data separately via mutually different repeating

installation.

A data-coupling means to combine the data which have the above-mentioned identification data mutually corresponding among data received from each data received in this data receiving means in an identification data extraction means to extract predetermined identification data, and the above-mentioned data receiving means.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the data communication system provided with the sending set which transmits data, and the receiving set which receives the data transmitted from the sending set, and a receiving set applicable to the data communication system.

[0002]

[Description of the Prior Art]Conventionally, in this kind of data communication system, receiving the data which transmitted data from the sending set via the telephone line and the cable, and was transmitted from that sending set with a receiving set is performed. Performing such data communications through the Internet is also considered in recent years.

[0003]

[Problem(s) to be Solved by the Invention]However, in this kind of data communication system, since the whole data was transmitted and received via a telephone line, a cable, etc., the data which spreads a telephone line, a cable, etc. may have been monitored by the 3rd person. For this reason, it was difficult to prevent disclosure of the data which communicates. Especially the Internet was easy to access and it was much more difficult to prevent disclosure of data.

[0004]Then, the invention according to claim 3 was made [that especially the invention according to claim 2 simplifies composition further for the purpose of the invention according to claim 1 to 3 providing the data communication system which can prevent disclosure of the data which communicates good, and] for the purpose of performing the reconstitution of data much more correctly. The invention according to claim 4 was made for the purpose of providing a receiving set applicable to the data communication system.

[0005]

[The means for solving a technical problem and an effect of the invention] The invention according to claim 1 made since the above-mentioned purpose was attained, In the data communication system provided with the sending set which transmits data, and the receiving set which receives the above-mentioned data transmitted from this sending set, Have two or more repeating installation which relays separately the above-mentioned data transmitted to the above-mentioned receiving set via a different communication path from the above-mentioned sending set, and. The data dividing means to which the above-mentioned sending set divides the above-mentioned data into plurality, and an identification data grant means to give the identification data in which the data is mutually matched with each data in which it was divided in this data dividing means, The data sending means which transmits each data in which the above-mentioned identification data was given to the mutually different above-mentioned repeating installation, It **** and is characterized by having a data-coupling means to combine the data which have identification data in which the above-mentioned receiving set corresponds mutually among each data received in the data receiving means which receives data separately from each above-mentioned repeating installation, and this data receiving means.

[0006]In this invention constituted in this way, a sending set divides data into plurality by a data dividing means, and gives the identification data which matches data with the data of each which was divided mutually by an identification data grant means. A sending set transmits each data in which the above-mentioned identification data was given to mutually different repeating installation by a data sending means. Then, each repeating installation relays each data separately via a mutually different communication path, and a receiving set receives each above-mentioned data separately from each repeating installation by a data receiving means. Then, a receiving set combines the data which have identification data mutually corresponding among each received data by a data-coupling means.

[0007]For this reason, data combined by a data-coupling means of a receiving set is in agreement with data before division by a data dividing means of a sending set. That is, it means that data before division was transmitted even to a receiving set. Data by which each above-mentioned communication path is spread via repeating installation is data after division by ******** and a data dividing means. For this reason, even if data by which a communication path is spread is monitored, that data will not be in agreement with data before division.

[0008]Therefore, in this invention, disclosure of data which communicates can be prevented good. As a communication path, a telephone line, the Internet besides a cable,

etc. are applicable, and also when it is any, disclosure of data can be prevented good. In addition to the composition according to claim 1, the invention according to claim 2 is characterized by the above-mentioned identification data containing transmission source data showing common transmitting origin, and transmission time data showing having been mostly transmitted to identical time.

[0009]That is, data after the above-mentioned division is usually transmitted to the almost same time (a difference is less than 1 minute) from the same sending set. So, in this invention, transmission source data which expresses common transmitting origin to the above-mentioned identification data, and transmission time data showing having been mostly transmitted to identical time are included. For this reason, in a receiving set, data can be combined easily and it can restore. A common sending set is also equipped with a function which gives transmission source data and transmission time data in many cases. Therefore, when this invention is applied to such a sending set, even if it does not provide composition special as an identification data grant means, the above-mentioned sending set can be realized.

[0010]Therefore, in addition to the effect according to claim 1, in this invention, an effect that it can simplify further produces composition of a sending set. The invention according to claim 3 is characterized by the above-mentioned identification data containing a serial number which has numerals common to at least a part in addition to the composition according to claim 1 or 2.

[0011]In this invention constituted in this way, data after division is matched using a serial number which has common numerals at least in part. For this reason, the data after division can be matched very correctly. For example, when each data after division is long and transmission time of each data shifts substantially, each data can be matched good.

[0012]Therefore, in addition to the effect of the invention according to claim 1 or 2, in this invention, an effect that it can restore much more correctly produces data after division. The receiving set according to claim 4 is provided with the following.

A data receiving means which receives data separately via mutually different repeating installation.

An identification data extraction means to extract predetermined identification data from each data received in this data receiving means.

A data-coupling means to combine the data which have the above-mentioned identification data mutually corresponding among data received in the above-mentioned data receiving means.

[0013]With this invention constituted in this way, a data receiving means receives data separately via mutually different repeating installation, and an identification data extraction means extracts predetermined identification data from each received data. Then, a data-coupling means combines the data which have identification data mutually corresponding among data received in a data receiving means.
[0014]For this reason, this invention is applicable good as a receiving set in the data communication system according to any one of claims 1 to 3. the above-mentioned identification data may contain transmission source data showing common transmitting origin, and transmission time data showing having been mostly transmitted to identical time, may contain a serial number which boils a part at least and has common numerals, and may be a thing of other gestalten.
[0015]
[Embodiment of the Invention]Next, an embodiment of the invention is described with a drawing. Drawing 1 is an outline lineblock diagram showing the data communication system which applied this invention. This embodiment applies this invention to the network print system using the Internet.
[0016]As shown in drawing 1, the personal computer (henceforth a personal computer) 1 of the users as a sending set is connected to the server 5 as a receiving set by the side of a print service station via the Internet which connects many providers 3. For this reason, if data is transmitted towards the server 5 from the personal computer 1, that data will be spread via [the adjoining provider 3] one by one. The data which communicates the Internet top is once memorized to the two providers 3a and 3b who exist on a different communication path, and the servers 7a and 7b as repeating installation which changes an address (address of a transmission destination) and transmits are connected to them.
[0017]The personal computer 1 and the servers 5, 7a, and 7b are all the computers of the common knowledge provided with the external memory or the modem for communication besides CPU, ROM, and RAM, and the printer 13 is further connected to the server 5 via the print server 11. This system is for transmitting image data etc. to the server 5 of a print service station (printer) from users' (customer) personal computer 1, and performing image formation with the printer 13. The servers 5, 7a, and 7b may be FTP (file transfer protocol) servers, or may be mail servers.
[0018]Next, processing of the personal computer 1 in this system and the servers 5, 7a, and 7b is explained using drawing 2 - the flow chart of four. Users' personal computer 1 will perform processing of drawing 2, if transmission of data is directed via the keyboard etc. which are not illustrated. If processing is started as shown in drawing 2,

the data first transmitted in S1 will be read, and the data will be divided into two by S3 continuing. The 1st data after division is transmitted to the 1st address corresponding to the server 7a, by S7, the 2nd data after division is transmitted to the 2nd address corresponding to the server 7b, and processing is ended S5 continuing. In transmission of the data in S5 and S7, the transmission source data showing the address of the personal computer 1 which is a transmitting agency, and the transmission time data showing the transmission time are given to the data to transmit. Since this processing is common knowledge, it is not explained in full detail here. It is good also considering which of the data after division as the 1st at S5 and S7.

[0019]On the other hand, the server 7a carries out repeat execution of the processing shown in drawing 3. The server 7b also carries out repeat execution of the same processing. As shown in drawing 3, when processing was started, and it judges whether data was received or not and receives in S11 (S11:YES), it shifts to S13. The received data is stored in a predetermined memory by the routine of the common knowledge which is not illustrated. In S13, the received data is transmitted to the prescribed address corresponding to the server 5, and it shifts to S11. When data is not received (S11:NO), it stands by in S11 as it is.

[0020]For this reason, if the data after the personal computer 1 dividing is transmitted to the servers 7a and 7b by processing of drawing 2 (S5, S7), by processing of drawing 3, the servers 7a and 7b will receive each data after division separately (S11;YES), and will transmit that data to the server 5 (S13). That is, the data after division is transmitted to the server 5 via a different communication path.

[0021]Next, drawing 4 is a flow chart showing the processing in which the server 5 carries out repeat execution. If processing is started, when it judges whether data was received or not and receives in S21 (S21:YES), it will shift to S23. The received data is stored in a predetermined memory by the routine of the common knowledge which is not illustrated. In S23, the transmission source data given to the data judges whether a match has a match, i.e., the address of a transmitting agency, in the data which already receives and is stored in the memory. The data whose transmission time which shifts to S25 and transmission time data expresses in the already received data if there are data received in S21 and data whose address of a transmitting agency corresponds (S23:YES) corresponds mostly judges whether it is in it.

[0022]When an affirmative judgment is carried out by S25, the data received in S21 and the corresponding data which already received and was stored in the memory are the data continuously transmitted by S5 of drawing 2, and S7. Then, the data after combination is sent to the print server 11 in S29 which combines two data in S27 and

continues in this case (S25:YES), and it returns to S21. Then, image formation with the printer 13 is performed based on the data after combination, i.e., the data read in S1 of drawing 2. On the other hand, when a negative judgment is carried out by SS21, S23, or 25, nothing is done but it returns to S21 as it is.

[0023]Thus, in this system, it can restore by the server 5 and image formation of the data transmitted via a communication path which divides with the personal computer 1 and is different can be carried out with the printer 13. The data spread via each provider 3 is data after division, respectively. For this reason, even if the data spread via each provider 3 is monitored, that data will not be in agreement with the data before division. Therefore, in this system, disclosure of the data which communicates can be prevented good. In this system, the data which should be combined in S27 is identified with transmission source data and transmission time data. The common personal computer is also equipped with the function which gives transmission source data and transmission time data in many cases. In this system, since such a general function is used, processing can be simplified further.

[0024]Next, other embodiments of this invention are described using drawing 5 - the flow chart of seven. In this embodiment, since only processing of each part differs from the above-mentioned embodiment, the numerals used by drawing 2 are used as it is. In drawing 5 -7, the same numerals are given to drawing 2 - the same processing as four, and detailed explanation of processing is omitted to them.

[0025]Drawing 5 is a flow chart showing the processing which the personal computer 1 performs, when transmission of data is directed. After reading the data to transmit (S1) and dividing the data into two if processing is started as shown in drawing 5 (S3), it shifts to S31. In S31, a serial number is generated using a random number etc. from current time. As a serial number, the thing containing numerals other than numbers, such as the alphabet, may be adopted. In S33 continuing, "1" of the serial number and a number is given to the 1st data, and "2" of the above-mentioned serial number and a number is given to the 2nd data in S35. Then, each data after the division to which the serial number etc. were given is transmitted to the 1st and 2nd addresses (it corresponds to the servers 7a and 7b), and processing is ended (S5, S7).

[0026]Drawing 6 is a flow chart showing the processing in which the servers 7a and 7b carry out repeat execution. If data is received (S11:YES), it will shift to S41, and it is judged whether the serial number is given to the data. When given (S41:YES), it shifts to S13, and data is transmitted to the prescribed address corresponding to the server 5, and it shifts to S11. When data is not received (S11:NO), and when the serial number is not given (S41:NO), it shifts to S11 as it is. That is, since it is not the data transmitted

by S5 of drawing 5, and S7 when the serial number is not given, other routines which are not illustrated perform the usual processing as the servers 7a and 7b.

[0027]Drawing 7 is a flow chart showing the processing in which the server 5 carries out repeat execution. In this processing, if data is received (S21:YES), it will shift to S51, and it is judged whether the serial number is given to that data. It is judged whether there are what was given to the data, and a thing which has the same serial number in the data which shifts to S53 when given (S51:YES), already receives, and is stored in the memory.

[0028]When an affirmative judgment is carried out by S53, the data received in S21 and the corresponding data which already received and was stored in the memory are the data continuously transmitted by S5 of drawing 5, and S7. Then, two data is combined in this case (S27), and it sends to the print server 11 (S29). Then, image formation with the printer 13 is performed based on the data after combination. On the other hand, when a negative judgment is carried out by SS21, S51, or 53, nothing is done but it returns to S21 as it is.

[0029]When this embodiment also divides data and makes a different communication path spread like the above-mentioned embodiment, disclosure of data can be prevented good. In this system, the data after division is matched using the serial number. For this reason, data can be restored much more correctly. For example, when each data after division is long and the transmission time of each data shifts substantially (i.e., when S5 of drawing 5 and the interval of S7 become large etc.), each data is matched good. When there is no serial number in data (S41:NO), the servers 7a and 7b perform the usual processing. For this reason, it is not necessary to extend the servers 7a and 7b for the above-mentioned processing.

[0030]The processing which gives the transmission source data and transmission time data in S5 and S7 in each above-mentioned embodiment, And in processing of S33 and S35, processing of S3 for an identification data grant means to a data dividing means. In transmitting processing of the data in S5 and S7, processing of S21 to a data sending means to a data receiving means. The processing which extracts transmission source data [in / to a data-coupling means / in processing of S27 / S23, S25, S51, and S53], transmission time data, or a serial number is equivalent to an identification data extraction means, respectively.

[0031]This invention is not limited to the above-mentioned embodiment at all, and can be carried out with various gestalten in the range which does not deviate from the gist of this invention. For example, this invention is applicable to the data communication system using various communication paths, such as a telephone line, a cable, radio

besides using the Internet a data communication system. However, the Internet is very easy to access. Therefore, when it applies to the data communication system using the Internet like the above-mentioned embodiment, the effect of the leakage control of the data based on this invention becomes much more remarkable.

[0032]Although this invention is applied to the server 5 of a receiver in the above-mentioned embodiment to the network print system which connected the printer 13, in addition to this, this invention is applicable to various data communication systems. For example, it is applicable also to the system which only transmits and receives data. In this case, what is necessary is just to omit processing (drawing 4, drawing 7) of the five serverS29.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is an outline lineblock diagram showing the data communication system which applied this invention.

[Drawing 2]It is a flow chart showing processing of the transmitting side personal computer of the system.

[Drawing 3]It is a flow chart showing processing of the server for relay of the system.

[Drawing 4]It is a flow chart showing processing of the receiver server of the system.

[Drawing 5]It is a flow chart showing other gestalten of processing of the above-mentioned transmitting side personal computer.

[Drawing 6]It is a flow chart showing other gestalten of processing of the above-mentioned server for relay.

[Drawing 7]It is a flow chart showing other gestalten of processing of the above-mentioned receiver server.

[Description of Notations]

1 -- Personal computer 3 -- Provider 5, 7a, 7b -- Server

11 -- Print server 13 -- Printer

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－70531

(43)公開日　平成10年(1998)３月10日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　12/22		9744－5K	Ｈ０４Ｌ	11/26	
Ｇ０６Ｆ　13/00	３５１		Ｇ０６Ｆ	13/00	３５１Ａ
Ｈ０４Ｋ　1/00			Ｈ０４Ｋ	1/00	Ｚ

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願平8－223898

(22)出願日　平成８年(1996)８月26日

(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町15番１号

(72)発明者　鈴木　正史
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

(72)発明者　松田　和彦
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

(72)発明者　佐郷　朗
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

(74)代理人　弁理士　足立　勉

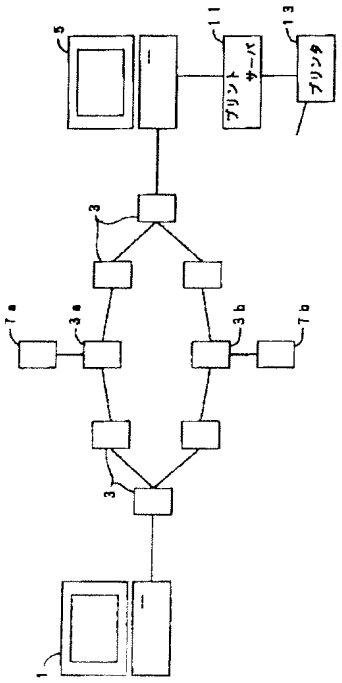
最終頁に続く

(54)【発明の名称】　データ通信システムおよび受信装置

(57)【要約】

【課題】　通信されるデータの漏洩を良好に防止できるデータ通信システムを提供することである。

【解決手段】　パソコン１によって、送信するデータを二つに分割し、その分割した各データにそれぞれ送信元データや送信時刻データを付して、その各データを異なる通信経路を介して別々のサーバ７ａ，７ｂに送信する。そして、各サーバ７ａ，７ｂは、受信した各データを異なる通信経路を介してサーバ５に送信する。サーバ５は、受信したデータと、既に受信しているデータとについて、前記送信元データや送信時刻データが一致するか否かを判断し、一致した場合は前記受信したデータと既に受信しているデータとを結合して分割前のデータにさせる。



Petitioner Apple Inc. - Exhibit 1026, p. 738

1

【特許請求の範囲】
【請求項１】　データを送信する送信装置と、
該送信装置から送信された上記データを受信する受信装置と、
を備えたデータ通信システムにおいて、
上記送信装置から上記受信装置へ送信される上記データを、異なる通信経路を介して個々に中継する複数の中継装置を備えると共に、
上記送信装置が、
上記データを複数に分割するデータ分割手段と、
該データ分割手段にて分割された個々のデータに、そのデータ同士を互いに対応付ける識別データを付与する識別データ付与手段と、
上記識別データが付与された各データを、互いに異なる上記中継装置へ送信するデータ送信手段と、
を有し、
上記受信装置が、
上記各中継装置から個々にデータを受信するデータ受信手段と、
該データ受信手段にて受信した各データの内、互いに対応する識別データを有するデータ同士を結合するデータ結合手段と、
を有することを特徴とするデータ通信システム。
【請求項２】　上記識別データが、共通の送信元を表す送信元データと、ほぼ同一時刻に送信されたことを表す送信時刻データとを含むことを特徴とする請求項１記載のデータ通信システム。
【請求項３】　上記識別データが、少なくとも一部分に共通の符号を有するシリアルナンバーを含むことを特徴とする請求項１または２記載のデータ通信システム。
【請求項４】　互いに異なる中継装置を介して個々にデータを受信するデータ受信手段と、
該データ受信手段にて受信した各データから、所定の識別データを抽出する識別データ抽出手段と、
上記データ受信手段にて受信したデータの内、互いに対応する上記識別データを有するデータ同士を結合するデータ結合手段と、
を備えたことを特徴とする受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データを送信する送信装置と、その送信装置から送信されたデータを受信する受信装置とを備えたデータ通信システム、およびそのデータ通信システムに適用可能な受信装置に関する。
【０００２】
【従来の技術】従来、この種のデータ通信システムでは、電話回線やケーブルを介して送信装置からデータを送信し、その送信装置から送信されたデータを受信装置にて受信することが行われている。また、近年、インターネットを通じてこのようなデータ通信を行うことも考

2

えられている。
【０００３】
【発明が解決しようとする課題】ところが、この種のデータ通信システムでは、電話回線やケーブル等を介してデータ全体が送受信されるので、電話回線やケーブル等を伝搬するデータが第３者によって傍受される可能性があった。このため、通信されるデータの漏洩を防止するのが困難であった。特に、インターネットはアクセスが容易であり、データの漏洩を防止することが一層困難であった。
【０００４】そこで、請求項１～３記載の発明は、通信されるデータの漏洩を良好に防止できるデータ通信システムを提供することを目的とし、特に、請求項２記載の発明は構成を一層簡略化することを、請求項３記載の発明はデータの復元を一層正確に行うことを目的としてなされた。また、請求項４記載の発明は、そのデータ通信システムに適用可能な受信装置を提供することを目的としてなされた。
【０００５】
【課題を解決するための手段および発明の効果】上記目的を達するためになされた請求項１記載の発明は、データを送信する送信装置と、該送信装置から送信された上記データを受信する受信装置と、を備えたデータ通信システムにおいて、上記送信装置から上記受信装置へ送信される上記データを、異なる通信経路を介して個々に中継する複数の中継装置を備えると共に、上記送信装置が、上記データを複数に分割するデータ分割手段と、該データ分割手段にて分割された個々のデータに、そのデータ同士を互いに対応付ける識別データを付与する識別データ付与手段と、上記識別データが付与された各データを、互いに異なる上記中継装置へ送信するデータ送信手段と、を有し、上記受信装置が、上記各中継装置から個々にデータを受信するデータ受信手段と、該データ受信手段にて受信した各データの内、互いに対応する識別データを有するデータ同士を結合するデータ結合手段と、を有することを特徴としている。
【０００６】このように構成された本発明では、送信装置は、データ分割手段によりデータを複数に分割し、その分割された個々のデータに、データ同士を互いに対応付ける識別データを、識別データ付与手段によって付与する。更に、送信装置は、データ送信手段により、上記識別データが付与された各データを互いに異なる中継装置に送信する。すると、各中継装置は、各データを互いに異なる通信経路を介して個々に中継し、受信装置は、データ受信手段により、上記各データを各中継装置から個々に受信する。続いて、受信装置は、データ結合手段により、受信した各データの内、互いに対応する識別データを有するデータ同士を結合する。
【０００７】このため、受信装置のデータ結合手段により結合されたデータは、送信装置のデータ分割手段によ

Petitioner Apple Inc. - Exhibit 1026, p. 739

る分割前のデータと一致する。すなわち、分割前のデータが受信装置まで送信されたことになる。また、中継装置を介して上記各通信経路を伝搬されるデータは、ぞれぞれ、データ分割手段による分割後のデータである。このため、通信経路を伝搬されるデータが仮に傍受されても、そのデータは分割前のデータとは一致しない。

【０００８】従って、本発明では、通信されるデータの漏洩を良好に防止することができる。なお、通信経路としては、電話回線やケーブルの他、インターネット等も適用することができ、いずれの場合もデータの漏洩を良好に防止することができる。請求項２記載の発明は、請求項１記載の構成に加え、上記識別データが、共通の送信元を表す送信元データと、ほぼ同一時刻に送信されたことを表す送信時刻データとを含むことを特徴としている。

【０００９】すなわち、上記分割後のデータは、通常、同じ送信装置からほぼ同じ時刻（例えば差が１分未満）に送信される。そこで、本発明では、上記識別データに、共通の送信元を表す送信元データと、ほぼ同一時刻に送信されたことを表す送信時刻データとを含めている。このため、受信装置では、データを容易に結合して復元することができる。また、送信元データおよび送信時刻データを付与する機能は、一般の送信装置にも備えられている場合が多い。よって、このような送信装置に本発明を適用した場合、識別データ付与手段として特別な構成を設けなくても上記送信装置を実現することができる。

【００１０】従って、本発明では、請求項１記載の効果に加えて、送信装置の構成を一層簡略化することができるといった効果が生じる。請求項３記載の発明は、請求項１または２記載の構成に加え、上記識別データが、少なくとも一部分に共通の符号を有するシリアルナンバーを含むことを特徴としている。

【００１１】このように構成された本発明では、分割後のデータを少なくとも一部に共通の符号を有するシリアルナンバーを用いて対応付けている。このため、分割後のデータ同士をきわめて正確に対応付けることができる。例えば、分割後の各データが長くて各データの送信時刻が大幅にずれたときなどにも、各データを良好に対応付けることができる。

【００１２】従って、本発明では、請求項１または２記載の発明の効果に加えて、分割後のデータを一層正確に復元することができるといった効果が生じる。請求項４記載の受信装置は、互いに異なる中継装置を介して個々にデータを受信するデータ受信手段と、該データ受信手段にて受信した各データから、所定の識別データを抽出する識別データ抽出手段と、上記データ受信手段にて受信したデータの内、互いに対応する上記識別データを有するデータ同士を結合するデータ結合手段と、を備えたことを特徴としている。

【００１３】このように構成された本発明では、データ受信手段は互いに異なる中継装置を介して個々にデータを受信し、識別データ抽出手段は、受信した各データから所定の識別データを抽出する。すると、データ結合手段は、データ受信手段にて受信したデータの内、互いに対応する識別データを有するデータ同士を結合する。

【００１４】このため、本発明は、請求項１～３のいずれかに記載のデータ通信システムにおける受信装置として、良好に適用することができる。なお、上記識別データは、共通の送信元を表す送信元データと、ほぼ同一時刻に送信されたことを表す送信時刻データとを含むものであってもよく、少なくとも一部分に共通の符号を有するシリアルナンバーを含むものであってもよく、その他の形態のものであってもよい。

【００１５】

【発明の実施の形態】次に、本発明の実施の形態を図面と共に説明する。図１は本発明を適用したデータ通信システムを表す概略構成図である。なお、本実施の形態は、インターネットを利用したネットワークプリントシステムに本発明を適用したものである。

【００１６】図１に示すように、送信装置としてのユーザー側のパーソナルコンピュータ（以下パソコンという）１は、多数のプロバイダ３を接続してなるインターネットを介してプリントサービスステーション側の受信装置としてのサーバ５に接続されている。このため、パソコン１からサーバ５に向けてデータを送信すると、そのデータは隣接するプロバイダ３を順次経由して伝搬される。また、異なる通信経路上に存在する二つのプロバイダ３ａ，３ｂには、インターネット上を通信されるデータを一旦記憶し、宛名（送信先のアドレス）を変えて送信する中継装置としてのサーバ７ａ，７ｂが接続されている。

【００１７】なお、パソコン１およびサーバ５，７ａ，７ｂは、いずれも、ＣＰＵ，ＲＯＭ，ＲＡＭの他、外付けのメモリや通信用のモデムを備えた周知のコンピュータで、サーバ５には、更に、プリントサーバ１１を介してプリンタ１３が接続されている。本システムは、ユーザー（顧客）側のパソコン１からプリントサービスステーション（印刷業者）のサーバ５へ画像データ等を送信して、プリンタ１３による画像形成を行うためのものである。また、サーバ５，７ａ，７ｂは、ＦＴＰ（ファイル・トランスファー・プロトコル）サーバであっても、メールサーバであってもよい。

【００１８】次に、本システムにおけるパソコン１およびサーバ５，７ａ，７ｂの処理を、図２～４のフローチャートを用いて説明する。ユーザー側のパソコン１は、図示しないキーボード等を介してデータの送信が指示されると、図２の処理を実行する。図２に示すように、処理を開始すると、先ずＳ１にて送信するデータを読み込み、続くＳ３でそのデータを二つに分割する。続くＳ５

Petitioner Apple Inc. - Exhibit 1026, p. 740

では、分割後の１つ目のデータをサーバ７ａに対応する第１アドレスへ送信し、Ｓ７では、分割後の２つ目のデータをサーバ７ｂに対応する第２アドレスへ送信して処理を終了する。なお、Ｓ５，Ｓ７におけるデータの送信に当たっては、送信元であるパソコン１のアドレスを表す送信元データと、その送信時刻を表す送信時刻データとが、送信するデータに付与される。この処理は周知であるのでここでは詳述しない。また、Ｓ５，Ｓ７では分割後のデータのどちらを１つ目としてもよい。

【００１９】一方、サーバ７ａは図３に示す処理を繰り返し実行する。なお、サーバ７ｂも同様の処理を繰り返し実行する。図３に示すように、処理を開始すると、Ｓ１１にてデータを受信したか否かを判断し、受信した場合（Ｓ１１：ＹＥＳ）はＳ１３へ移行する。なお、受信したデータは、図示しない周知のルーチンにより所定のメモリに格納される。Ｓ１３では、受信したデータをサーバ５に対応する所定アドレスへ送信してＳ１１へ移行する。また、データを受信していない場合（Ｓ１１：ＮＯ）は、そのままＳ１１にて待機する。

【００２０】このため、図２の処理により、パソコン１が分割後のデータをサーバ７ａ，７ｂに送信すると（Ｓ５，Ｓ７）、図３の処理により、サーバ７ａ，７ｂは分割後の各データを個々に受信し（Ｓ１１；ＹＥＳ）、そのデータをサーバ５に送信する（Ｓ１３）。すなわち、分割後のデータが異なる通信経路を介してサーバ５に送信される。

【００２１】次に、図４はサーバ５が繰り返し実行する処理を表すフローチャートである。処理を開始すると、Ｓ２１にてデータを受信したか否かを判断し、受信した場合（Ｓ２１：ＹＥＳ）はＳ２３へ移行する。なお、受信したデータは、図示しない周知のルーチンにより所定のメモリに格納される。Ｓ２３では、既に受信してメモリに格納されているデータの中で、そのデータに付与された送信元データが一致するもの、すなわち、送信元のアドレスが一致するものがあるか否かを判断する。既に受信したデータの中で、Ｓ２１にて受信したデータと送信元のアドレスが一致するデータがあれば（Ｓ２３：ＹＥＳ）、Ｓ２５へ移行し、送信時刻データが表す送信時刻がほぼ一致するデータが、その中にあるか否かを判断する。

【００２２】Ｓ２５で肯定判断した場合、Ｓ２１にて受信したデータと、既に受信してメモリに格納されていた該当データとは、図２のＳ５，Ｓ７で連続して送信されたデータである。そこで、この場合（Ｓ２５：ＹＥＳ）、Ｓ２７にて二つのデータを結合し、続くＳ２９にて結合後のデータをプリントサーバ１１へ送付してＳ２１へ戻る。すると、結合後のデータ、すなわち、図２のＳ１にて読み込まれたデータに基づき、プリンタ１３による画像形成が実行される。一方、Ｓ２１，Ｓ２３，Ｓ２５のいずれかで否定判断した場合は、何もせずそのままＳ２１へ戻る。

【００２３】このように、本システムでは、パソコン１により分割して異なる通信経路を介して送信されたデータを、サーバ５にて復元し、プリンタ１３にて画像形成することができる。また、各プロバイダ３を介して伝搬されるデータは、それぞれ分割後のデータである。このため、各プロバイダ３を介して伝搬されるデータが仮に傍受されても、そのデータは分割前のデータとは一致しない。従って、本システムでは、通信されるデータの漏洩を良好に防止することができる。更に、本システムでは、Ｓ２７にて結合すべきデータを、送信元データおよび送信時刻データによって識別している。送信元データおよび送信時刻データを付与する機能は、一般のパソコンにも備えられている場合が多い。本システムでは、このような一般的な機能を利用しているので、処理を一層簡略化することができる。

【００２４】次に、本発明の他の実施の形態を図５～７のフローチャートを用いて説明する。なお、本実施の形態では、前述の実施の形態とは各部の処理のみが異なるので、図２で使用した符号等はそのまま使用する。また、図５～７では、図２～４と同様の処理には同一の符号を付して、処理の詳細な説明を省略する。

【００２５】図５は、データの送信が指示されたときパソコン１が実行する処理を表すフローチャートである。図５に示すように、処理を開始すると、送信するデータを読み込み（Ｓ１）、そのデータを二つに分割した（Ｓ３）後、Ｓ３１へ移行する。Ｓ３１では、現在時刻から乱数等を用いてシリアルナンバーを発生する。なお、シリアルナンバーとしては、アルファベット等の数字以外の符号を含むものを採用してもよい。続くＳ３３では、１つ目のデータにそのシリアルナンバーおよび数字の「１」を付与し、Ｓ３５では、２つ目のデータに上記シリアルナンバーおよび数字の「２」を付与する。続いて、シリアルナンバー等が付与された分割後の各データを、第１および第２のアドレス（サーバ７ａおよび７ｂに対応）に送信して処理を終了する（Ｓ５，Ｓ７）。

【００２６】図６はサーバ７ａ，７ｂが繰り返し実行する処理を表すフローチャートである。データを受信すると（Ｓ１１：ＹＥＳ）Ｓ４１へ移行し、そのデータにシリアルナンバーが付与されているか否かを判断する。付与されている場合（Ｓ４１：ＹＥＳ）はＳ１３へ移行し、データをサーバ５に対応する所定アドレスへ送信してＳ１１へ移行する。また、データを受信していない場合（Ｓ１１：ＮＯ）、およびシリアルナンバーが付与されていない場合（Ｓ４１：ＮＯ）は、そのままＳ１１へ移行する。すなわち、シリアルナンバーが付与されていない場合は、図５のＳ５，Ｓ７によって送信されたデータではないので、図示しない他のルーチンにより、サーバ７ａ，７ｂとしての通常の処理を行うのである。

【００２７】図７は、サーバ５が繰り返し実行する処理

Petitioner Apple Inc. - Exhibit 1026, p. 741

を表すフローチャートである。この処理では、データを受信すると（Ｓ２１：ＹＥＳ）Ｓ５１へ移行し、そのデータにシリアルナンバーが付与されているか否かを判断する。付与されている場合（Ｓ５１：ＹＥＳ）Ｓ５３へ移行し、既に受信してメモリに格納されているデータの中で、そのデータに付与されたものと同一のシリアルナンバーを有するものがあるか否かを判断する。

【００２８】Ｓ５３で肯定判断した場合、Ｓ２１にて受信したデータと、既に受信してメモリに格納されていた該当データとは、図５のＳ５，Ｓ７で連続して送信されたデータである。そこで、この場合、二つのデータを結合し（Ｓ２７）、プリントサーバ１１へ送付する（Ｓ２９）。すると、結合後のデータに基づき、プリンタ１３による画像形成が実行される。一方、Ｓ２１，Ｓ５１，Ｓ５３のいずれかで否定判断した場合は、何もせずそのままＳ２１へ戻る。

【００２９】本実施の形態でも、前述の実施の形態と同様、データを分割し、異なる通信経路を伝搬させることにより、データの漏洩を良好に防止することができる。また、本システムでは、分割後のデータをシリアルナンバーを用いて対応付けている。このため、データを一層正確に復元することができる。例えば、分割後の各データが長くて各データの送信時刻が大幅にずれたとき、すなわち、図５のＳ５，Ｓ７の間隔が大きくなったときなどにも、各データが良好に対応付けられる。更に、データにシリアルナンバーがない場合（Ｓ４１：ＮＯ）、サーバ７ａ，７ｂは通常の処理を行う。このため、上記処理のためにサーバ７ａ，７ｂを増設する必要もない。

【００３０】なお、上記各実施の形態において、Ｓ５，Ｓ７における送信元データおよび送信時刻データを付与する処理、並びに、Ｓ３３，Ｓ３５の処理が識別データ付与手段に、Ｓ３の処理がデータ分割手段に、Ｓ５，Ｓ７におけるデータの送信処理がデータ送信手段に、Ｓ２１の処理がデータ受信手段に、Ｓ２７の処理がデータ結合手段に、Ｓ２３，Ｓ２５，Ｓ５１，Ｓ５３における送信元データ，送信時刻データ，またはシリアルナンバーを抽出する処理が識別データ抽出手段に、それぞれ相当する。

【００３１】また、本発明は、上記実施の形態になんら限定されるものではなく、本発明の要旨を逸脱しない範囲で種々の形態で実施することができる。例えば、本発明は、インターネットを利用したデータ通信システムの他、電話回線やケーブル，無線等、種々の通信経路を利用したデータ通信システムに適用することができる。但し、インターネットはきわめてアクセスが容易である。従って、上記実施の形態のように、インターネットを利用したデータ通信システムに適用した場合、本発明によるデータの漏洩防止の効果が一層顕著になる。

【００３２】更に、上記実施の形態では、受信側のサーバ５にプリンタ１３を接続したネットワークプリントシステムに対して本発明を適用しているが、本発明は、この他種々のデータ通信システムに適用することができる。例えば、単にデータを送受信するだけのシステムにも適用することができる。この場合、サーバ５のＳ２９の処理（図４，図７）を省略すればよい。

【図面の簡単な説明】

【図１】本発明を適用したデータ通信システムを表す概略構成図である。

【図２】そのシステムの送信側パソコンの処理を表すフローチャートである。

【図３】そのシステムの中継用サーバの処理を表すフローチャートである。

【図４】そのシステムの受信側サーバの処理を表すフローチャートである。

【図５】上記送信側パソコンの処理の他の形態を表すフローチャートである。

【図６】上記中継用サーバの処理の他の形態を表すフローチャートである。

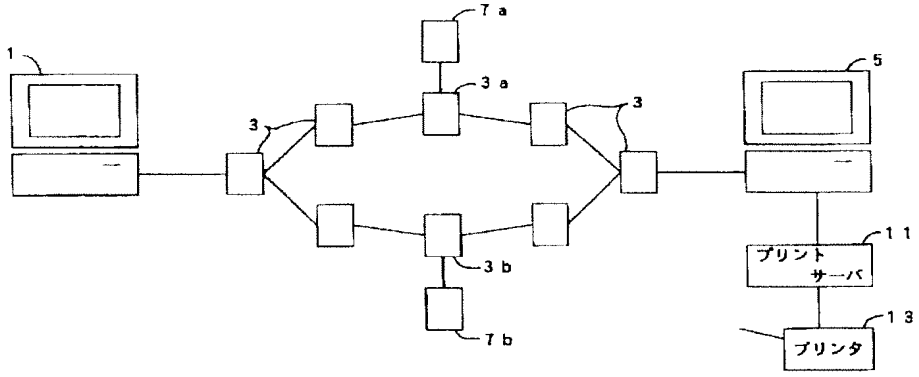
【図７】上記受信側サーバの処理の他の形態を表すフローチャートである。

【符号の説明】

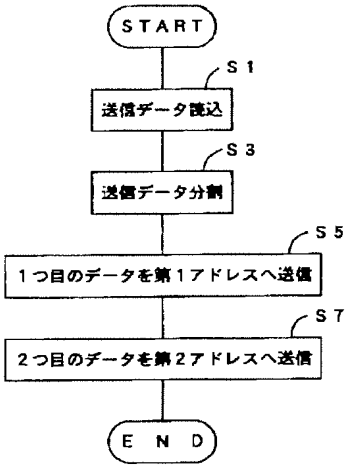
１…パソコン　　３…プロバイダ
５，７ａ，７ｂ…サーバ
１１…プリントサーバ　　１３…プリンタ

Petitioner Apple Inc. - Exhibit 1026, p. 742

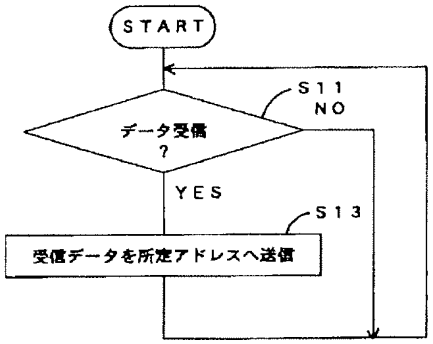
【図１】


1
7a
3a
3
3
5
11
プリントサーバ
3b
7b
13
プリンタ

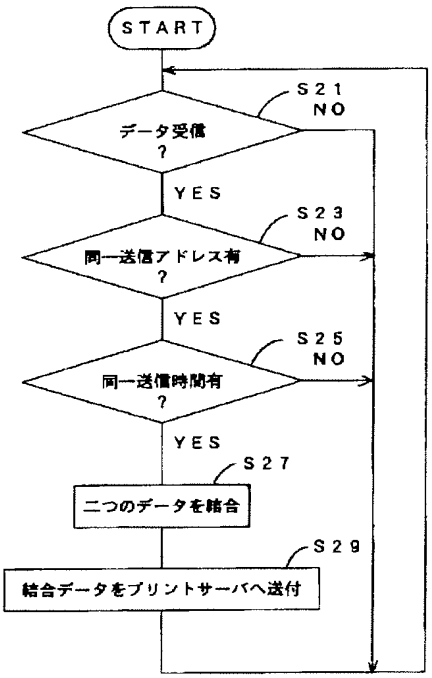
【図２】


START
S1
送信データ読込
S3
送信データ分割
S5
1つ目のデータを第1アドレスへ送信
S7
2つ目のデータを第2アドレスへ送信
END

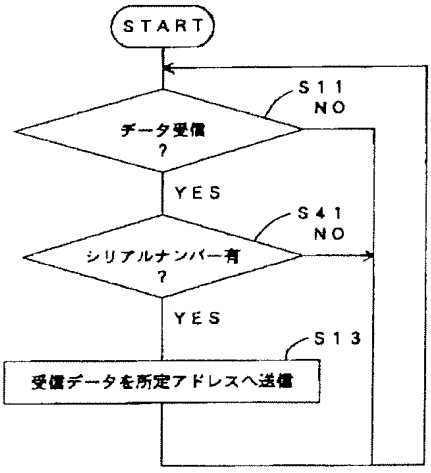
【図３】


START
S11
NO
データ受信？
YES
S13
受信データを所定アドレスへ送信

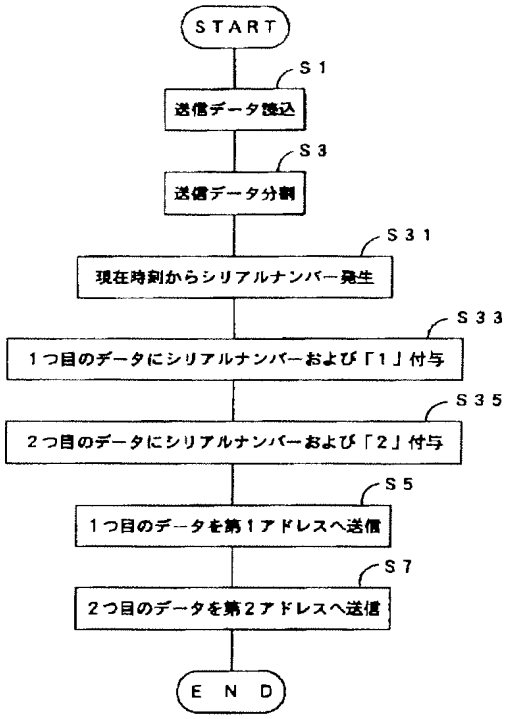
【図４】


START
S21
NO
データ受信？
YES
S23
NO
同一送信アドレス有？
YES
S25
NO
同一送信時間有？
YES
S27
二つのデータを結合
S29
結合データをプリントサーバへ送付

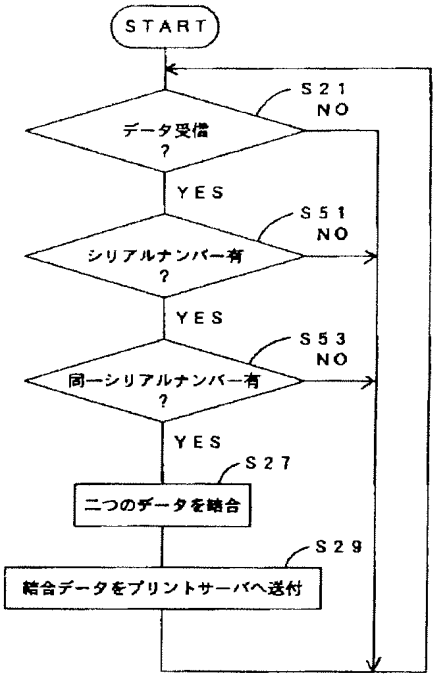
【図６】


START
S11
NO
データ受信？
YES
S41
NO
シリアルナンバー有？
YES
S13
受信データを所定アドレスへ送信

【図５】



【図７】



フロントページの続き

(72)発明者　近藤　博大
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

(72)発明者　安井　恒夫
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **04-363941**

(43)Date of publication of application : **16.12.1992**

(51)Int.Cl. **H04L 12/48**
H04L 9/00
H04L 9/10
H04L 9/12

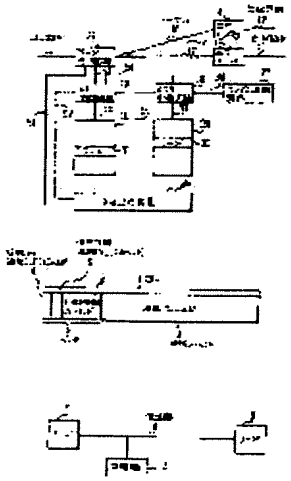
(21)Application number : **03-044062**

(22)Date of filing : **18.02.1991**

(71)Applicant : **NIPPON TELEGR & TELEPH CORP <NTT>**

(72)Inventor : **NAKAJIMA SEIICHI**
HARADA YONOSUKE

(54) INTERCEPT PREVENTION METHOD IN ASYNCHRONOUS TRANSFER MODE COMMUNICATION



(57)Abstract:

PURPOSE: To prevent intercept without losing high speed performance of the asynchronous transfer mode(ATM) by using optional one of plural virtual bus identifiers (VPI) and virtual line identifiers (VCI) allocated to one call channel at random so as to transfer a cell.

CONSTITUTION: Plural VPI, VCI are assigned to one call channel and one of the plural VCI, VPI allocated is used at random optionally to transfer a cell. Since the VPI, VCI relating to the same call channel are always changed in the unit of cells through a transmission line 9 between a transmission node and a reception node, even when a cell having the specific VPI, VCI is extracted, it is impossible to collect the communication content of the specific call. Even when all cells on the transmission line 9 are collected, it is difficult to extract a cell of the specific call and the intercept is prevented. Furthermore, since only the VPI and VCI are revised in the unit of cells, the processing of the header 2 is easy and intercept is prevented without losing the high speed performance of the ATM.

Cited Document 3 (JP-A (Kokai) H04-363941)

<1>

[0019]

[Effects of the Invention]

As explained above, in the method of preventing intercept in ATM communication of the present invention, a plurality of VPIs and VCIs which identify a channel multiplexed by cells are allocated, and are differentiated in each cell. Thus, it is impossible to collect a communication content of a specific call, even when specific VPIs and VCIs are extracted. Accordingly, the method enables prevention of intercept. Furthermore, since only VPIs and VCIs are converted in this method, header processing does not become complicated and a circuit configuration becomes simple. Accordingly, the present method enables prevention of intercept without losing high speed performance of ATM.

<2>

[Explanations of Letters or Numerals]

1, cell; 2, header; 3, information field; 4, virtual path identifier (VPI) field; 5, virtual channel identifier (VCI) field; 6, information field; 7 and 8, nodes; 9, transmission line; 10, eavesdropping device; 11, input transmission line; 12 and 13, output transmission lines; 14 and 15, output buffers; 16 and 17, highways; 21, header processing circuit; 22 and 23, memory control circuits; 24 and 25, memories; 26, central processing device; 27, random selection circuit; 31 and 32, words; 41, 42, 43, 44, and 45, fields; 51, 52, 53, 54, 55, 56, 57, and 58, control lines.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平4－363941

(43)公開日　平成４年(1992)12月16日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　12/48					
9/00					
9/10					
		8529－5K	Ｈ０４Ｌ　11／20	Ｚ	
		7117－5K	9／00	Ｚ	

審査請求　未請求　請求項の数１(全　5　頁)　最終頁に続く

(21)出願番号　特願平3－44062

(22)出願日　平成３年(1991)２月18日

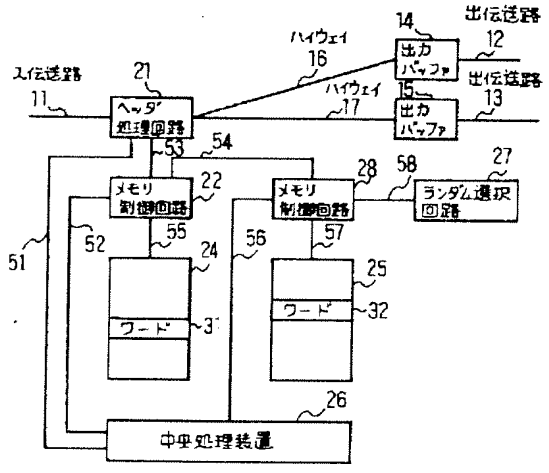
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　中島　誠一
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(72)発明者　原田　要之助
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　並木　昭夫

(54)【発明の名称】　非同期転送モード通信における盗聴防止方法

(57)【要約】

【目的】　ＡＴＭ（非同期転送モード）通信の高速性を損なわずに盗聴防止を可能にする。

【構成】　１つの呼のチャネル（セル多重化されたチャネル）に対して該チャネルを識別する複数のＶＰＩ、ＶＣＩを割り当て、割り当てられた複数のＶＰＩ、ＶＣＩの中から任意の一つをランダム選択回路２７によりランダムに選択、使用してセルを転送するようにする。



Petitioner Apple Inc. - Exhibit 1026, p. 747

1

【特許請求の範囲】

【請求項1】　非同期転送モード通信において、1つの呼のチャネルに対して複数の仮想パス識別の割り当て、或いは複数の仮想回線識別の割り当て、の少なくとも一方を実施し、該呼の情報を転送するに際し、セル単位に割り当てられた複数の仮想パス識別の中の任意の一つのランダム使用、或いはセル単位に割り当てられた複数の仮想回線識別の中の任意の一つのランダム使用、の少なくとも一方を実施してセルを転送することを特徴とする非同期転送モード通信における盗聴防止方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、非同期転送モード通信において、セル多重化された回線での情報の盗聴防止方法に関するものである。

【0002】

【従来の技術】高度情報化社会において情報の盗聴防止が重要であることは述べるまでもない。本発明は、かかる意味での非同期転送モード通信における盗聴防止方法に関するものであるが、先ず非同期転送モード通信についての簡単な説明から始める。さて、時分割多重方式には、時間軸上の位置の識別によって多重する方式とラベルの識別によって多重する方式とがある。従来、ラベル多重方式として情報フィールドの長さを可変として多重するパケット方式があるが、最近、固定長のパケット（セル）を用いて多重する方式（被同期転送モード Asynchronous Transfer Mode 以降ＡＴＭと略記する）が提案されている。ＡＴＭでは、情報転送の要求時のみセルが送出されるので、その頻度に応じて間欠的／連続的通信が可能になり、低速から高速までの任意の転送速度に対応することができ、かつ、情報がない場合には空きセルが挿入されるため、決まったタイミングでセルが出現し、セルの先頭の識別と交換とを高速に行うことができる特徴があり、今後の広帯域ＩＳＤＮの転送モードとして有望な方式である。なお、ＡＴＭについて記載した文献としては、川原崎他，「ＡＴＭ通信技術の動向－－高速広帯域系への展開に向けて－－」、電子情報通信学会誌，71,8，pp.809-814（昭63-08）を挙げることができる。

【0003】図3は国際標準のＡＴＭセル構造を示す説明図である。同図において、1はセル、2はヘッダ、3は情報フィールド、4は仮想パス識別（ＶＰＩ）フィールド、5は仮想回線識別（ＶＣＩ）フィールド、6はその他の制御情報フィールドであり、セル1は53バイト、ヘッダ2は5バイト、情報フィールド3は48バイト、ＶＰＩフィールド4は網内では12ビット、ユーザ・網間では8ビット、ＶＣＩフィールド5は16ビットで構成される。ヘッダ2には多重、セル交換、トラヒック制御等に必要な制御情報が含まれている。

【0004】ノードにおいて、通常、ハードウェアによ

2

りヘッダ2が分析されて多重、セル交換、トラヒック制御が高速に行われる。多重化された伝送路上の1つの特定のチャネルは（ＶＰＩ＋ＶＣＩ）で識別され、交換ノードでＶＰＩ，ＶＣＩは新たな値に付け替えられる。図4はノード間における盗聴の例を示すブロック図で、7，8はノード、9は伝送路、10は盗聴機であり、伝送路9にはセル1が転送される。特定のチャネルを盗聴するには、盗聴機10で特定のＶＰＩ，ＶＣＩのセルを選択すればよく、容易に盗聴される恐れがある。盗聴を防止する方法には、従来の技術としてはセル1に暗号をかける方式が考えられる。

【0005】しかし、ＡＴＭでは伝送速度として数Ｇｂｉｔ／ｓ以上の速度までを想定しているため、交換ノードでセルを復号化し、ヘッダ2を分析することは実現不可能である。また、ＶＰＩ，ＶＣＩのみを暗号化しても、暗号化されたＶＰＩ，ＶＣＩは、交換機における交換時の行先を示す情報であり、常に通信中同じ値をとるので、その値でセルを抽出すれば容易に盗聴されることになる。

【0006】

【発明が解決しようとする課題】本発明は、上記事情に鑑みてなされたもので、その目的とするところはＡＴＭの高速性を損なわずに盗聴を防止することのできる非同期転送モード通信における盗聴防止方法を提供することにある。

【0007】

【課題を解決するための手段】本発明は、上記の課題を解決するため、1つの呼のチャネルに対して複数のＶＰＩ，ＶＣＩを割り当て、割り当てられたＶＰＩ，ＶＣＩの中から任意の一つをランダムに使用してセルを転送するようにしたものである。

【0008】

【作用】本発明は、1つの呼のチャネルに対して複数のＶＰＩ，ＶＣＩを割り当て、割り当てられた複数のＶＰＩ，ＶＣＩの中から任意の一つをランダムに使用してセルを転送することを最も特徴とするものである。したがって、送信ノードと受信ノードと間の伝送路において、同一の呼のチャネルに関するＶＰＩ，ＶＣＩはセル単位で常に変化するため、特定のＶＰＩ，ＶＣＩのセルを抽出しても特定の呼の通信内容を収集することは不可能になる。また、伝送路上のすべてのセルを収集したとしても、特定の呼のセルを抽出することは困難であり、盗聴の防止が可能になる。本発明では、ＶＰＩ，ＶＣＩのみをセル単位で変更するため、送信ノード、受信ノードのヘッダ2の処理は容易であり、ＡＴＭの高速性を損なうことなく盗聴の防止が可能となる。

【0009】

【実施例】本発明の実施例を図面に基づいて詳細に説明する。説明を簡単にするため、ＶＣＩにのみ本発明を適用した場合を例にとって説明する。図1は本発明の盗聴

Petitioner Apple Inc. - Exhibit 1026, p. 748

3

防止方法を実現する交換ノードの実施例であって、11は入り伝送路、12，13は出伝送路、14，15は出力バッファ、16，17は交換ノード内のハイウェイ、21はヘッダ処理回路、22，23はメモリ制御回路、24，25はメモリ、26は中央処理装置、27はランダム選択回路、31，32はメモリ24，25のワード、41，42，43，44，45はワード32のフィールド、51，52，53，54，55，56，57，58は制御線である。

【0010】メモリ24は、入り伝送路11から到着するセルの「入りVCI」と「変換VCI」との対応をとるメモリであり、入りVCIをアドレスとして変換VCIを得ることができる。メモリ25は「変換VCI」と、「出VCI」との対応をとるメモリであり、変換VCIをアドレスとして出VCIを得ることができる。入り伝送路11からセルが到着すると、ヘッダ処理回路21は入りVCIを制御線53を介してメモリ制御回路22に入力する。

【0011】メモリ制御回路22は、制御線55を介して入りVCIをアドレスとして入力し、メモリ24のワード31から変換VCIを読み出し、変換VCIを制御線54を介してメモリ制御回路23に入力する。メモリ制御回路23は、制御線57を介して変換VCIをアドレスとしてメモリ25に入力し、出VCI（複数）をワード32から読み出し、制御線58を介してランダム選択回路27により、複数の出VCIの中から1つの出VCIを決定し、制御線54、メモリ制御回路22、制御線53を介してヘッダ処理回路21に出VCIを返送し、ヘッダ処理回路21は、該セルの入りVCIをその出VCIに置き換えて、例えばハイウェイ17を介して出力バッファ15に入力する。該セルは出力バッファ15から出伝送路13に送出される。

【0012】1つの呼に関するセルのVCIは複数割り当てられるが、この割り当ては呼の設定時に送信側の交換ノードから呼設定制御セルを用いて、例えば、入りVCIとして#3，#38，#74を使用することを通知してくる。ヘッダ処理回路21がヘッダを分析して呼設定制御セルを検出すると制御線51を介して中央処理装置26に該セルを転送する。中央処理装置26は、出方路の選択制御等に加えて、変換VCI、出VCIを決定する。まず、空きの変換VCIを決定すると、変換VCIをメモリ24の入りVCIに対応するアドレスに書くため、送信側交換ノードから指定された複数のVCIと中央処理装置26が決定した変換VCIを制御線52を介してメモリ制御回路22に転送する。

【0013】メモリ制御回路22は、その指示に従って変換VCIを指定のアドレスに書き込む。例えば、変換VCIを#21とすれば、上記の例ではメモリ24のアドレス#3，#38，#74に変換VCIの#21が書かれる。したがって、該呼のセルの入りVCIが#3，

4

#38，#74の何れかであれば、変換VCIは#21に変換されることになる。中央処理装置26は同時に、空いた複数の出VCI（例えば#55，#89，#93）を決定し、制御線56を介してメモリ25の変換VCIに対応するアドレスに、複数の出VCIを書き込むため、変換VCIと出VCIをメモリ制御回路23に転送する。

【0014】メモリ制御回路23は、変換VCIに対応するアドレスに出VCI（この例では#55，#89，#93）を書き込む。具体的には、図2に示すワード32のフィールド41～45に、1つのフィールドに1つの出VCIを、例えば#55とか、#89のように、書き込む。この例では3つの出VCIを使用しているため、フィールド41，42，43に#55，#89，#93が各々書き込まれる。メモリ制御回路23は、ワード32を読み出すと、制御線58を介してランダム選択回路27に複数の出VCIを入力し、ランダム選択回路27は乱数を発生して複数の出VCIから1つの出VCIを選択し、制御線58、メモリ制御回路23、制御線54、メモリ制御回路22、制御線53を介してヘッダ処理回路21に該出VCIを返送する。

【0015】このため、ワード32を読み出す毎に、上記の例では出VCIは#55，#89，#93の中の一つがランダムに選択されることになる。従って、入り伝送路11から該呼のセルが到着すると、入りVCIは（#3，#38，#74のいずれかでセル単位に変わる）変換VCIの#21に一旦変換され、出VCIは#55，#89，#93ののいずれかに変換されることになる。このため、入り伝送路11、出伝送路13に流れる該呼チャネルのVCIは固定されず常に変化しており、盗聴を防止することができる。

【0016】上記説明では、割り当て入りVCI、出VCIの数は数個であったが、VCIは16ビットの容量があるため、割り付けるVCIの数を数百以上にすることも特に大きな制約にはならない。上記例では、入りVCI、出VCIの割り当ては呼設定時に行われるため、通信中は割り当てられた複数のVCIは固定されるが、通信中にこれを変更することも可能である。これは、通信中に送信ノードで新たなVCIを決定し、受信ノードでは中央処理装置26からメモリ24、25の内容を書き換えれば良く、この場合にはVCIのランダム性が増加するため、盗聴に対する耐力を高めることが可能となる。

【0017】上記説明では、VCIの複数割り当てを呼設定時に行った例であるが、あらかじめ、ノード間でVCIの割り当てグループを定めておき、その呼設定時にはそのグループ内の1つのVCIを相手ノードに通知する方法をとってもよい。上記説明では、VCIをセル単位で変更する例であったが、さらにVPIをもセル単位に変更する場合、あるいはVPIのみを変更する場合に

Petitioner Apple Inc. - Exhibit 1026, p. 749

5

も図１と同様な構成で実現できることは明らかである。

【００１８】上記実施例に加えて、入り伝送路１、出伝送路１３等に流れる情報に従来行われているスクランブラを掛ければ、さらに盗聴に対する耐力を高めることが可能となる。また、送信ノードから割り当てたＶＰＩ、ＶＣＩを通知する情報に対して暗号をかければ、さらに盗聴にたいする耐力を高めることが可能となる。上記説明では、特殊な呼が非常に少ない場合には複数のＶＣＩを用いても盗聴の可能性が高いが、ダミーのチャネルを設定したり、空きセルに複数のＶＣＩを割り当てる等により対処すればよい。

<1>

【００１９】

【発明の効果】以上説明したように、本発明のＡＴＭ通信における盗聴防止方法によれば、セル多重化されたチャネルを識別するＶＰＩ、ＶＣＩを複数割り当て、ＶＰＩ，ＶＣＩをセル単位に変更するため、伝送路上で特定ＶＰＩ，ＶＣＩを抽出しても特定呼の通信情報を得ることが不可能であり、盗聴の防止をすることが可能となる。また、本方法ではＶＰＩ、ＶＣＩのみを変更するため、ヘッダの処理が複雑にならず簡単な回路構成とすることができ、ＡＴＭの高速性を損なうことなく盗聴防止

6

が実現できる。

【図面の簡単な説明】

【図１】本発明の一実施例を示すブロック図である。

【図２】図１におけるワード３２の構成例を示す説明図である。

【図３】ＡＴＭセル構造を示す説明図である。

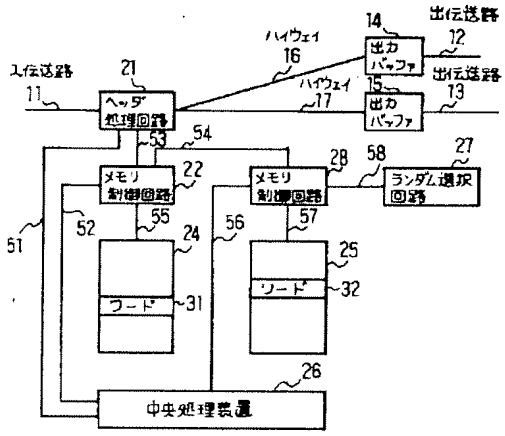
【図４】ノード間における盗聴の例を示すブロック図である。

<2>

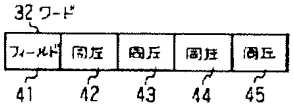
【符号の説明】

１…セル、２…ヘッダ、３…情報フィールド、４…仮想パス識別（ＶＰＩ）フィールド、５…仮想回線識別（ＶＣＩ）フィールド、６…情報フィールド、７，８…ノード、９…伝送路、１０…盗聴機、１１…入り伝送路、１２，１３…出伝送路、１４，１５…出力バッファ、１６，１７…ハイウェイ、２１…ヘッダ処理回路、２２，２３…メモリ制御回路、２４，２５…メモリ、２６…中央処理装置、２７…ランダム選択回路、３１，３２…ワード、４１，４２，４３，４４，４５…フィールド、５１，５２，５３，５４，５５，５６，５７，５８…制御線

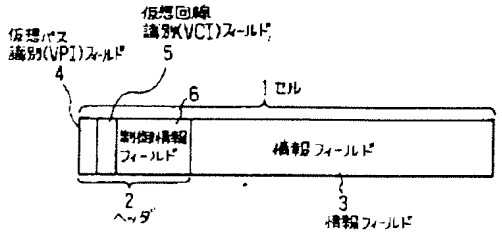
【図１】



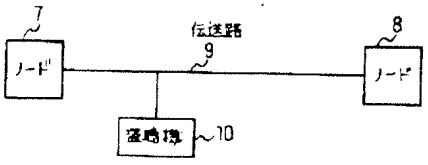
【図２】



【図３】



【図４】



Petitioner Apple Inc. - Exhibit 1026, p. 750

【手続補正書】
【提出日】平成４年６月１８日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　非同期転送モード通信において、１つの呼のチャネルに対して複数の仮想パス識別の割り当て、或いは複数の仮想回線識別の割り当て、の少なくとも一方を実施し、該呼の情報を転送するに際し、セル単位に割り当てられた複数の仮想パス識別の中の任意の一つのランダム使用、或いはセル単位に割り当てられた複数の仮想回線識別の中の任意の一つのランダム使用、の少なくとも一方を実施してセルを転送することを特徴とする非同期転送モード通信における盗聴防止方法。

フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/12				

Petitioner Apple Inc. - Exhibit 1026, p. 751

Cited Document 5
translated by Computer

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-018492**

(43)Date of publication of application : **17.01.1997**

(51)Int.Cl. **H04L 12/28**
H04L 12/02
H04Q 3/00

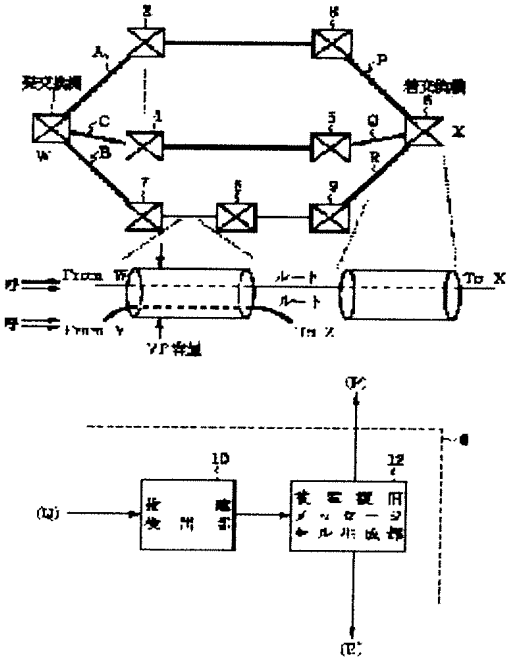
(21)Application number : **07-166048**

(22)Date of filing : **30.06.1995**

(71)Applicant : **NIPPON TELEGR & TELEPH CORP <NTT>**

(72)Inventor : **OKI EIJI**
YAMANAKA NAOAKI

(54) ATM COMMUNICATION NETWORK AND FAILURE RESTORATION METHOD



(57)Abstract:

PURPOSE: To reduce the cost of an exchange and further to enforce a fault restoration without providing a device concentratedly restoring a fault by omitting a redundant hardware constitution for securing the high reliability of an exchange.

CONSTITUTION: An incoming exchange 6 is provided with a fault restoration message generation part 12 as a means transmitting a fault restoration message to a virtual pass. A fault restoration message cell has a destination area and a message area. On the destination area, information for reaching a transmitting exchange 1 is mounted via one or more repeating exchanges 2 to 5 and 7 to 9. The repeating exchanges 2 to 5 and 7 to 9 are

provided with a fault restoration message cell information mounting parts 14 mounting null band information on the repeating exchanges 2 to 5 and 7 to 9 in the message area of the routing fault restoration message cell. By this constitution, constitution, the cost of the exchange is reduced and further, the restoration is made possible without providing a device concentrately performing a fault restoration.

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]An ATM communication network comprising:

Two or more subscriber exchange.

Two or more physical transmission lines which connect between [this] two or more subscriber exchange.

In an ATM communication network which is provided with a transit exchange inserted in two or more of these physical transmission lines and with which a virtual path is set up among said two or more subscriber exchange, to said subscriber exchange. Have a means to send out a fault restoration message cell to a virtual path, and this fault restoration message cell, A means to have a destination area and a message area, and for information for arriving at the destination area via one or more transit exchanges at subscriber exchange of the other party to be carried, and to make empty band region information on the transit exchange carry in a message area of said fault restoration message cell via which it goes in said transit exchange.

[Claim 2]The ATM communication network according to claim 1 provided with a means to add the number of transit exchanges carried in this hop counter field whenever a hop counter field which carries the number of transit exchanges via which it goes in said message area was provided and a fault restoration message cell passed to said transit exchange.

[Claim 3]The ATM communication network according to claim 1 or 2 with which a means to equip said subscriber exchange with a means to recognize the possibility of failure of a transit exchange inserted in a virtual path, and to send out said fault restoration message cell sends out a fault restoration message cell according to an output of this means to recognize.

[Claim 4]Said subscriber exchange is equipped with a means to receive a fault restoration message cell which comes via two or more virtual paths, The ATM communication network according to any one of claims 1 to 3 provided with a means to choose a virtual path used according to the number of empty band region information included in this fault restoration message cell, and transit exchanges.

[Claim 5]a virtual path set as subscriber exchange -- present -- a virtual path of business and

a spare virtual path, and two or more virtual paths that can become being set up beforehand, and, this -- present, when the possibility of failure to a transit exchange inserted in a virtual path of business has been recognized, Said subscriber exchange sends out a fault restoration message cell to a virtual path of said reserve, and two or more virtual paths which can become, respectively, A fault restoration method choosing two or more either virtual path of said reserve or virtual paths which can become according to the number of empty band region information and transit exchanges which were carried in this fault restoration message cell in subscriber exchange used as an address of this fault restoration message cell.
[Claim 6]A way a large number distribute, said subscriber exchange exists in one communications network, and each subscriber exchange performs a fault restoration method according to claim 5 on an autonomous distribution target.
[Claim 7]a virtual path set as subscriber exchange -- present -- a virtual path of business and a spare virtual path, and two or more virtual paths that can become being set up beforehand, and, this -- present, even if there is no failure of a transit exchange inserted in a virtual path of business, Said subscriber exchange sends out a fault restoration message cell to a virtual path of said reserve, and two or more virtual paths which can become, respectively, In subscriber exchange used as an address of this fault restoration message cell. A standby method of fault restoration choosing beforehand two or more either virtual path of said reserve or virtual paths which can become as a spare virtual path candidate according to the number of empty band region information and transit exchanges which were carried in this fault restoration message cell.
[Claim 8]A way a large number distribute, said subscriber exchange exists in one communications network, and each subscriber exchange performs a standby method of the fault restoration according to claim 7 on an autonomous distribution target.
[Claim 9]A fault restoration method, wherein it addresses subscriber exchange in one communications network to other subscriber exchange belonging to self which sets a virtual path as self, and/or its communications network and it sends out a fault restoration message cell to a virtual path, respectively.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application]This invention is used for an ATM (Asynchronous Transfer Mode) communications network. It is related with the fault restoration art over failure of the communication apparatus especially inserted in the transmission line.
[0002]
[Description of the Prior Art]The virtual channel hair drier (Virtual Channel Handler,

switchboard) which switches by an ATM communication network making a unit physically a virtual channel (Virtual Channel: it is called following VC), It is connected by the transmission line and the virtual path hair drier (Virtual Path Handler:VPH or cross connect, XC) which sets up the route of information transfer by making a virtual path (Virtual Path: henceforth VP) into a unit is constituted. Theoretically, between VCH is connected by VP and the termination of VP is carried out by VCH via zero or one or more VPH(s).

[0003]The fault restoration method for failure of the conventional communication apparatus is shown in drawing 12. Drawing 12 is a figure showing the concept of the conventional fault restoration method. There is fault restoration of VP level shown in the fault restoration and drawing 12 (a) of the physical level shown in drawing 12 (b) in the conventional fault restoration method. making the physical transmission-line link double, in order to realize fault restoration of a physical level -- one side -- present -- business -- a system and another side are made into the reserve system. if -- present -- business -- if failure occurs in the communication apparatus of a system -- present -- business -- it changes from a system to a reserve system, and failure is restored. However, in the fault restoration of a physical level, a physical transmission-line link must be made double and there is always a problem that a network resource cannot be used efficiently.

[0004]Then, there is the fault restoration method of VP level which applied the concept of VP which is the feature of an ATM communication network. VP is identified by VPI (Virtual Path Identifier) in the header area given to the cell which is a functional information unit, and a course is set up in VPH by the pass connection (routing) table which described the connection destination of the path. Fault restoration of VP level is realized by switching VP cut by failure to VP which bypassed the locating fault and was newly formed using the ability of the course and capacity of VP to set up independently. It is based on the detour path information to which the central post office which is supervising the ATM communication network unitary was especially set beforehand at the time of a failure occurrence, and is each node () within the net. [VCH and] The fault restoration method with which a centralized control system and each node make an autonomous distribution target look for and restore a detour path for the method which controls to VPH and others is called self healing method. As compared with the fault restoration of a physical level, it excels in the fault restoration of VP level with the point that the network resource of a transmission line can be used efficiently, or the point that it can respond to change of a net flexibly. Therefore, the fault restoration method which combined the physical level and VP level is applied as the conventional fault restoration method.

[0005]

[Problem(s) to be Solved by the Invention]However, in the fault restoration method of only the conventional physical level and VP level, sake [premised], a high reliability switchboard is required for failure of VCH (switchboard). In the ATM communication

network with which two or more media are intermingled, although the reliability demanded for every media differed, the switchboard was designed satisfy reliability according to the reliability demanded most highly, and it was redundant not much to the media which do not require reliability. Although drawing 13 is a key map of the high-reliability-ized switchboard, in the high-reliability-ized switchboard, the switch part, the I/O part, and the CPU section have doubled like drawing 13, and these units are further combined by the crossing route. The cost of the high-reliability-ized switchboard will become high about 6 times from 4 times compared with the cost of a switchboard with simple composition by such double-ization.

[0006]This invention is carried out to such a background and is a thing.

It is providing the ATM communication network and the fault restoration method of performing the measure against fault restoration on condition of the purpose.

An object of this invention is to provide the ATM communication network and the fault restoration method the redundant hardware constitutions for securing the high-reliability of a switchboard are omissible. An object of this invention is to provide the ATM communication network and the fault restoration method of reducing the cost of a switchboard. An object of this invention is to provide the ATM communication network and the fault restoration method of performing fault restoration, without forming the device which performs fault restoration intensively.

[0007]

[Means for Solving the Problem]When applying a switchboard with simple composition as a communication apparatus, it is necessary to restore quickly VC route obstacle at the time of failure of a switchboard. Then, this invention provides a method of restoring VC route obstacle quickly at the time of failure of a switchboard. As the method, at the time of failure of a switchboard, in order to restore a working route obstacle between arrival-and-departure switchboards, a fault restoration message cell is sent out from an incoming exchange, A switchboard exchanges information with an autonomous distribution target, and notifies reticulated voice to ********, a route is changed, and a route obstacle by switchboard failure is restored by VC route level. This is called self healing of VC route level.

[0008]In conventional technology, although self healing of VP level was performed, there is a place by which it is characterized [of this invention] in the ability to restore VC route obstacle at the time of switchboard failure by self healing of VC route level.

[0009]That is, the first viewpoint of this invention is an ATM communication network which is provided with two or more physical transmission lines which connect between [this] two or more subscriber exchange with two or more subscriber exchange, and a transit exchange inserted in two or more of these physical transmission lines and with which a virtual path is set up among said two or more subscriber exchange.

[0010]Here a place by which it is characterized [of this invention] to said subscriber

exchange. Have a means to send out a fault restoration message cell to a virtual path, and this fault restoration message cell, Have a destination area and a message area, it is carried by information for arriving at the destination area via one or more transit exchanges at subscriber exchange of the other party, and to said transit exchange. It is in a place provided with a means to make empty band region information on the transit exchange carry in a message area of said fault restoration message cell via which it goes.

[0011]Whenever a hop counter field which carries the number of transit exchanges via which it goes in said message area is provided and a fault restoration message cell passes to said transit exchange, it is desirable to have a means to add the number of transit exchanges carried in this hop counter field.

[0012]As for a means to equip said subscriber exchange with a means to recognize the possibility of failure of a transit exchange inserted in a virtual path, and to send out said fault restoration message cell, it is desirable to send out a fault restoration message cell according to an output of this means to recognize.

[0013]It is desirable to equip said subscriber exchange with a means to receive a fault restoration message cell which comes via two or more virtual paths, and to have a means to choose a virtual path used according to the number of empty band region information included in this fault restoration message cell and transit exchanges.

[0014]A place by which the second viewpoint of this invention is the fault restoration method, and it is characterized [the], a virtual path set as subscriber exchange -- present -- a virtual path of business and a spare virtual path, and two or more virtual paths that can become being set up beforehand, and, this -- present, when the possibility of failure to a transit exchange inserted in a virtual path of business has been recognized, Said subscriber exchange sends out a fault restoration message cell to a virtual path of said reserve, and two or more virtual paths which can become, respectively, In subscriber exchange used as an address of this fault restoration message cell, it is in a place which chooses two or more either virtual path of said reserve or virtual paths which can become according to the number of empty band region information and transit exchanges which were carried in this fault restoration message cell.

[0015]It is the feature that a large number distribute, said subscriber exchange exists in one communications network in this fault restoration method, and each subscriber exchange performs this fault restoration method on an autonomous distribution target.

[0016]A place by which the third viewpoint of this invention is a fault restoration standby method, and it is characterized [the], a virtual path set as subscriber exchange -- present -- a virtual path of business and a spare virtual path, and two or more virtual paths that can become being set up beforehand, and, this -- present, even if there is no failure of a transit exchange inserted in a virtual path of business, Said subscriber exchange sends out a fault restoration message cell to a virtual path of said reserve, and two or more virtual paths which

can become, respectively, In subscriber exchange used as an address of this fault restoration message cell. It is in a place which chooses beforehand two or more either virtual path of said reserve or virtual paths which can become as a spare virtual path candidate according to the number of empty band region information and transit exchanges which were carried in this fault restoration message cell.

[0017]It is the feature that a large number distribute, said subscriber exchange exists in one communications network in this fault restoration standby method, and each subscriber exchange performs this fault restoration standby method on an autonomous distribution target.

[0018]A place by which the fourth viewpoint of this invention is the fault restoration method, and it is characterized [the], Subscriber exchange in one communications network is in a place which addresses to other subscriber exchange belonging to self which sets a virtual path as self, and/or its communications network, and sends out a fault restoration message cell to a virtual path, respectively.

[0019]Although that expression [like] which is a communication apparatus which is different in subscriber exchange and a transit exchange is used in this specification, this is for explaining plainly and a communication apparatus of the same hardware constitutions can realize it.

[0020]

[Function]In the method of this invention, by self healing of VC route level. Since a fault restoration message cell is sent out from an incoming exchange, a switchboard can exchange information with an autonomous distribution target, and can notify reticulated voice to ********, a route can be changed and VC route obstacle at the time of switchboard failure can be restored, The necessity which uses a high reliability switchboard is lost and cost reduction is planned by using a switchboard with simple composition.

[0021]The fault restoration message cell which an incoming exchange sends out reaches ******** via a virtual path. The virtual path beforehand defined as a virtual path which can turn into a spare virtual path may be sufficient as this virtual path, and the unspecified virtual path in which failure is not recognized may be sufficient as it.

[0022]A fault restoration message cell collects the empty band region information on the virtual path passed while reaching ******** from an incoming exchange. If a way of speaking is changed, the transit exchange inserted in the virtual path to pass carries the empty band region information in a self transit exchange in the message area of a fault restoration message cell, when passing a fault restoration message cell. The number of the transit exchanges passed simultaneously also carries as information. In ********, empty band region information and a number of a transit exchange of passed information are referred to, and the virtual path optimal as a spare virtual path is chosen. Henceforth, a virtual channel is set as this virtual path, and communication is resumed.

[0023]sending out of a fault restoration message cell -- present -- the virtual path of business -- or -- present -- it may control to be carried out when a certain failure has been recognized by the transit exchange on the virtual path of business -- by carrying out. Or it is also good to send out a fault restoration message cell also at the time of usual, and to always choose the virtual path candidate optimal as a spare virtual path.
[0024]In this invention, it is characterized [main] by each switchboard contained in an ATM communication network carrying out such fault restoration control to autonomous distribution.
[0025]
[Example]
(The first example) The composition of the first example of this invention is explained with reference to drawing 1 - drawing 5. Drawing 1 is an entire configuration figure of this invention. Drawing 2 is an important section block lineblock diagram of an incoming exchange. Drawing 3 is a lineblock diagram of a fault restoration message cell. Drawing 4 is an important section block lineblock diagram of a transit exchange. Drawing 5 is an important section block lineblock diagram of ********.
[0026]******** 1 and the incoming exchange 6 whose this invention is subscriber exchange, and physical transmission-line P-R which connects this ******** 1 and between incoming-exchange 6, It is an ATM communication network which is provided with the transit exchanges 2, 3, 4, 5, 7, 8, and 9 inserted in this physical transmission-line P-R and with which a virtual path is set up between ******** 1 and the incoming exchange 6.
[0027]Here the place by which it is characterized [of this invention] to the incoming exchange 6. Have the fault restoration message cell generation part 12 as a means to send out a fault restoration message cell to a virtual path, and this fault restoration message cell, Have the destination area H and message area M, and the information for arriving at the destination area H at ******** 1 via the one or more transit exchanges 2, 3, 4, 5, 7, 8, and 9 is carried, It is in the place which equipped the transit exchanges 2, 3, 4, 5, 7, 8, and 9 with the fault restoration message cell information mount part 14 as a means which makes the empty band region information on the transit exchanges 2, 3, 4, 5, 7, 8, and 9 carry in message area M of the fault restoration message cell via which it goes.
[0028]In this invention example, in order to explain plainly, express as if it was the communication apparatus provided with hardware constitutions which are different, respectively in ******** 1, the incoming exchange 6, and the transit exchanges 2, 3, 4, 5, 7, 8, and 9, but. These are realizable as one communication apparatus provided with each function in common.
[0029]It is provided by hop counter field HC which carries the number of the transit exchanges 2, 3, 4, 5, 7, 8, and 9 via which it goes in message area M, and to the transit exchanges 2, 3, 4, 5, 7, 8, and 9. Whenever a fault restoration message cell passes, a means

to add the number of the transit exchanges carried in this hop counter field HC was combined with the fault restoration message cell information mount part 14, and it has it.
[0030]******** 1 and the incoming exchange 6 are equipped with the failure detection part 10 as the transit exchanges 2, 3, 4, 5, 7, and 8 inserted in the virtual path, and a means to recognize the possibility of failure of nine, The fault restoration message cell generation part 12 sends out a fault restoration message cell according to the output of this failure detection part 10.
[0031]******** 1 is equipped with the spare-routes set part 16 as a means which receives the fault restoration message cell which comes via two or more virtual paths, A means to choose the virtual path used according to the number of the empty band region information included in this fault restoration message cell and transit exchanges was combined with the spare-routes set part 16, and it has it.
[0032]VC route is set as the incoming exchange 6 through one or more VP from ******** 1. In ******** 1, when a call occurs, a certain route is chosen from two or more VC routes, and a call admission judging (Connection Admission Control:CAC) is performed. For example, selection of a route is chosen at random. It becomes call loss, if a call is received by CAC, VC connection will be set up and a call will not be received by it.
[0033]Next, operation of the first example of this invention is explained with reference to drawing 6. Drawing 6 is a figure for explaining operation of the first example of this invention. As shown in drawing 6, only paying attention to one working route, the failure recovery method of the first example of this invention when failure occurs is shown in the transit exchange 5. The working route (1->4->5->6) is set up via two transit exchanges between ******** 1 and the incoming exchange 6, a working route is this time, and it is B. The zone of [Mbps] is used.
[0034]To this working route, a call is received after CAC, and VC connection is set up or it is cut. The usage band of this working route is called for, for example in ******** 1 by observing the number of cells currently used by the working route in a certain window size. There are a jumping window and a sliding window as a window used for observation.
[0035]Here, a jumping window is the observation method which changes without a window position (observation post) overlapping with a constant period, and a sliding window is the observation method which changes gradually, while a window position overlaps with a constant period. When it says very roughly, observation with a high-speed jumping window is an advantage, and observation with an exact sliding window is an advantage.
[0036]In drawing 6 which prepares for a working route becoming unusable and sets up two or more spare routes beforehand by failure, two spare routes (the route P:1->2->3->6, the route R:1->7->8->9->6) are set up. When failure occurs, the switchboard 1 from a twist and the incoming exchange 6 recognize that a working route is in an unusable state to the cell which notifies alarm, and others. the call of VC newly demanded after a failure occurrence

although relief of VC connection set as the working route at present is not performed -- the maximum reception ******** -- an alternative route is searched like. Here, the sender and ******** 1 to which the incoming exchange 6 sends out a fault restoration message cell serve as Chooser which receives a fault restoration message cell, changes it out of spare routes, and chooses a route. The incoming exchange (sender) 6 sends out a fault restoration message cell, in order to investigate the state to spare routes. A fault restoration message cell investigates the state of VP on the course of the spare routes P and R in accordance with the course of the spare routes P and R. The route R is raised to an example and explained. Minimum b_{min}(4) channel-information RD of a (1) hop counter HC(2) hop limit HL(3) VP intact zone is written in message area [of a fault restoration message cell] M as a pay load. The hop limit HL is beforehand set up in consideration of delay conditions and others. The value of minimum b_{min} is made into infinity and the value of minimum b_{min} is written in the fault restoration message cell. The fault restoration message cell which goes via the route R is sent out to the transit exchange 9 from the incoming exchange 6, and in the transit exchange 9, if it $b<B_{min}$ Becomes, it will make the value of the intact VP zone b b_{min}. In the transit exchange 9, b is called for, when VP intact zone in a certain window size observes the number of use cells. There are a jumping window and a sliding window as a window used for observation. Hop counter HC is further sent out to the following switchboard, unless it counts up one and the hop limit HL is exceeded, whenever it goes via the transit exchange 9->8->7. However, spare routes are usually set up beforehand not exceed a hop limit. In the following switchboard 8, it is b= 2, and since it is $b<B_{min}$, it is set to b_{min}=2. Repeating the process of fault restoration message cell sending out similarly, a fault restoration message cell reaches ******** 1. The fault restoration message cell A sent out on spare-routes P reaches ******** 1 similarly. One or more ******** 1 are chosen as a route of a switch destination from the spare routes P or R in consideration of the usage band B, and the spare-routes information (minimum b_{min} of VP intact zone, hop number) and others of a working route. In the example of drawing 7, although drawing 7 is a figure showing the route change situation in the first example of this invention, since the minimum of VP intact zone is [the route P] the largest in spare routes, the route P is chosen as a route of a switch destination, and the route P is used as a working route after fault restoration.

[0037]Therefore, since a switchboard exchanges information with an autonomous distribution target by sending out of a fault restoration message cell, a route is changed at the time of failure of a switchboard and failure is restored, Even if it is not a high reliability switchboard like before made double, using a switchboard with simple composition, or since it can do, the cost reduction of a switchboard can be planned.

[0038]The (second example), next the second example of this invention are described with reference to drawing 8. Drawing 8 is a figure for explaining operation of the second example of this invention. Although the fault restoration message cell was sent out in the first

example of this invention at the time of a failure occurrence, At the second example of this invention, it is usually the incoming exchange (sender) 6 to RM (Resource Management) also by the time like drawing 8. A cell is sent out and the state of the spare routes P and R is supervised. Operation of an RM cell is the same as operation of the fault restoration message cell of the first example of this invention. Out of the spare routes P or R, in consideration of the usage band B, and the spare-routes information (minimum b_{min} of VP intact zone, hop number) and others of a working route, it has ******** (Chooser) 1 at the time of the obstacle of a working route, and it determines the route of the switch destination.

[0039]Here, an RM cell is periodically sent out from the incoming exchange (sender) 6, and ******** (Chooser) 1 which received the RM cell updates the route of the switch destination according to reticulated voice. The sending-out interval of an RM cell is determined from the degree of change of reticulated voice.

[0040]When failure occurs, the switchboard 1 from a twist recognizes that a working route is in an unusable state to the cell which notifies alarm, and others. The switchboard 1 from ******** is changed to the switch destination route with which it equipped usual at the time of a working route obstacle, and the obstacle of a working route is used as a working route.

[0041]Therefore, shortening of fault restoration time can be attained by sometimes sending out RM (Resource Management) cell from the incoming exchange (sender) 6, sometimes supervising the state of spare routes, and usually deciding the switch destination route to be it in preparation for the time of the obstacle of a working route.

[0042]The (third example), next the third example of this invention are described with reference to drawing 9. Drawing 9 is a figure for explaining operation of the third example of this invention. In the first example of this invention, the spare routes P and R were set up beforehand, and the fault restoration message cell was sent out on spare-routes P and R at the time of a failure occurrence. In the third example of this invention, the spare routes P and R are not set up beforehand, but a fault restoration message cell is sent out with flooding (Flooding) like drawing 9, and ******** 1 chooses spare routes according to the fault restoration message cell which reached ******** 1.

[0043]Here, flooding is "Flood, i.e., the term based on the image of sending out a cell to the unspecified direction just like a "flood",", and it uses for the meaning of sending out a fault restoration message cell to all the switchboards which send out VP to a self-switchboard.

[0044]As the first example of this invention explained, minimum b_{min}(4) channel-information RD of a (1) hop counter HC(2) hop limit HL(3) VP intact zone is written in the pay load of a fault restoration message cell. The hop limit HL is beforehand set up in consideration of delay conditions and others. The value of minimum b_{min} is made into infinity and the value of minimum b_{min} is written in the fault restoration message cell.

[0045]First, the incoming exchange (sender) 6 sends out a fault restoration message cell to all the switchboards which send out VP to a self-switchboard. The switchboard which

received the fault restoration message cell will make the value of the intact VP zone b b_{min}, if it $b<B_{min}$ Becomes. In a switchboard, b is called for, when VP intact zone in a certain window size observes the number of use cells. The information on the switchboard via which it went is written in as channel information. Whenever hop counter HC goes via a switchboard, one is counted up, and if it is over the hop limit HL or has already gone via the same switchboard by channel information RD, a fault restoration message cell will be discarded. Otherwise, a fault restoration message cell is further sent out to all the switchboards which send out VP to a self-switchboard, the switchboard which received the fault restoration message cell repeats the same operation, and a fault restoration message reaches ********.

[0046]One or more ******** (Chooser) 1 are chosen from the fault restoration message cell which arrived as a route of a switch destination in consideration of the route information (minimum b_{min} of VP intact zone, hop number) and others based on the usage band B and the fault restoration message cell which arrived of a working route.

[0047]Therefore, fault restoration which was flexibly equivalent to net topology, VP capacity, and other change can be performed by sending out a fault restoration message cell with flooding, and making a fault restoration message cell reach ******** 1, without setting up spare routes beforehand.

[0048]The fault restoration concept by the fault restoration method of this invention is shown in drawing 10 and drawing 11. Drawing 10 is a figure showing the concept of the fault restoration method of this invention. Drawing 11 is a key map of the ATM communication network which applied the fault restoration method of this invention. Drawing 10 (b) and (c) is a fault restoration concept of VP level and a physical level known from the former. An ATM communication network can consist of this inventions, without using a highly reliable switchboard by performing fault restoration of VC route level, as shown in drawing 11 as shown in drawing 10 (a).

[0049]

[Effect of the Invention]As explained above, according to this invention, fault restoration control on condition of failure of a switchboard can be performed. For this reason, the redundant hardware constitutions for securing the high-reliability of a switchboard are omissible. Therefore, the cost of a switchboard can be reduced. Fault restoration can be performed without forming the device which performs fault restoration intensively.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The entire configuration figure of this invention.

[Drawing 2]The important section block lineblock diagram of an incoming exchange.

[Drawing 3]The lineblock diagram of a fault restoration message cell.
[Drawing 4]The important section block lineblock diagram of a transit exchange.
[Drawing 5]The important section block lineblock diagram of ********.
[Drawing 6]The figure for explaining operation of the first example of this invention.
[Drawing 7]The figure showing the route change situation in the first example of this invention.
[Drawing 8]The figure for explaining operation of the second example of this invention.
[Drawing 9]The figure for explaining operation of the third example of this invention.
[Drawing 10]The figure showing the concept of the fault restoration method of this invention.
[Drawing 11]The key map of the ATM communication network which applied the fault restoration method of this invention.
[Drawing 12]The figure showing the concept of the conventional fault restoration method.
[Drawing 13]The key map of the high-reliability-ized switchboard.
[Description of Notations]
1 ********
2-5, 7-9 Transit exchange
6 Incoming exchange
10 Failure detection part
12 Fault restoration message cell generation part
14 Fault restoration message cell information mount part
16 Spare-routes set part
H Destination area
HC Hop counter
HL Hop limit
M Message area
RD Channel information
b_{min} minimum
P, Q, and R Route

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－18492

(43)公開日　平成９年(1997)１月17日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　12/28		9466－5K	Ｈ０４Ｌ　11/20	Ｄ	
12/02			Ｈ０４Ｑ　3/00		
Ｈ０４Ｑ　3/00		9466－5K	Ｈ０４Ｌ　11/02	Ａ	

審査請求　未請求　請求項の数９　ＯＬ　（全９頁）

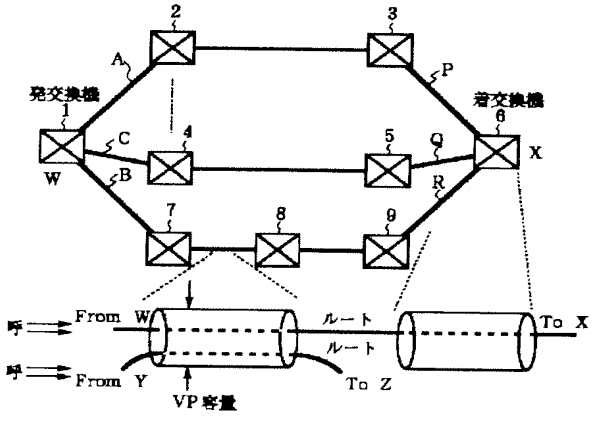
(21)出願番号　特願平7－166048

(22)出願日　平成７年(1995)６月30日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(72)発明者　大木　英司
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(72)発明者　山中　直明
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　井出　直孝　（外１名）

(54)【発明の名称】　ＡＴＭ通信網および故障復旧方法

(57)【要約】
【目的】　交換機の故障を前提とした故障復旧対策を行う。
【構成】　交換機の故障時に、着交換機から故障復旧メッセージセルを送出して交換機が自律分散的に情報を交換し、発交換機に網状態を通知してルートの切替えを行い、交換機故障によるルート障害がＶＣルートレベルにより復旧される。
【効果】　交換機の高信頼性を確保するための冗長なハードウェア構成を省略することができる。このため交換機のコストを低減することができる。さらに、集中的に故障復旧を行う装置を設けることなく故障復旧を行うことができる。



Petitioner Apple Inc. - Exhibit 1026, p. 766

1

【特許請求の範囲】

【請求項１】　複数の加入者交換機と、この複数の加入者交換機相互間を接続する複数の物理伝送路と、この複数の物理伝送路に介挿される中継交換機とを備え、前記複数の加入者交換機の間にバーチャルパスが設定されるＡＴＭ通信網において、

前記加入者交換機には、バーチャルパスに故障復旧メッセージセルを送出する手段を備え、この故障復旧メッセージセルは、宛先領域およびメッセージ領域を有し、その宛先領域に一以上の中継交換機を経由して相手側の加入者交換機に到達するための情報が搭載され、

前記中継交換機には、経由する前記故障復旧メッセージセルのメッセージ領域にその中継交換機の空帯域情報を搭載させる手段を備えたことを特徴とするＡＴＭ通信網。

【請求項２】　前記メッセージ領域には、経由する中継交換機の数を搭載するホップカウンタ領域が設けられ、前記中継交換機には、故障復旧メッセージセルが通過する毎にこのホップカウンタ領域に搭載された中継交換機の数を加算する手段を備えた請求項１記載のＡＴＭ通信網。

【請求項３】　前記加入者交換機には、バーチャルパスに介挿された中継交換機の故障の可能性を認識する手段を備え、前記故障復旧メッセージセルを送出する手段は、この認識する手段の出力にしたがって故障復旧メッセージセルを送出する請求項１または２記載のＡＴＭ通信網。

【請求項４】　前記加入者交換機には、複数のバーチャルパスを介して到来する故障復旧メッセージセルを受信する手段を備え、この故障復旧メッセージセルに含まれる空帯域情報および中継交換機の数にしたがって利用するバーチャルパスを選択する手段を備えた請求項１ないし３のいずれかに記載のＡＴＭ通信網。

【請求項５】　加入者交換機に設定されるバーチャルパスには現用のバーチャルパスおよび予備のバーチャルパスとなりうる複数のバーチャルパスがあらかじめ設定され、この現用のバーチャルパスに介挿される中継交換機に故障の可能性が認識されたとき、前記加入者交換機は故障復旧メッセージセルを前記予備のバーチャルパスとなりうる複数のバーチャルパスにそれぞれ送出し、この故障復旧メッセージセルの宛先となる加入者交換機では、この故障復旧メッセージセルに搭載された空帯域情報および中継交換機の数にしたがって前記予備のバーチャルパスとなりうる複数のバーチャルパスのいずれかを選択することを特徴とする故障復旧方法。

【請求項６】　前記加入者交換機は一つの通信網の中に多数分散して存在し、各加入者交換機が請求項５記載の故障復旧方法を自律分散的に実行する方法。

【請求項７】　加入者交換機に設定されるバーチャルパスには現用のバーチャルパスおよび予備のバーチャルパスとなりうる複数のバーチャルパスがあらかじめ設定され、この現用のバーチャルパスに介挿される中継交換機の故障がなくても、前記加入者交換機は故障復旧メッセージセルを前記予備のバーチャルパスとなりうる複数のバーチャルパスにそれぞれ送出し、この故障復旧メッセージセルの宛先となる加入者交換機では、この故障復旧メッセージセルに搭載された空帯域情報および中継交換機の数にしたがって前記予備のバーチャルパスとなりうる複数のバーチャルパスのいずれかを予備のバーチャルパス候補としてあらかじめ選択することを特徴とする故障復旧の待機方法。

【請求項８】　前記加入者交換機は一つの通信網の中に多数分散して存在し、各加入者交換機が請求項７記載の故障復旧の待機方法を自律分散的に実行する方法。

【請求項９】　一つの通信網内にある加入者交換機は自己にバーチャルパスを設定する自己およびまたはその通信網に属する他の加入者交換機に宛てて故障復旧メッセージセルをバーチャルパスにそれぞれ送出することを特徴とする故障復旧方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はＡＴＭ（非同期転送モード）通信網に利用する。特に、伝送路に介挿された通信装置の故障に対する故障復旧技術に関する。

【０００２】

【従来の技術】ＡＴＭ通信網は、物理的には、バーチャルチャネル(Virtual Channel: 以下ＶＣという）を単位としてスイッチングを行うバーチャルチャネルハンドラ(Virtual Channel Handler、交換機）と、バーチャルパス(Virtual Path:以下ＶＰという）を単位として情報転送の方路を設定するバーチャルパスハンドラ(Virtual Path Handler:ＶＰＨ、またはクロスコネクト、ＸＣ）とが伝送路により接続されて構成される。理論的には、ＶＣＨ間がＶＰにより接続され、ＶＰは零または１以上のＶＰＨを経由してＶＣＨで終端される。

【０００３】従来の通信装置の故障に対する故障復旧方法を図１２に示す。図１２は従来の故障復旧方法の概念を示す図である。従来の故障復旧方法には、図１２（ｂ）に示す物理レベルの故障復旧と図１２（ａ）に示すＶＰレベルの故障復旧がある。物理レベルの故障復旧を実現するためには、物理伝送路リンクを２重化しておき、一方を現用系、もう一方を予備系としておく。もし、現用系の通信装置に故障が発生したら、現用系から予備系に切替えられ、故障が復旧される。しかし、物理レベルの故障復旧では、常時、物理伝送路リンクを２重化しておかなければならず、網リソースを効率的に利用できないという問題がある。

【０００４】そこで、ＡＴＭ通信網の特徴であるＶＰの概念を適用したＶＰレベルの故障復旧方法がある。ＶＰは、情報転送単位であるセルに付与されたヘッダ領域中

Petitioner Apple Inc. - Exhibit 1026, p. 767

のＶＰＩ(Virtual Path Identifier) により識別され、ＶＰＨにおいては、パスの接続先を記述したパス接続（ルーティング）テーブルにより経路が設定される。ＶＰレベルの故障復旧は、ＶＰの経路と容量が独立に設定できることを利用して、故障により切断されたＶＰを、故障箇所を迂回して新たに形成されたＶＰに切り換えることにより実現される。特に、故障発生時に、ＡＴＭ通信網を一元的に監視している集中局があらかじめ設定された迂回パス情報に基づき網内の各ノード（ＶＣＨ、ＶＰＨその他）に対して制御を行う方式を集中制御方式、各ノードが自律分散的に迂回パスを探索・復旧させる故障復旧方式をセルフヒーリング方式という。ＶＰレベルの故障復旧では、物理レベルの故障復旧と比較して、伝送路の網リソースを効率良く利用できる点や網の変化に柔軟に対応できる点で、優れている。したがって、従来の故障復旧方法として、物理レベルとＶＰレベルとを組み合わせた故障復旧方法が適用されている。

【０００５】

【発明が解決しようとする課題】しかし、従来の物理レベルとＶＰレベルのみの故障復旧方法では、ＶＣＨ（交換機）の故障は前提とされないため、高信頼な交換機が必要である。また、複数のメディアが混在するＡＴＭ通信網においては、メディア毎に要求される信頼度が異なるが、最も高く要求される信頼度に合わせて信頼性を満足するように交換機が設計されており、あまり、信頼度を要求しないメディアに対しては、冗長であった。図１３は高信頼化された交換機の概念図であるが、高信頼化された交換機では、図１３のようにスイッチ部、Ｉ／Ｏ部、およびＣＰＵ部が二重化されており、さらに、これらのユニットはクロスルートで結合されている。このような２重化によって高信頼化された交換機のコストは、単純な構成を持つ交換機のコストと比べ、４倍から６倍程度高くなってしまう。

【０００６】本発明は、このような背景に行われたものであり、交換機の故障を前提とした故障復旧対策を行うことができるＡＴＭ通信網および故障復旧方法を提供することを目的とする。本発明は、交換機の高信頼性を確保するための冗長なハードウェア構成を省略することができるＡＴＭ通信網および故障復旧方法を提供することを目的とする。本発明は、交換機のコストを低減することができるＡＴＭ通信網および故障復旧方法を提供することを目的とする。本発明は、集中的に故障復旧を行う装置を設けることなく故障復旧を行うことができるＡＴＭ通信網および故障復旧方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】単純な構成を持つ交換機を通信装置として適用するとき、交換機の故障時のＶＣルート障害を敏速に復旧する必要がある。そこで、本発明は、交換機の故障時にＶＣルート障害を敏速に復旧する方法を提供することを特徴とする。その方法としては交換機の故障時に、発着交換機間の現用ルート障害を復旧するために着交換機から故障復旧メッセージセルを送出し、交換機が自律分散的に情報を交換して発交換機に網状態を通知し、ルートの切替えを行い、交換機故障によるルート障害がＶＣルートレベルにより復旧される。これをＶＣルートレベルのセルフヒーリングという。

【０００８】従来技術では、ＶＰレベルのセルフヒーリングが行われていたが、本発明の特徴とするところは、ＶＣルートレベルのセルフヒーリングによって、交換機故障時のＶＣルート障害を復旧することができることにある。

【０００９】すなわち、本発明の第一の観点は、複数の加入者交換機と、この複数の加入者交換機相互間を接続する複数の物理伝送路と、この複数の物理伝送路に介挿される中継交換機とを備え、前記複数の加入者交換機の間にバーチャルパスが設定されるＡＴＭ通信網である。

【００１０】ここで、本発明の特徴とするところは、前記加入者交換機には、バーチャルパスに故障復旧メッセージセルを送出する手段を備え、この故障復旧メッセージセルは、宛先領域およびメッセージ領域を有し、その宛先領域に一以上の中継交換機を経由して相手側の加入者交換機に到達するための情報が搭載され、前記中継交換機には、経由する前記故障復旧メッセージセルのメッセージ領域にその中継交換機の空帯域情報を搭載させる手段を備えたところにある。

【００１１】前記メッセージ領域には、経由する中継交換機の数を搭載するホップカウンタ領域が設けられ、前記中継交換機には、故障復旧メッセージセルが通過する毎にこのホップカウンタ領域に搭載された中継交換機の数を加算する手段を備えることが望ましい。

【００１２】前記加入者交換機には、バーチャルパスに介挿された中継交換機の故障の可能性を認識する手段を備え、前記故障復旧メッセージセルを送出する手段は、この認識する手段の出力にしたがって故障復旧メッセージセルを送出することが望ましい。

【００１３】前記加入者交換機には、複数のバーチャルパスを介して到来する故障復旧メッセージセルを受信する手段を備え、この故障復旧メッセージセルに含まれる空帯域情報および中継交換機の数にしたがって利用するバーチャルパスを選択する手段を備えることが望ましい。

【００１４】本発明の第二の観点は故障復旧方法であり、その特徴とするところは、加入者交換機に設定されるバーチャルパスには現用のバーチャルパスおよび予備のバーチャルパスとなりうる複数のバーチャルパスがあらかじめ設定され、この現用のバーチャルパスに介挿される中継交換機に故障の可能性が認識されたとき、前記加入者交換機は故障復旧メッセージセルを前記予備のバーチャルパスとなりうる複数のバーチャルパスにそれぞ

Petitioner Apple Inc. - Exhibit 1026, p. 768

れ送出し、この故障復旧メッセージセルの宛先となる加入者交換機では、この故障復旧メッセージセルに搭載された空帯域情報および中継交換機の数にしたがって前記予備のバーチャルパスとなりうる複数のバーチャルパスのいずれかを選択するところにある。

【００１５】この故障復旧方法では、前記加入者交換機は一つの通信網の中に多数分散して存在し、各加入者交換機がこの故障復旧方法を自律分散的に実行することが特徴である。

【００１６】本発明の第三の観点は故障復旧待機方法であり、その特徴とするところは、加入者交換機に設定されるバーチャルパスには現用のバーチャルパスおよび予備のバーチャルパスとなりうる複数のバーチャルパスがあらかじめ設定され、この現用のバーチャルパスに介挿される中継交換機の故障がなくても、前記加入者交換機は故障復旧メッセージセルを前記予備のバーチャルパスとなりうる複数のバーチャルパスにそれぞれ送出し、この故障復旧メッセージセルの宛先となる加入者交換機では、この故障復旧メッセージセルに搭載された空帯域情報および中継交換機の数にしたがって前記予備のバーチャルパスとなりうる複数のバーチャルパスのいずれかを予備のバーチャルパス候補としてあらかじめ選択するところにある。

【００１７】この故障復旧待機方法では、前記加入者交換機は一つの通信網の中に多数分散して存在し、各加入者交換機がこの故障復旧待機方法を自律分散的に実行することが特徴である。

【００１８】本発明の第四の観点は故障復旧方法であり、その特徴とするところは、一つの通信網内にある加入者交換機は自己にバーチャルパスを設定する自己およびまたはその通信網に属する他の加入者交換機に宛てて故障復旧メッセージセルをバーチャルパスにそれぞれ送出するところにある。

【００１９】この明細書では、加入者交換機と中継交換機とをあたかも異なる通信装置であるかのような表現を用いているが、これは説明をわかりやすくするためのものであり、同一のハードウェア構成の通信装置により実現することができる。

【００２０】

【作用】本発明の方法では、ＶＣルートレベルのセルフヒーリングによって、着交換機から故障復旧メッセージセルを送出して、交換機が自律分散的に情報を交換し、発交換機に網状態を通知し、ルートの切替えを行い、交換機故障時のＶＣルート障害を復旧することができるので、高信頼な交換機を使用する必然性がなくなり、単純な構成を持つ交換機を使用することにより、コスト削減が図られる。

【００２１】着交換機が送出する故障復旧メッセージセルはバーチャルパスを介して発交換機に到達する。このバーチャルパスは、予備のバーチャルパスとなりうるバーチャルパスとしてあらかじめ定められているバーチャルパスでもよいし、故障が認識されていない不特定のバーチャルパスでもよい。

【００２２】故障復旧メッセージセルは、着交換機から発交換機に到達する間に通過するバーチャルパスの空帯域情報を収集する。言い方を替えると、通過するバーチャルパスに介挿されている中継交換機は、故障復旧メッセージセルを通過させるときに、自己の中継交換機における空帯域情報を故障復旧メッセージセルの例えばメッセージ領域に搭載する。また、同時に通過した中継交換機の数も情報として搭載する。発交換機では、空帯域情報および通過した中継交換機の数の情報を参考にして予備のバーチャルパスとして最適なバーチャルパスを選択する。以降は、このバーチャルパスにバーチャルチャネルを設定して通信を再開する。

【００２３】故障復旧メッセージセルの送出は現用のバーチャルパスあるいは現用のバーチャルパス上の中継交換機に何らかの故障が認識されたときに行われるように制御してもよいし、あるいは、平常時にも故障復旧メッセージセルを送出し、常時、予備のバーチャルパスとして最適なバーチャルパス候補を選択しておくこともよい。

【００２４】本発明では、このような故障復旧制御をＡＴＭ通信網に含まれる各交換機が自律分散に行うことを主要な特徴としている。

【００２５】

【実施例】

（第一実施例）本発明第一実施例の構成を図１～図５を参照して説明する。図１は本発明の全体構成図である。図２は着交換機の要部ブロック構成図である。図３は故障復旧メッセージセルの構成図である。図４は中継交換機の要部ブロック構成図である。図５は発交換機の要部ブロック構成図である。

【００２６】本発明は、加入者交換機である発交換機１および着交換機６と、この発交換機１および着交換機６相互間を接続する物理伝送路Ｐ～Ｒと、この物理伝送路Ｐ～Ｒに介挿される中継交換機２、３、４、５、７、８、９とを備え、発交換機１および着交換機６の間にバーチャルパスが設定されるＡＴＭ通信網である。

【００２７】ここで、本発明の特徴とするところは、着交換機６には、バーチャルパスに故障復旧メッセージセルを送出する手段としての故障復旧メッセージセル生成部１２を備え、この故障復旧メッセージセルは、宛先領域Ｈおよびメッセージ領域Ｍを有し、その宛先領域Ｈに一以上の中継交換機２、３、４、５、７、８、９を経由して発交換機１に到達するための情報が搭載され、中継交換機２、３、４、５、７、８、９には、経由する故障復旧メッセージセルのメッセージ領域Ｍにその中継交換機２、３、４、５、７、８、９の空帯域情報を搭載させる手段としての故障復旧メッセージセル情報搭載部１４

Petitioner Apple Inc. - Exhibit 1026, p. 769

を備えたところにある。

【００２８】本発明実施例では、説明をわかりやすくするために、発交換機１、着交換機６、中継交換機２、３、４、５、７、８、９をそれぞれあたかも異なるハードウェア構成を備えた通信装置であるかのように表現するが、これらは各機能を共通に備えた一つの通信装置として実現することができる。

【００２９】メッセージ領域Ｍには、経由する中継交換機２、３、４、５、７、８、９の数を搭載するホップカウンタ領域ＨＣが設けられ、中継交換機２、３、４、５、７、８、９には、故障復旧メッセージセルが通過する毎にこのホップカウンタ領域ＨＣに搭載された中継交換機の数を加算する手段を故障復旧メッセージセル情報搭載部１４に併せて備えている。

【００３０】発交換機１および着交換機６には、バーチャルパスに介挿された中継交換機２、３、４、５、７、８、９の故障の可能性を認識する手段としての故障検出部１０を備え、故障復旧メッセージセル生成部１２は、この故障検出部１０の出力にしたがって故障復旧メッセージセルを送出する。

【００３１】発交換機１には、複数のバーチャルパスを介して到来する故障復旧メッセージセルを受信する手段としての予備ルート設定部１６を備え、この故障復旧メッセージセルに含まれる空帯域情報および中継交換機の数にしたがって利用するバーチャルパスを選択する手段を予備ルート設定部１６に併せて備えている。

【００３２】ＶＣルートは発交換機１から１つ以上のＶＰを経て着交換機６に設定される。発交換機１において、呼が発生したときに、複数のＶＣルートの中からあるルートを選択して、呼受付判定(Connection Admission Control:CAC)を行う。例えば、ルートの選択は、ランダムに選択される。ＣＡＣによって、呼が受付けられたら、ＶＣコネクションを設定し、呼が受付けられなければ呼損となる。

【００３３】次に、本発明第一実施例の動作を図６を参照して説明する。図６は本発明第一実施例の動作を説明するための図である。図６に示すように、１つの現用ルートのみに着目し、中継交換機５に故障が発生したときの、本発明第一実施例の故障回復方法を示す。発交換機１と着交換機６との間に現用ルート（１→４→５→６）が２つの中継交換機を介して設定されており、現用ルートは現時点でＢ〔Ｍｂｐｓ〕の帯域を使用している。

【００３４】この現用ルートに対して、ＣＡＣの後に呼が受付けられ、ＶＣコネクションが設定されたり、切断されたりしている。この現用ルートの使用帯域は、例えば、発交換機１において、あるウィンドウサイズ内の現用ルートで使用されているセル数を観測することによって求められる。観測に使用されるウィンドウとして、ジャンピングウィンドウやスライディングウィンドウがある。

【００３５】ここで、ジャンピングウィンドウとは、ウィンドウ位置（観測位置）が一定周期でオーバーラップすることなく遷移する観測方法であり、スライディングウィンドウとは、ウィンドウ位置が一定周期でオーバーラップしながら徐々に遷移する観測方法である。ごく大まかにいうとジャンピングウィンドウは高速な観測が利点であり、スライディングウィンドウは正確な観測が利点である。

【００３６】故障により、現用ルートが使用不可能になることに備えて、複数の予備ルートを予め設定しておく、図６では、２つの予備ルート（ルートＰ：１→２→３→６、ルートＲ：１→７→８→９→６）が設定されている。故障が発生したとき、現用ルートが使用不可能な状態であることは、アラームを通知するセルその他により発交換機１および着交換機６が認識する。現用ルートに現時点で設定されていたＶＣコネクションの救済は行わないが、故障発生後に、新たに要求してくるＶＣの呼を最大限受付けられるように、迂回ルートを探索する。ここで、着交換機６は故障復旧メッセージセルを送出するセンダ、発交換機１は故障復旧メッセージセルを受取り予備ルートの中から切替えルートを選択するチューザとなる。着交換機（センダ）６は、予備ルートに対してその状態を調べるために、故障復旧メッセージセルを送出する。故障復旧メッセージセルは予備ルートＰおよびＲの経路に沿って、予備ルートＰおよびＲの経路上のＶＰの状態を調べる。ルートＲを例に上げて説明する。故障復旧メッセージセルのメッセージ領域Ｍにはペイロードとして、

（１）ホップカウンタＨＣ
（２）ホップリミットＨＬ
（３）ＶＰ未使用帯域の最小値b_{min}
（４）経路情報ＲＤ

が書込まれる。ホップリミットＨＬは、遅延条件その他を考慮して、予め設定されている。最小値b_{min}の値を∞としておき、最小値b_{min}の値は故障復旧メッセージセルに書込まれている。ルートＲを経由する故障復旧メッセージセルは、着交換機６から中継交換機９に送出され、中継交換機９では、

$b < b_{min}$

ならば、未使用ＶＰ帯域ｂの値をb_{min}とする。ｂは中継交換機９において、例えば、あるウィンドウサイズ内のＶＰ未使用帯域は、使用セル数を観測することによって求められる。観測に使用されるウィンドウとして、ジャンピングウィンドウやスライディングウィンドウがある。ホップカウンタＨＣは中継交換機９→８→７を経由する毎に、１つカウントアップされ、ホップリミットＨＬを超えない限り、さらに次の交換機に送出される。しかし、通常、予備ルートは、ホップリミットを超えないように予め設定されている。次の交換機８では、ｂ＝２であり、$b < b_{min}$なので、b_{min}＝２となる。同様に

Petitioner Apple Inc. - Exhibit 1026, p. 770

故障復旧メッセージセル送出のプロセスを繰り返し、故障復旧メッセージセルは、発交換機１に到着する。また、予備ルートＰ上に送出された故障復旧メッセージセルＡも同様にして、発交換機１に到着する。発交換機１は、予備ルートＰまたはＲの中から、現用ルートの使用帯域Ｂや予備ルート情報（ＶＰ未使用帯域の最小値b_{min}、ホップ数）その他を考慮して、切替先のルートとして１つまたは複数選択する。図７は本発明第一実施例におけるルート切替状況を示す図であるが、図７の例では、予備ルートの中でルートＰが最もＶＰ未使用帯域の最小値が大きいので、ルートＰが切替先のルートとして選択され、故障復旧後はルートＰが現用ルートとして使用される。

【００３７】したがって、交換機の故障時に、故障復旧メッセージセルの送出により交換機が自律分散的に情報を交換し、ルートの切替えを行い、故障が復旧されるので、従来のような２重化された高信頼な交換機でなくても単純な構成を持つ交換機を用いることかできるため、交換機のコスト削減が図れる。

【００３８】（第二実施例）次に、本発明第二実施例を図８を参照して説明する。図８は本発明第二実施例の動作を説明するための図である。本発明第一実施例では、故障発生時に故障復旧メッセージセルを送出していたが、本発明第二実施例では、図８のように、通常時でも、着交換機（センダ）６からＲＭ(Resource Management) セルを送出して、予備ルートＰおよびＲの状態を監視しておく。ＲＭセルの動作は、本発明第一実施例の故障復旧メッセージセルの動作と同様である。発交換機（チューザ）１は、予備ルートＰまたはＲの中から、現用ルートの使用帯域Ｂや予備ルート情報（ＶＰ未使用帯域の最小値b_{min}、ホップ数）その他を考慮して、現用ルートの障害時に備えて、切替先のルートを決めておく。

【００３９】ここで、着交換機（センダ）６からＲＭセルは、定期的に送出され、ＲＭセルを受け取った発交換機（チューザ）１は、網状態に応じて切替先のルートを更新しておく。ＲＭセルの送出間隔は、網状態の変化の度合いから決定される。

【００４０】故障が発生したとき、現用ルートが使用不可能な状態であることは、アラームを通知するセルその他により発交換機１が認識する。現用ルートの障害を検知した発交換機１は、通常に現用ルート障害時に備えてあった切替先ルートに切替えられ、現用ルートとして使用される。

【００４１】したがって、通常時に、着交換機（センダ）６からＲＭ(Resource Management) セルを送出して、予備ルートの状態を監視して、現用ルートの障害時に備えて切替先ルートを決めておくことにより、故障復旧時間の短縮化が図れる。

【００４２】（第三実施例）次に、本発明第三実施例を図９を参照して説明する。図９は本発明第三実施例の動作を説明するための図である。本発明第一実施例では、予め予備ルートＰおよびＲを設定しておき、故障発生時に予備ルートＰおよびＲ上に故障復旧メッセージセルを送出していた。本発明第三実施例では、予め予備ルートＰおよびＲを設定しておかず、図９のようにフラッディング(Flooding)により故障復旧メッセージセルを送出し、発交換機１に到達した故障復旧メッセージセルにしたがって発交換機１が予備ルートを選択する。

【００４３】ここで、フラッディングとは、“Ｆｌｏｏｄ”すなわち、あたかも“洪水”のように不特定方向に対してセルを送出させるというイメージに基づいた用語であり、自交換機へＶＰを送出するすべての交換機へ故障復旧メッセージセルを送出するという意味に用いる。

【００４４】故障復旧メッセージセルのペイロードには、本発明第一実施例で説明したように、

（１）ホップカウンタＨＣ
（２）ホップリミットＨＬ
（３）ＶＰ未使用帯域の最小値b_{min}
（４）経路情報ＲＤ

が書込まれる。ホップリミットＨＬは、遅延条件その他を考慮して、予め設定されている。最小値b_{min}の値を∞としておき、最小値b_{min}の値は故障復旧メッセージセルに書込まれている。

【００４５】まず、着交換機（センダ）６は、自交換機へＶＰを送出するすべての交換機へ故障復旧メッセージセルを送出する。故障復旧メッセージセルを受信した交換機は、$b < b_{min}$ならば、未使用ＶＰ帯域ｂの値をb_{min}とする。ｂは交換機において、例えば、あるウィンドウサイズ内のＶＰ未使用帯域は、使用セル数を観測することによって求められる。経由した交換機の情報が経路情報として書込まれる。ホップカウンタＨＣは交換機を経由する毎に、１つカウントアップされ、もし、ホップリミットＨＬを超えているか、または、経路情報ＲＤにより既に同じ交換機を経由していれば、故障復旧メッセージセルは廃棄される。そうでなければ、さらに、自交換機へＶＰを送出するすべての交換機へ故障復旧メッセージセルを送出し、故障復旧メッセージセルを受信した交換機は同様の動作を繰り返し、故障復旧メッセージは、発交換機に到着する。

【００４６】発交換機（チューザ）１は、到着した故障復旧メッセージセルから現用ルートの使用帯域Ｂや到着した故障復旧メッセージセルを基にしたルート情報（ＶＰ未使用帯域の最小値b_{min}、ホップ数）その他を考慮して、切替先のルートとして１つまたは複数選択する。

【００４７】したがって、予め予備ルートを設定しておくことなく、フラッディングにより故障復旧メッセージセルを送出し、発交換機１に故障復旧メッセージセルを到着させることにより、網トポロジやＶＰ容量その他の変化に柔軟に対応した故障復旧を行うことができる。

Petitioner Apple Inc. - Exhibit 1026, p. 771

11

【００４８】本発明の故障復旧方法による故障復旧概念を図１０および図１１に示す。図１０は本発明の故障復旧方法の概念を示す図である。図１１は本発明の故障復旧方法を適用したＡＴＭ通信網の概念図である。図１０（ｂ）および（ｃ）は、従来から知られているＶＰレベルおよび物理レベルの故障復旧概念である。本発明では図１０（ａ）に示すように、ＶＣルートレベルの故障復旧を行うことにより図１１に示すように、高信頼性の交換機を用いることなくＡＴＭ通信網を構成することができる。

【００４９】

【発明の効果】以上説明したように、本発明によれば、交換機の故障を前提とした故障復旧制御を行うことができる。このため、交換機の高信頼性を確保するための冗長なハードウェア構成を省略することができる。したがって、交換機のコストを低減することができる。さらに、集中的に故障復旧を行う装置を設けることなく故障復旧を行うことができる。

【図面の簡単な説明】

【図１】本発明の全体構成図。

【図２】着交換機の要部ブロック構成図。

【図３】故障復旧メッセージセルの構成図。

【図４】中継交換機の要部ブロック構成図。

【図５】発交換機の要部ブロック構成図。

【図６】本発明第一実施例の動作を説明するための図。

12

【図７】本発明第一実施例におけるルート切替状況を示す図。

【図８】本発明第二実施例の動作を説明するための図。

【図９】本発明第三実施例の動作を説明するための図。

【図１０】本発明の故障復旧方法の概念を示す図。

【図１１】本発明の故障復旧方法を適用したＡＴＭ通信網の概念図。

【図１２】従来の故障復旧方法の概念を示す図。

【図１３】高信頼化された交換機の概念図。

【符号の説明】

１　発交換機

２～５、７～９　中継交換機

６　着交換機

１０　故障検出部

１２　故障復旧メッセージセル生成部

１４　故障復旧メッセージセル情報搭載部

１６　予備ルート設定部

Ｈ　宛先領域

ＨＣ　ホップカウンタ

ＨＬ　ホップリミット

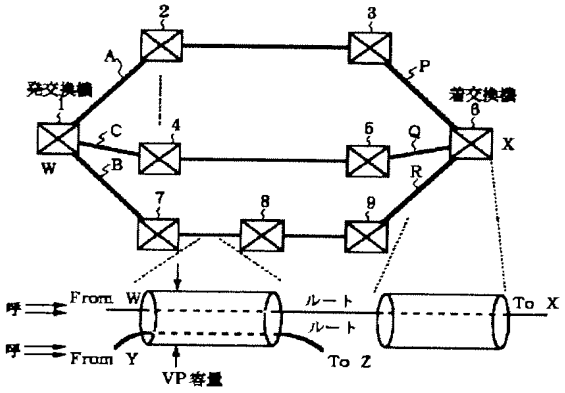
Ｍ　メッセージ領域

ＲＤ　経路情報

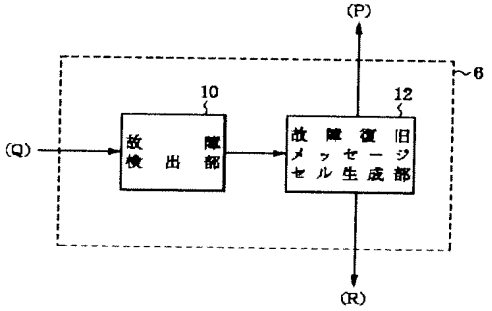
b_{min}　最小値

Ｐ、Ｑ、Ｒ　ルート

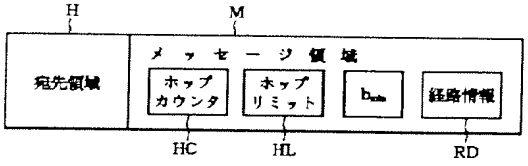
【図１】



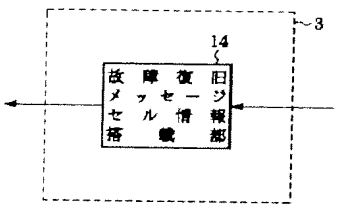
【図２】



【図３】

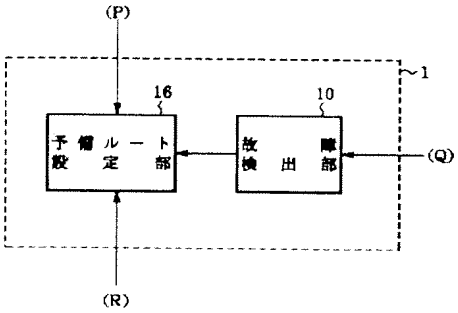


【図４】

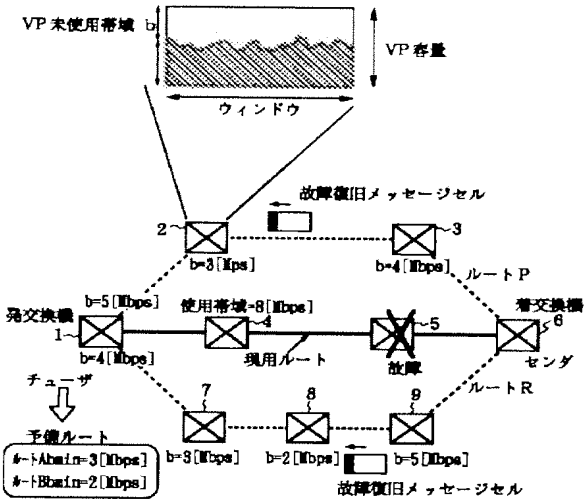


Petitioner Apple Inc. - Exhibit 1026, p. 772

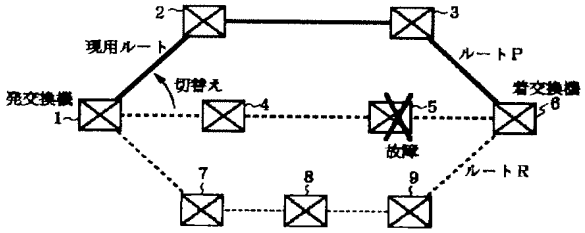
【図５】



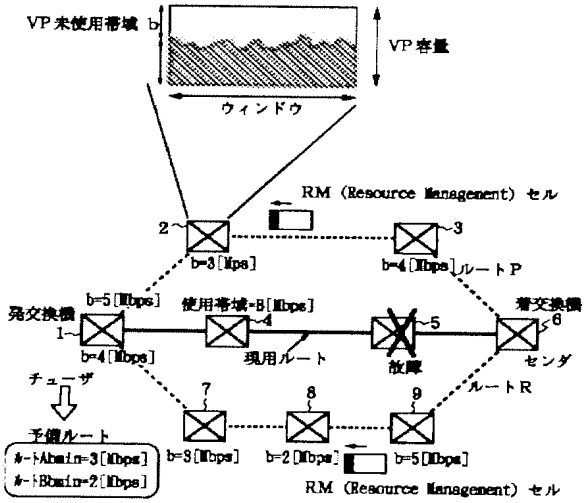
【図６】



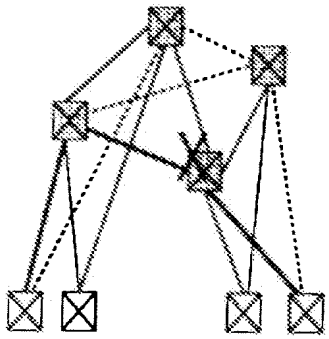
【図７】



【図８】

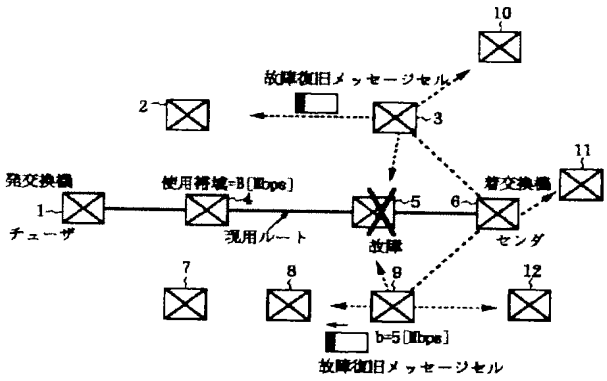


【図１１】

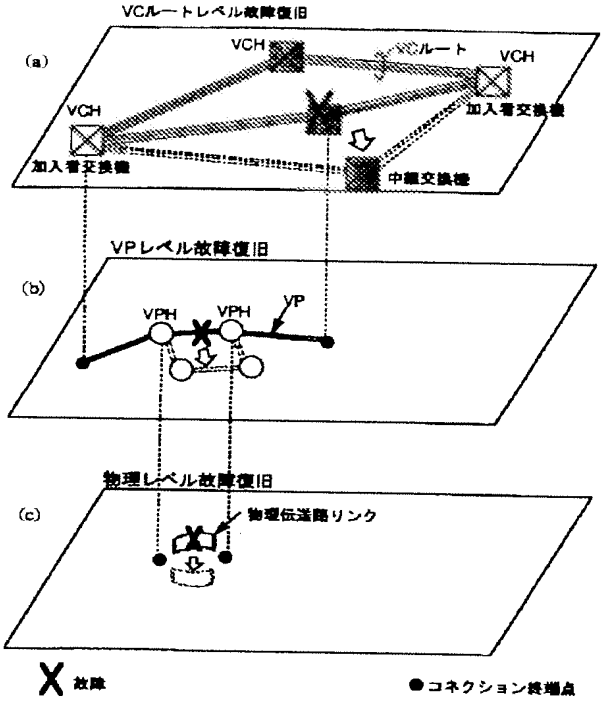


交換機のダウンサイジング化

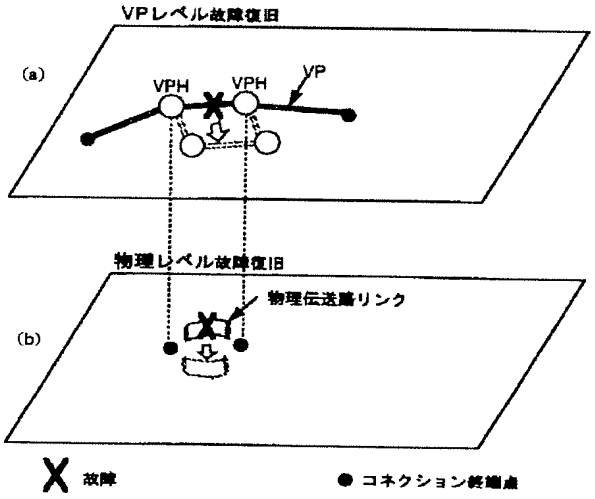
【図９】



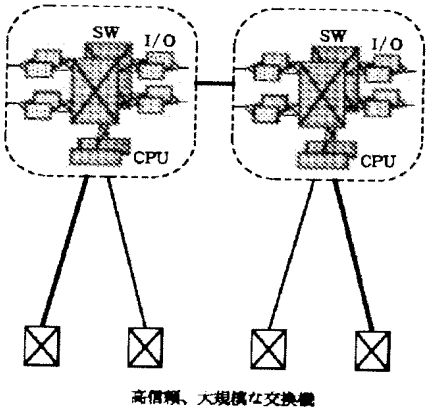
【図１０】



【図１２】



【図１３】



Electronic Patent Application Fee Transmittal

Application Number:	11679416
Filing Date:	27-Feb-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Atabak R Royaee/Melissa Molchan
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	7341460
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royaee/Melissa Molchan
Filer Authorized By:	Atabak R Royaee
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)
Receipt Date:	02-APR-2010
Filing Date:	27-FEB-2007
Time Stamp:	12:19:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	7572
Deposit Account	501133
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Information Disclosure Statement (IDS) Filed (SB/08)	0015.pdf	81746 86f54de5d8afd5e64e516f69bf4a7faac174700b	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
2		jp.pdf	2159740 c1f5c3a6d9721eec83fbef0087e759d448898a69	yes	53

Multipart Description/PDF files in .zip description

Document Description	Start	End
Foreign Reference	1	6
Foreign Reference	7	23
Foreign Reference	24	30
Foreign Reference	31	53

Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	NPL Documents	Feng.pdf	215626 58bf05014b12aa13483ab383b6d7b0c529b2e711	no	4
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
4	NPL Documents	Davies.pdf	572855 570f1932ebcd625d840e44ae1e6c1c78603cf33c	no	15
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
5	Fee Worksheet (PTO-875)	fee-info.pdf	30669 baf8a5dcf1519007a85380055c72be9102a12ad6	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	3060636

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/679,416	02/27/2007	Victor Larson	77580-015 (VRNK-1CP2DVCN)	3528

23630 7590 04/08/2010

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
LIM, KRISNA	

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
04/08/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mweipdocket@mwe.com

Office Action Summary	Application No.	Applicant(s)	
	11/679,416	LARSON ET AL.	
	Examiner	Art Unit	
	Krisna Lim	2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 December 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Claims 2-30 are newly added for examination, and claim 1 was canceled.

As required by M.P.E.P. 609(C), the applicant's submissions of the Information Disclosure Statement dated December 14, 2009 is acknowledged by the examiner and the cited references have been considered in the examination of the claims now pending. As required by M.P.E.P 609 C(2), a copy of the PTOL-1449 initialed and dated by the examiner is attached to the instant office action..

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The specification does not mention or define "machine readable medium" which is found in claims 28-30. Depending on the definition given "machine readable medium" may include embodiments that are not statutory in view of 35 USC § 101. Therefore, the applicant should amend the specification giving "machine readable medium" a definition that would be available to one having ordinary skill in the art at the time of the invention so that it can be determined if the limitations are statutory.

Claims 2-30 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claim 2, at line 3, it is unclear from where a message is sent. It is unclear what kind of "name service" that the applicants are talking about (i.e., is it a secure domain name service? or is it a domain name service?) It is unclear what kind of an address that the applicants are talking about (i.e., is it an address of a secure computer network?). At line 5, it is unclear where a message is received.

In claims 3-23, they contain similar languages and problems as in claim 2 above.

In claim 24, it is unclear what kind of “secure name” that the applicants are talking about (i.e., is it a secure domain name?). At line 4, it is unclear that kind of an address that the applicants are talking about. It is unclear what kind of the first device

and the second device that the applicants are talking about. Are they the same or different?

In claims 25-30, they contain similar languages and problems as in claim 24 above.

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title.

Claims 28-30 are rejected under 35 U.S.C. §101 because they are rejected under 35 US.C. § 101 as on-statutory subject matter.

The broadest reasonable interpretationof a claim drawn to a **computer readable medium** (also called **machine readable medium** and other such variations) typically covers forms of non-transitory tangible media and transitory propagating signals per *se* in view of the ordinary and customary meaning of computer readable media, particularly when the specification is silent. *See* MPEP 2111.01. *See In re Nuijten,* 500 F.3d 1346, 1356-57 (Fed. Cir. 2007) (transitory embodiments are not directed to statutory subject matter) and *Interim Examination Instructions for Evaluating Subject Matter Eligibility Under* 35 *Us.* C. § *101,* Aug. 24, 2009; p. 2.

Note: adding the limitation "non-transitory" to the claim would not raise the issue of new matter even the specification is silent because the broadest reasonable interpretation relies on the ordinary and customary meaning that includes signal per se.

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct

from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 2, 24, 26 and 28-30 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 7,188,180. Although the conflicting claims are not identical, they are not patentably distinct from each other because they are directed to a method of accessing a secure computer network address (i.e., a method of communicating with a device having a secure name), comprising steps of: a) sending a query message to a secure domain ...; b) receiving from the secure domain name center ...; and c) sending a message … to the address using a secure communication link.

Claims 2, 24, 26 and 28-30 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of copending Application No. 11/839,987. Although the conflicting claims are not identical, they are not patentably distinct from each other because a method of accessing a secure computer network address (i.e., a method of communicating with a device having a secure name), comprising steps of: a) sending a query message to a secure domain ...; b) receiving from the secure domain name center ...; and c) sending a message … to the address using a secure communication link.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

A shortened statutory period for response to this action is set to expire 3 (three) months and 0 (zero) days from the mail date of this letter.

Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.

If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.

Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Krisna Lim whose telephone number is 571-272-3956 The examiner can normally be reached on Tuesday to Friday from 7:10 AM to 5:40 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas, can be reached on 571-272-6776. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kl

March 27, 2010

/Krisna Lim/

Primary Examiner, Art Unit 2453

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11679416	LARSON ET AL.
	Examiner	Art Unit
	Krisna Lim	2453

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/05/2009	03/27/2010							
	1	✓								
	2		✓							
	3		✓							
	4		✓							
	5		✓							
	6		✓							
	7		✓							
	8		✓							
	9		✓							
	10		✓							
	11		✓							
	12		✓							
	13		✓							
	14		✓							
	15		✓							
	16		✓							
	17		✓							
	18		✓							
	19		✓							
	20		✓							
	21		✓							
	22		✓							
	23		✓							
	24		✓							
	25		✓							
	26		✓							
	27		✓							
	28		✓							
	29		✓							
	30		✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	111679416	LARSON ET AL.
	Examiner	Art Unit
	Krisna Lim	2453

SEARCHED			
Class	Subclass	Date	Examiner
709	225-229, 245	6/6/09	kl

SEARCH NOTES		
Search Notes	Date	Examiner
Inventors, EAST	6/6/09	kl

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

OIPE IAP9 NOV 06 2009 PATENT & TRADEMARK OFFICE

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**11/679,416**
Filing Date	**February 27, 2007**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**LIM, Krisna**
Docket Number	**077580-0015 (VRNK-1CP2DVCN)**

Sheet 1 of 2

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1227	Microsoft Corporation's Fifth Amended Invalidity Contentions dated September 18, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation and invalidity claim charts for U.S. Patent Nos. 7,188,180 and 6,839,759	
	C1228	The IPSEC Protocol as described in Atkinson, et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401"); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1229	S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1230	C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1231	C. Madson and R. Glenn, "The Use HMAC-SHA-1-96 within ESP and AH," RFC 2404 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/27/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2453**
				Examiner Name	**LIM, Krisna**
Sheet	2	of	2	Docket Number	**077580-0015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
	C1232	C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1233	S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1234	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1235	Douglas Maughan, et al, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1236	D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1237	R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1238	R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1239	Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (November 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (July 1996) ("Galvin")	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/27/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

BST99 1632946-1.077580.0015

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OIPE IAP93
OCT 06 2009
PATENT & TRADEMARK OFFICE

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	**11/679,416**
Filing Date	**February 27, 2007**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Lim, Krisna**
Sheet 1 of 1	Docket Number **77580-015 (VRNK-1CP2DVCN)**

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1177	WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000)	
	C1178	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999)	
	C1179	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000)	
	C1180	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000)	
	C1181	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000) **(resubmitted)**	
	C1182	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Release Notes* (July 21, 2000)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/27/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

BST99 1630399-1.077580.0015

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

OIPE
SEP 08 2009
PATENT & TRADEMARK OFFICE

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Sheet	1	of	2

Complete if Known	
Application Number	**11/679,416**
Filing Date	**February 27, 2007**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Lim, Krisna**
Docket Number	**77580-015 (VRNK-1CP2DVCN)**

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number 4-Kind Codes *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)	
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1)	
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)	
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/soc kswp.html (1997). (Socks, Aventail)	
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)	
	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3)	
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4)	
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5)	
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6)	
	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7)	
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8)	
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/27/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO **SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(Use as many sheets as necessary)*				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**February 27, 2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2453**
				Examiner Name	**Lim, Krisna**
Sheet	2	of	2	Docket Number	**77580-015 (VRNK-1CP2DVCN)**

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10)	
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11)	
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail)	
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail)	
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail)	
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW)	
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12)	
	C1081	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	C1090	Assured Digital Products. (Assured Digital)	
	C1146	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3)	
	C1155	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)	
	C1163	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4)	
	C1164	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview)	
	C1168	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager)	
	C1201	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000)	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/27/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.
BST99 1628591-1.077580.0015

(2)
ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

RIPE IAP19 DEC 14 2009 PATENT & TRADEMARK OFFICE

Complete if Known	
Application Number	**11/679,416**
Filing Date	**February 27, 2007**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**LIM, Krisna**
Sheet 1 of 1	
Docket Number	**077580-0015 (VRNK-1CP2DVCN)**

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1019	US	7,461,334	12/02/08	Lu, et al.	
	A1020	US	7,353,841	04/08/08	Kono, et al.	
	A1021	US	7,188,175	03/06/07	McKeeth, James A.	
	A1022	US	7,167,904	01/23/07	Devarajan, et al.	
	A1023	US	7,039,713	05/02/06	Van Gunter, et al.	
	A1024	US	6,757,740	06/29/04	Parekh, et al.	
	A1025	US	6,752,166	06/22/04	Lull, et al.	
	A1026	US	6,687,746	02/03/04	Shuster, et al.	
	A1027	US	6,338,082	01/08/02	Schneider, Eric	
	A1028	US	6,333,272	12/25/01	McMillin, et al.	
	A1029	US	6,314,463	11/06/01	Abbott, et al.	
	A1030	US	6,298,341	10/02/01	Mann, et al.	
	A1031	US	6,262,987	07/17/01	Mogul, Jeffrey C.	
	A1032	US	6,199,112	03/06/04	Wilson, Stephen K.	
	A1033	US	2,895,502	07/21/59	Garland Roper Charles, et al.	
	A1034	US	2001/0049741	12/06/01	Skene, et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes3-Number 4-Kind Codes (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1240	David Kosiur, "Building and Managing Virtual Private Networks" (1998)	
	C1241	P. Mockapetris, "Domain Names – Implementation and Specification," Network Working Group, RFC 1035 (November 1987)	
	C1242	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.	
	C1243	Request for Inter Partes Reexamination of Patent No. 7,188,180, dated Nov. 25, 2009.	

EXAMINER	/Krisna Lim/	DATE CONSIDERED	03/27/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

PTO/SB/25 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION

Docket Number (Optional)
77580-15 (VRNK-1CP2DVCN)

In re Application of: Victor Larson et al.

Application No.: 11/679,416

Filed: February 27, 2007

For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

The owner*, VirnetX, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 11/839,987, filed on 08/16/2007, as such term is defined in 35 U.S.C. 154 and 173, and as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent: granted on the pending **reference** application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 26418

/Toby H. Kusmer/ — Signature
10/08/2010 — Date

Toby H. Kusmer — Typed or printed name

617-535-3000 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/26 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT

Docket Number (Optional)
77580-15 (VRNK-1CP2DVCN)

In re Application of: Victor Larson et al.

Application No.: 11/679,416

Filed: February 27, 2007

For: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

The owner*, VirnetX, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term **prior patent** No. 7,188,180 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;
is held unenforceable;
is found invalid by a court of competent jurisdiction;
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
has all claims canceled by a reexamination certificate;
is reissued; or
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☑ The undersigned is an attorney or agent of record. Reg. No. 26418

/Toby H. Kusmer/ — Signature
10/08/2010 — Date

Toby H. Kusmer — Typed or printed name

617-535-4000 — Telephone Number

☑ Terminal disclaimer fee under 37 CFR 1.20(d) included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	11/679,416
Filing Date	02/27/2007
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Attorney Docket Number	77580-15 (VRNK-1CP2DVCN)

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      ii. ☐ Other _____

   b. ☑ Enclosed

      i. ☑ Amendment/Reply

      ii. ☐ Affidavit(s)/ Declaration(s)

      iii. ☐ Information Disclosure Statement (IDS)

      iv. ☐ Other _____

2. Miscellaneous

   a. ☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months. Fee under 37 CFR 1.17(i) required)

   b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

   a. ☑ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Deposit Account No. 501133.

      i. ☑ RCE fee required under 37 CFR 1.17(e)

      ii. ☑ Extension of time fee (37 CFR 1.136 and 1.17)

      iii. ☐ Other _____

   b. ☐ Check in the amount of $ _____ enclosed

   c. ☐ Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/Toby H. Kusmer/	Date	10/05/2010
Name (Print/Type)	Toby H. Kusmer	Registration No.	26418

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print/Type)		Date	

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	11679416
Filing Date:	27-Feb-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 3 months with $0 paid	1253	1	1110	1110

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for continued examination	1801	1	810	810
Statutory disclaimer	1814	2	140	280
		Total in USD ($)		**2200**

Electronic Acknowledgement Receipt

EFS ID:	8593739
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kelly Ciarmataro
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)
Receipt Date:	08-OCT-2010
Filing Date:	27-FEB-2007
Time Stamp:	17:43:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2200
RAM confirmation Number	4363
Deposit Account	501133
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		AmendB.pdf	139647 6d049be1109874b1459eda427761db856a987249	yes	12

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment Submitted/Entered with Filing of CPA/RCE	1	1
Claims	2	6
Applicant Arguments/Remarks Made in an Amendment	7	12

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

2	Terminal Disclaimer Filed	TermDis_Prov.pdf	207469 eb8d1db111d7f9d70e1efabd61dfb2f7df224bd0	no	2

Warnings:

Information:

3	Terminal Disclaimer Filed	TermDisc_PriorPat.pdf	210421 678c19221d031a575ca48e5c972648d1053a5152	no	2

Warnings:

Information:

4	Request for Continued Examination (RCE)	RCE.pdf	354166 d5711414c4f0f658aa45673f9556f50d20ee8957	no	1

Warnings:

This is not a USPTO supplied RCE SB30 form.

Information:

5	Fee Worksheet (PTO-875)	fee-info.pdf	34261 74b2f2d30c06a84e5010adc081d6702b4c88d521	no	2

Warnings:

Information:

Total Files Size (in bytes):	945964

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	:	Customer Number:
Victor Larson	:	Confirmation Number: 3528
Serial No.: 11/679,416	:	Group Art Unit: 2453
Filed: February 27, 2007	:	Examiner: Krisna Lim
For:	:	Attorney Reference No:
METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK		077580-0015 (VRNK-1CP2DVCN)

FILED VIA EFS-WEB

RESPONSE/AMENDMENT "B"

Sir:

In response to the final Office Action dated April 8, 2010, it is respectfully requested that the time for response to the Office Action be extended for three (3) months to October 8, 2010, and reconsideration and further examination of the above-identified application are respectfully requested based on the following:

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

AMENDMENTS TO THE CLAIMS

Petitioner Apple Inc. - Exhibit 1026, p. 805

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Cancelled)

2. (Currently Amended) A method of ~~communicating~~ using a first device to communicate with a second device having a secure name, the method comprising:

from the first device, sending a message to a secure name service, the message requesting [[an]] a network address associated with the secure name of the second device;

at the first device, receiving a message containing the network address associated with the secure name of the second device; and

from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.

3. (Currently Amended) The method according to claim 2, wherein the secure name of the second device is a secure domain name~~further including supporting a plurality of services through the secure communication link~~.

4. (Previously Presented) The method according to claim 2, wherein the secure name indicates security.

5. (Currently Amended) The method according to claim 2, wherein receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form.

6. (Previously Presented) The method according to claim 5, further including decrypting the message.

7. (Currently Amended) The method according to claim 2, wherein the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed...

Petitioner Apple Inc. - Exhibit 1026, p. 806

8. (Currently Amended) The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device.

9. (Previously Presented) The method according to claim 2, further including automatically initiating the secure communication link after it is enabled.

10. (Currently Amended) The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link.

11. (Currently Amended) The method according to claim 2, wherein receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet.

12. (Previously Presented) The method according to claim 2, wherein the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols.

13. (Currently Amended) The method according to claim 2, wherein the receiving ~~an~~ and sending of messages through the secure communication link includes multiple sessions.

14. (Previously Presented) The method according to claim 2, further including supporting a plurality of services over the secure communication link.

15. (Previously Presented) The method according to claim 14, wherein the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof.

16. (Previously Presented) The method according to claim15, wherein the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof.

17. (Previously Presented) The method according to claim 15, wherein the plurality of services comprises audio, video or a combination thereof.

Petitioner Apple Inc. - Exhibit 1026, p. 807

18. (Previously Presented) The method according to claim 2, wherein the secure communication link is an authenticated link.

19. (Currently Amended) The method according to claim 2, wherein the first device is a computer, and the steps are performed on the computer.

20. (Currently Amended) The method according to claim 2, wherein the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network.

21. (Currently Amended) The method according to claim 2, further including providing an ~~unsecure~~ unsecured name associated with the device.

22. (Currently Amended) The method according to claim 2, wherein the secure name is registered prior to the step of sending a message to a secure name service.

23. (Currently Amended) The method according to claim 2, wherein the secure name of the second device is a secure, non-standard domain name.

~~wherein sending a message to a name service comprises sending a first message from a first device to the name service, the first message requesting from the name service the address associated with the secure name of the device,~~

~~wherein receiving a message comprises receiving at the first device a second message from the name service, the second message containing the address associated with the secure name of the device, and~~

~~wherein sending a message to the address comprises sending a third message from the first device to the address associated with the secure name of the device using the secure communication link.~~

24. (Currently Amended) A method ~~for~~ of using a first device to securely communicate ~~communicating~~ with a second device over~~in~~ a communication network, ~~the device having a secure name,~~ the method comprising:

at the first device requesting and obtaining registration of a secure name ~~of a~~for the first device, the secure name being associated with [[an]] a network address;

Petitioner Apple Inc. - Exhibit 1026, p. 808

receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and

sending a message securely from the first device to the second device.

25. (Currently Amended) The method according to claim 24, wherein requesting and obtaining registration of a secure name ~~of a~~ for the first device comprises ~~requesting from~~ using the first device to obtain a registration of the secure name ~~of the~~ for the first device, and wherein sending a message securely comprises sending the message from the first device to the second device using a secure communication link.

26. (Currently Amended) A method ~~for communicating~~of using a first device to communicate with a second device ~~in~~ over a communication network, ~~the device associated with a secure name and an unsecured name,~~ the method comprising:

from the first device requesting and obtaining registration of an unsecured name associated with ~~a~~the first device;

from the first device requesting and obtaining registration of a secure name associated with the first device, wherein [[an]] a unique network address corresponds to the secure name associated with the first device;

receiving at the unique network address associated with the secure name a message from a second device requesting the desire to securely communicate with the first device; and

from the first device sending a message securely from the first device to the second device.

27. (Currently Amended) The method according to claim 26,

wherein requesting and obtaining registration of an unsecured name associated with ~~a~~the first device comprises ~~requesting from~~ using the first device to obtain a registration of the unsecured name associated with the first device, and

wherein requesting and obtaining registration of a secure name associated with the first device comprises ~~requesting from~~ using the first device to obtain a registration of the secure name associated with the first device.

28. (Currently Amended) A non-transitory machine-readable medium comprising instructions for:

Petitioner Apple Inc. - Exhibit 1026, p. 809

sending a message to a secure name service, the message requesting [[an]] a network address associated with a secure name of a device;

receiving a message containing the network address associated with the secure name of the device; and

sending a message to the network address associated with the secure name of the device using a secure communication link.

29. (Currently Amended) A non-transitory machine-readable medium comprising instructions for a method ~~for~~ of communicating with a device having a secure name, the method comprising:

receiving at [[an]] a network address associated with a secure name of a first device a message from a second device requesting the desired to securely communicate with the first device, wherein the secure name of the first device is registered; and

sending a message securely from the first device to the second device.

30. (Currently Amended) A non-transitory machine-readable medium comprising instructions for a method ~~for~~ of communicating with a first device associated with a secure name and an unsecured name, the method comprising:

receiving, at [[an]] a network address corresponding to ~~a~~ the secure name associated with ~~a~~the first device, a message from a second device of the desired to securely communicate with the first device, ~~wherein an unsecured name is associated with the first device, and the secure name and the unsecured name are registered~~; and

sending a message ~~securely~~ over a secure communication link from the first device to the second device.

Petitioner Apple Inc. - Exhibit 1026, p. 810

REMARKS/ARGUMENTS

Claims 2-30 remain in the application, of which claims 2, 24, 26, 28, 29, and 30 are the independent claims. Claims 2, 3, 5, 7, 8, 10, 11, 13, 19-30 have been amended to more clearly define the invention. The changes to the claims are fully supported by the original disclosure. No new matter has been introduced into the claims. Reconsideration and further examination are respectfully requested.

The changes to the application are fully supported by the original disclosure, including, for example, original paragraphs [0313] to [0331].

Objection to the Specification

The Specification has been objected to for failing to provide support for "machine readable medium," as recited in claims 28-30, because "machine readable medium" may be defined to broadly include non-statutory subject matter. The Office Action notes that adding "non-transitory" to claims 28-30 does not raise the issue of new subject matter. Because claims 28-30 have been amended to recite "non-transitory," the Applicant respectfully submits that this objection is moot.

Rejection under 35 U.S.C. § 112, second paragraph

Claims 2-30 have been rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicant regards as the invention.. The rejection is respectfully traversed, and reconsideration and withdrawal of the § 112 rejection is respectfully requested.

Regarding claim 2, the Office Action states that it is unclear from where a message is sent. It states that is also unclear what kind of "name service" is being claimed (*i.e.*, a secure

Petitioner Apple Inc. - Exhibit 1026, p. 811

domain name service? A domain name service?). It further states that it is also unclear what kind of address is being claimed (*i.e.*, an address for a secure computer network?). It further states that it is also unclear where a message is being received.

As amended, claim 2 recites as follows:

> A method of using a first device to communicate with a second device having a secure name, the method comprising:
> from the first device, sending a message to a secure name service, the message requesting a network address associated with the secure name of the second device;
> at the first device, receiving a message containing the network address associated with the secure name of the second device; and
> from the first device, sending a message to the network address associated with the secure name of the second device using a secure communication link.

The Applicant responds to the rejections of claim 2 as follows. First, the Applicant has amended claim 2 to clarify that it is the first device that is "sending a message" and "receiving a message" to so that it can send a message over "a secure communication link."

Second, the Applicant has amended "name service" to read "secure name service." This secure name service is a service for resolving secure names into network addresses. This secure name service offers functionality that cannot be accomplished by a standard domain name service.

Third, the Applicant has amended "address" to read "network address." This network address is one that is associated with a device connected to a communications network. It is not limited to an address of a secure computer network, as suggested in the Office Action. A network address can be associated with any device registered on a network, including, but not limited to, web servers, mobile handsets, and/or computers.

The Applicant respectfully submits that, as amended, these limitations in claim 2 are not unclear. The Applicant further submits that claims 3-23, which depend on claim 2, are not

Petitioner Apple Inc. - Exhibit 1026, p. 812

unclear for similar reasons. Accordingly the Applicant respectfully requests withdrawal of these rejections and reconsideration of claims 2-23.

Regarding claim 24, the Office Action states that "secure name" is unclear, and questions whether this is a secure domain name. It further states that it is unclear what kind of address is being claimed. It further states that it is unclear what kind of the first device and second device are being claimed, and whether they are the same or different.

As amended, claim 24 recites as follows:

> A method of using a first device to securely communicate with a second device over a communication network, the method comprising:
>
> at the first device requesting and obtaining registration of a secure name for the first device, the secure name being associated with a network address;
>
> receiving at the network address associated with the secure name of the first device a message from a second device of the desire to securely communicate with the first device; and
>
> sending a message securely from the first device to the second device.

The Applicant responds to the rejection of claim 24 as follows. First, the Applicant submits that a "secure name" is a name associated with a network address of a first device. The name can be registered such that a second device can obtain the network address associated with the first device from a secure name registry and send a message to the first device. The first device can then send a secure message to the second device. The claimed "secure name" includes, but is not limited to, a secure domain name. For example, a "secure name" can be a secure non-standard domain name, such as a secure non-standard top-level domain name (*e.g.*, .scom) or a telephone number.

Second, the Applicant has amended "address" to read "network address." This network address is one that is associated with a device on a communications network. It is not limited to an address of a secure computer network, as suggested in the Office Action. A network address

Petitioner Apple Inc. - Exhibit 1026, p. 813

can be associated with any device registered on a network, including, but not limited to, web servers, mobile handsets, and computers.

Third, the Applicant submits that the first device and second device are different to the extent that they are associated with two different network addresses. These devices can include, but are not limited to, web servers, mobile handsets, and/or computers.

The Applicant respectfully submits that, as amended, these limitations in claim 24 are not unclear. The Applicant further submits that claim 25, which depends on claim 24, is not unclear for similar reasons.

Regarding claims 26-30, the Office Action states that they are also unclear because they recite similar language to claim 24. For at least the reasons stated above, the Applicant respectfully submits that claims 26-30, as amended, are similarly not unclear.

In sum, the Applicant respectfully submits that, in view of the foregoing amendments and remarks, the rejections under 35 U.S.C. § 112, second paragraph have been traversed. Accordingly, the Applicant respectfully requests reconsideration and withdrawal of these rejections.

Rejection under 35 U.S.C. § 101

Claims 28-30 have been rejected under 35 U.S.C. § 101 for claiming non-statutory subject matter. The Office Action states that claims drawn to a "machine-readable medium" includes both non-transitory tangible media and transitory propagating signals. It states that transitory embodiments are not directed to statutory subject matter.

Although the Applicant respectfully disagrees with this interpretation of "machine-readable medium," the Applicant has nevertheless amended claims 28-30 to make explicit that they are drawn to statutory subject matter, namely "non-transitory machine-readable medi[a]."

Petitioner Apple Inc. - Exhibit 1026, p. 814

Accordingly, the Applicant respectfully requests reconsideration and withdrawal of these rejections.

Non-Statutory Obviousness-Type Double Patenting Rejections

Claims 2, 24, 26, and 28-30 have been rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 7,188,180. The Applicant submits herewith a terminal disclaimer to overcome this rejection. Accordingly, the Applicant respectfully submits that this rejection has been overcome, and requests withdrawal of the rejection accordingly.

Claims 2, 24, 26, and 28-30 have been provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of copending U.S. Patent Application Serial No. 11/839,987. The Applicant submits herewith a terminal disclaimer to overcome this rejection. Accordingly, the Applicant respectfully submits that these rejections are traversed and requests withdrawal of the rejections accordingly.

The absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be other reasons for patentability of any or all claims that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede, or an actual concession of, any issue with regard to any claim, or any cited art, except as specifically stated in this paper, and the amendment or cancellation of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment or cancellation.

Petitioner Apple Inc. - Exhibit 1026, p. 815

CONCLUSION

In view of the foregoing amendments and remarks, the entire application is believed to be in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience. Should the Examiner have any questions, please call the undersigned at the phone number listed below.

Authorization is hereby given to charge our deposit account, No. 50-1133, for an Extension of Time (three-months) Under 37 CFR 1.136, and for any other fees that may be required for the prosecution of the subject application.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: October 8, 2010

/Toby H. Kusmer/

Toby Kusmer, Reg. No.: 26,418
McDERMOTT WILL & EMERY LLP
28 State Street
Boston, Massachusetts 02109
Telephone: (617) 535-4065
Facsimile: (617) 535-3800
e-mail: tkusmer@mwe.com

BST99 1659565-2.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 816

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
11/679,416	02/27/2007	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 10/08/2010	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 29	Minus	** 29	= 0	X $ =		OR	X $52=	0
Independent (37 CFR 1.16(h))	* 6	Minus	***6	= 0	X $ =		OR	X $220=	0
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/DIANE WILLIAMS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	11/679,416
Filing Date	02-27-2007
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	077580-0015

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code[3] – Number[4] – Kind Code[5] (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C1	EP0838930	4/29/1988	Digital Equipment Corporation			
	C2	EP0814589	12/29/1997	AT&T Corp.			
	C3	GB2317792	04/01/1998	Secure Computing Corporation			
	C4	WO98/27783	06/25/1998	Northern Telecom Limited			
	C5	WO99/11019	03/04/1999	V One Corp			
	C6	GB2334181	08/11/1999	NEC Technologies			
	C7	GB2340702	02/23/2000	Sun Microsystems Inc.			

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1	Baumgartner et al, "Differentiated Services: A New Approach for Quality of Service in the Internet," International Conference on High Performance Networking, 255-273 (1998)	
	D2	Chapman et al., "Domain Name System (DNS)," 278-296 (1995)	
	D4	Davila et al., "Implementation of Virtual Private Networks at the Transport Layer," M. Mambo, Y. Zheng (Eds), Information Security (Second International) Workshop, ISW' 99. Lecture Notes in Computer Science (LNCS), Vol. 1729; 85-102 (1999)	
	D5	De Raadt et al., "Cryptography in OpenBSD," 10 pages (1999)	
	D6	Eastlake, "Domain Name System Security Extensions," Internet Citation, Retrieved from the Internet: URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt (1998)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** ***(Use as many sheets as necessary)***				**Complete if Known**	
				Application Number	11/679,416
				Filing Date	02-27-2007
				First Named Inventor	Victor Larson
				Art Unit	2453
				Examiner Name	Krisna Lim
				Docket Number	077580-0015

	D8	Gunter et al., "An Architecture for Managing QoS-Enabled VRNs Over the Internet," Proceedings 24th Conference on Local Computer Networks. LCN' 99 IEEE Comput. Soc Los Alamitos, CA, pages 122-131 (1999)	
	D9	Shimizu, "Special Feature: Mastering the Internet with Windows 2000", Internet Magazine, 63:296-307 (2000)	
	D10	Stallings, "Cryptography and Network Security," Principals and Practice, 2nd Edition, pages 399-440 (1999)	
	D11	Takata, "U.S. Vendors Take Serious Action to Act Against Crackers – A Tracking Tool and a Highly Safe DNS Software are Released", Nikkei Communications, 257:87 (1997)	
	D12	Wells, Email (Lancasterb1be@mail.msn.com), Subject: "Security Icon," (1998)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** ***(Use as many sheets as necessary)***				**Complete if Known**	
				Application Number	11/679,416
				Filing Date	02-27-2007
				First Named Inventor	Victor Larson
				Art Unit	2453
				Examiner Name	Krisna Lim
				Docket Number	077580-0015

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[X] Information Disclosure Statement is being after the filing of the Request for Continued Examination filed on October 8, 2010. No fee is believed to be due. The Commissioner is hereby authorized to charge fee deficiencies to Deposit Account 50-1133.

[ ] Items contained in this Information Disclosure Statement were first cited in any communication from a foreign patent office in a counterpart foreign application.

[ ] No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned, after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of this Information Disclosure Statement

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[X] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

/Toby H. Kusmer/ Date: October 11, 2010

Toby H. Kusmer, Reg. No.: 26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02108
Tel. (617) 535-4000
Fax (617) 535-3800

BST99 1654975-1.077580.0015

Electronic Acknowledgement Receipt

EFS ID:	8596462
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Melissa Molchan
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)
Receipt Date:	11-OCT-2010
Filing Date:	27-FEB-2007
Time Stamp:	09:59:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	EP0838930A2.pdf	1724786 9a383b35683829ae78abb4965b90cde255795d93	no	34

Warnings:	
Information:	

2	Foreign Reference	EP0814589A2.pdf	1094602 10c06cd368d846b9f6c82e5622edd22ebc63e401	no	19
Warnings:					
Information:					
3	Foreign Reference	GB2317792A.pdf	1256657 d50989c41fac545a0929025d919331dfbf7136ef	no	34
Warnings:					
Information:					
4	Foreign Reference	WO9827783A1.pdf	846395 2a2ead44cf92a436d19c46f7f35211b7e6ad33cf	no	23
Warnings:					
Information:					
5	Foreign Reference	WO99011019.pdf	2034462 a88bd9be7182a86a8e75ebf9a5aa6e210b0962a5	no	60
Warnings:					
Information:					
6	Foreign Reference	GB2334181A.pdf	431753 98657594c9b37568cbca8e5569b8b1b6fd6f75a0	no	14
Warnings:					
Information:					
7	Foreign Reference	GB2340702A.pdf	1504772 b9d55f72785502abe4081ceb482776f5d62d0f15	no	36
Warnings:					
Information:					
8	NPL Documents	Baumgartner.pdf	535114 e1cfd368a442fe0e98ec5f0b34dc39d0d51aee53	no	20
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
9	NPL Documents	Chapman.pdf	1713700 39c5c492b168aa3e7de9fca2a4031545bed0e957	no	19
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					

10	NPL Documents	Davila.pdf	461212 0300df8d7b65f715e893e7e8d5e7985e93b9ed97	no	18
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
11	NPL Documents	DeRaadt.pdf	333587 fdad8832507203c9875d1e55fdc679bf42cecc48	no	10
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
12	NPL Documents	Eastlake.pdf	1007823 7f990c13c14c9426828dd74c35dd10f320f607b2	no	45
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
13	NPL Documents	Gunter.pdf	330364 b806a4f735e709274fa23d1b659fcf93f2e555a2	no	10
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
14	NPL Documents	Stallings.pdf	1451887 b32ca3a1d283b7ceeadc81e075be896ce51656dd	no	42
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
15	NPL Documents	Takata.pdf	109936 009f8475adb2a0557fdfcff79670b4a3112a0119	no	3
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
16	NPL Documents	Wells.pdf	63145 095ce48eaedeaf4359dd456e88732c1e895de5e3	no	1
Warnings:					

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
17	Information Disclosure Statement (IDS) Filed (SB/08)	IDS3.pdf	124131 eca2f5cd5c7eef1e62e1180b70b191a832e4e3d2	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
			Total Files Size (in bytes):	15024326	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 838 930 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.04.1998 Bulletin 1998/18

(51) Int. Cl.[6]: **H04L 29/06**

(21) Application number: **97118556.6**

(22) Date of filing: **24.10.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV RO SI

(30) Priority: **25.10.1996 US 738155**

(71) Applicant:
DIGITAL EQUIPMENT CORPORATION
Maynard, Massachusetts 01754 (US)

(72) Inventors:
- **Alden, Kenneth F.**
  Boylston, Massachusetts 01505 (US)
- **Lichtenberg, Mitchell P.**
  Sunnyvale, CA 94087 (US)
- **Wobber, Edward P.**
  Menlo Park, California 94025 (US)

(74) Representative: **Betten & Resch**
Reichenbachstrasse 19
80469 München (DE)

(54) Pseudo network adapter for frame capture, encapsulation and encryption

(57) A new pseudo network adapter provides an interface for capturing packets from a local communications protocol stack for transmission on the virtual private network, and includes a Dynamic Host Configuration Protocol (DHCP) server emulator, and an Address Resolution Protocol (ARP) server emulator. The new system indicates to the local communications protocol stack that nodes on a remote private network are reachable through a gateway that is in turn reachable through the pseudo network adapter. A transmit path in the system processes data packets from the local communications protocol stack for transmission through the pseudo network adapter. An encryption engine encrypts the data packets and an encapsulation engine encapsulates the encrypted data packets into tunnel data frames. The network adapter further includes an interface into a transport layer of the local communications protocol stack for capturing received data packets from the remote server node, and a receive path for processing received data packets captured from the transport layer of the local communications protocol stack. The receive path includes a decapsulation engine, and a decryption engine, and passes the decrypted, decapsulated data packets back to the local communications protocol stack for delivery to a user.

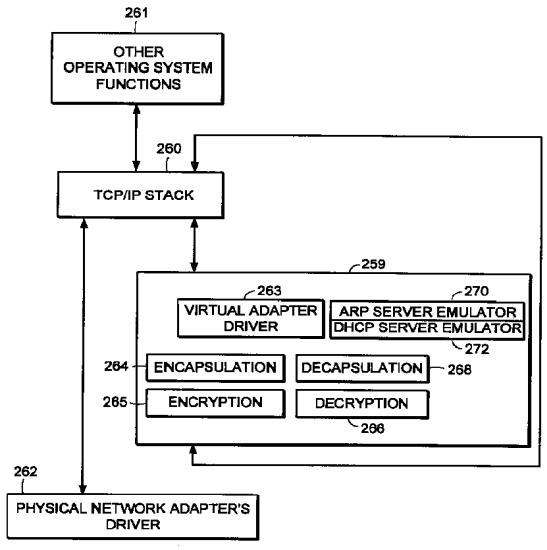


FIG. 15

EP 0 838 930 A2

Petitioner Apple Inc. - Exhibit 1026, p. 825

Description

FIELD OF THE INVENTION

The invention relates generally to establishing secure virtual private networks. The invention relates specifically to a pseudo network adapter for capturing, encapsulating and encrypting messages or frames.

BACKGROUND

In data communications it is often required that secure communications be provided between users of network stations (also referred to as "network nodes") at different physical locations. Secure communications must potentially extend over public networks as well as through secure private networks. Secure private networks are protected by "firewalls", which separate the private network from a public network. Firewalls ordinarily provide some combination of packet filtering, circuit gateway, and application gateway technology, insulating the private network from unwanted communications with the public network.

One approach to providing secure communications is to form a virtual private network. In a virtual private network, secure communications are provided by encapsulating and encrypting messages. Encapsulated messaging in general is referred to as "tunneling". Tunnels using encryption may provide protected communications between users separated by a public network, or among a subset of users of a private network.

Encryption may for example be performed using an encryption algorithm using one or more encryption "keys". When an encryption key is used, the value of the key determines how the data is encrypted and decrypted. When a public-key encryption system is used, a key pair is associated with each communicating entity. The key pair consists of an encryption key and a decryption key. The two keys are formed such that it is unfeasible to generate one key from the other. Each entity makes its encryption key public, while keeping its decryption key secret. When sending a message to node A, for example, the transmitting entity uses the public key of node A to encrypt the message, and then the message can only be decrypted by node A using node A's private key.

In a symmetric key encryption system a single key is used as the basis for both encryption and decryption. An encryption key in a symmetric key encryption system is sometimes referred to as a "shared" key. For example, a pair of communicating nodes A and B could communicate securely as follows: a first shared key is used to encrypt data sent from node A to node B, while a second shared key is to be used to encrypt data sent from node B to node A. In such a system, the two shared keys must be known by both node A and node B. More examples of encryption algorithms and keyed encryption are disclosed in many textbooks, for example "Applied Cryptography - Protocols, Algorithms, and Source Code in C", by Bruce Schneier, published by John Wiley and Sons, New York, New York, copyright 1994.

Information regarding what encryption key or keys are to be used, and how they are to be used to encrypt data for a given secure communications session is referred to as "key exchange material". Key exchange material may for example determine what keys are used and a time duration for which each key is valid. Key exchange material for a pair of communicating stations must be known by both stations before encrypted data can be exchanged in a secure communications session. How key exchange material is made known to the communicating stations for a given secure communications session is referred to as "session key establishment".

A tunnel may be implemented using a virtual or "pseudo" network adapter that appears to the communications protocol stack as a physical device and which provides a virtual private network. A pseudo network adapter must have the capability to receive packets from the communications protocol stack, and to pass received packets back through the protocol stack either to a user or to be transmitted.

A tunnel endpoint is the point at which any encryption/decryption and encapsulation/decapsulation provided by a tunnel is performed. In existing systems, the tunnel end points are pre-determined network layer addresses. The source network layer address in a received message is used to determine the "credentials" of an entity requesting establishment of a tunnel connection. For example, a tunnel server uses the source network layer address to determine whether a requested tunnel connection is authorized. The source network layer address is also used to determine which cryptographic key or keys to use to decrypt received messages.

Existing tunneling technology is typically performed by encapsulating encrypted network layer packets (also referred to as "frames") at the network layer. Such systems provide "network layer within network layer" encapsulation of encrypted messages. Tunnels in existing systems are typically between firewall nodes which have statically allocated IP addresses. In such existing systems, the statically allocated IP address of the firewall is the address of a tunnel end point within the firewall. Existing systems fail to provide a tunnel which can perform authorization based for an entity which must dynamically allocate its network layer address. This is especially problematic for a user wishing to establish a tunnel in a mobile computing environment, and who requests a dynamically allocated IP address from an Internet Service Provider (ISP).

Because existing virtual private networks are based on network layer within network layer encapsulation, they are generally only capable of providing connectionless datagram type services. Because datagram type services do not guarantee delivery of packets, existing

Petitioner Apple Inc. - Exhibit 1026, p. 826

tunnels can only easily employ encryption methods over the data contained within each transmitted packet. Encryption based on the contents of multiple packets is desirable, such as cipher block chaining or stream ciphering over multiple packets. For example, encrypted data would advantageously be formed based not only on the contents of the present packet data being encrypted, but also based on some attribute of the connection or session history between the communicating stations. Examples of encryption algorithms and keyed encryption are disclosed in many textbooks, for example "Applied Cryptography - Protocols, Algorithms, and Source Code in C", by Bruce Schneier, published by John Wiley and Sons, New York, New York, copyright 1994.

Thus there is required a new pseudo network adapter providing a virtual private network having a dynamically determined end point to support a user in a mobile computing environment. The new pseudo network adapter should appear to the communications protocol stack of the node as an interface to an actual physical device. The new pseudo network adapter should support guaranteed, in-order delivery of frames over a tunnel to conveniently support cipher block chaining mode or stream cipher encryption over multiple packets.

SUMMARY OF THE INVENTION

A new pseudo network adapter is disclosed providing a virtual private network. The new system includes an interface for capturing packets from a local communications protocol stack for transmission on the virtual private network. The interface appears to the local communications stack as a network adapter device driver for a network adapter.

The invention, in its broad form, includes a pseudo network adapter as recited in claim 1, providing a virtual network and a method therefor as recited in claim 9.

The system as described hereinafter further includes a Dynamic Host Configuration Protocol (DHCP) server emulator, and an Address Resolution Protocol (ARP) server emulator. The new system indicates to the local communications protocol stack that nodes on a remote private network are reachable through a gateway that is in turn reachable through the pseudo network adapter. The new pseudo network adapter includes a transmit path for processing data packets from the local communications protocol stack for transmission through the pseudo network adapter. The transmit path includes an encryption engine for encrypting the data packets and an encapsulation engine for encapsulating the encrypted data packets into tunnel data frames. The pseudo network adapter passes the tunnel data frames back to the local communications protocol stack for transmission to a physical network adapter on a remote server node.

Preferably, as described hereinafter, the pseudo network adapter includes a digest value in a digest field in each of the tunnel data frames. A keyed hash function is a hash function which takes data and a shared cryptographic key as inputs, and outputs a digital signature referred to as a digest. The value of the digest field is equal to an output of a keyed hash function applied to data consisting of the data packet encapsulated within the tunnel data frame concatenated with a counter value equal to a total number of tunnel data frames previously transmitted to the remote server node. In another aspect of the system, the pseudo network adapter processes an Ethernet header in each one of the captured data packets, including removing the Ethernet header.

The new pseudo network adapter further includes an interface into a transport layer of the local communications protocol stack for capturing received data packets from the remote server node, and a receive path for processing received data packets captured from the transport layer of the local communications protocol stack. The receive path includes a decapsulation engine, and a decryption engine, and passes the decrypted, decapsulated data packets back to the local communications protocol stack for delivery to a user.

Thus there is disclosed a new pseudo network adapter providing a virtual private network having dynamically determined end points to support users in a mobile computing environment. The new pseudo network adapter provides a system for capturing a fully formed frame prior to transmission. The new pseudo network adapter appears to the communications protocol stack of the station as an interface to an actual physical device. The new pseudo network adapter further includes encryption capabilities to conveniently provide secure communications between tunnel end points using stream mode encryption or cipher block chaining over multiple packets.

BRIEF DESCRIPTION OF THE DRAWINGS

A more detailed understanding of the invention may be had from the following description of a preferred embodiment, given by way of example and to be understood in conjunction with the accompanying drawing in which:

- Fig. 1 is a block diagram showing the Open Systems Interconnection (OSI) reference model;
- Fig. 2 is a block diagram showing the TCP/IP internet protocol suite;
- Fig. 3 is a block diagram showing an examplary embodiment of a tunnel connection across a public network between two tunnel servers;
- Fig. 4 is a flow chart showing an examplary embodiment of steps performed to establish a tunnel con-

Petitioner Apple Inc. - Exhibit 1026, p. 827

nection;

- Fig. 5 is a flow chart showing an examplary embodiment of steps performed to perform session key management for a tunnel connection;
- Fig. 6 is a block diagram showing an examplary embodiment of a relay frame;
- Fig. 7 is a block diagram showing an examplary embodiment of a connection request frame;
- Fig. 8 is a block diagram showing an examplary embodiment of a connection response frame;
- Fig. 9 is a block diagram showing an examplary embodiment of a data frame;
- Fig. 10 is a block diagram showing an examplary embodiment of a close connection frame;
- Fig. 11 is a state diagram showing an examplary embodiment of a state machine forming a tunnel connection in a network node initiating a tunnel connection;
- Fig. 12 is a state diagram showing an examplary embodiment of a state machine forming a tunnel connection in a server computer;
- Fig. 13 is a state diagram showing an examplary embodiment of a state machine forming a tunnel connection in a relay node;
- Fig. 14 is a block diagram showing an examplary embodiment of a tunnel connection between a client computer (tunnel client) and a server computer (tunnel server);
- Fig. 15 is a block diagram showing an examplary embodiment of a pseudo network adapter;
- Fig. 16 is a block diagram showing an examplary embodiment of a pseudo network adapter;
- Fig. 17 is a flow chart showing steps performed by an examplary embodiment of a pseudo network adapter during packet transmission;
- Fig. 18 is a flow chart showing steps performed by an examplary embodiment of a pseudo network adapter during packet receipt;
- Fig. 19 is a data flow diagram showing data flow in an examplary embodiment of a pseudo network adapter during packet transmission;
- Fig. 20 is a data flow diagram showing data flow in an examplary embodiment of a pseudo network adapter during packet receipt;
- Fig. 21 is a diagram showing the movement of encrypted and unencrypted data in an examplary embodiment of a system including a pseudo network adapter;
- Fig. 22 is a diagram showing the movement of encrypted and unencrypted data in an examplary embodiment of a system including a pseudo network adapter; and
- Fig. 23 is a flow chart showing steps initialization of an examplary embodiment of a system including a pseudo network adapter.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Now with reference to Fig. 1 there is described for purposes of explanation, communications based on the Open Systems Interconnection (OSI) reference model. In Fig. 1 there is shown communications 12 between a first protocol stack 10 and a second protocol stack 14. The first protocol stack 10 and second protocol stack 14 are implementations of the seven protocol layers (Application layer, Presentation layer, Session layer, Transport layer, Network layer, Data link layer, and Physical layer) of the OSI reference model. A protocol stack implementation is typically in some combination of software and hardware. Descriptions of the specific services provided by each protocol layer in the OSI reference model are found in many text books, for example "Computer Networks", Second Edition, by Andrew S. Tannenbaum, published by Prentice-Hall, Englewood Cliffs, New Jersey, copyright 1988.

As shown in Fig. 1, data 11 to be transmitted from a sending process 13 to a receiving process 15 is passed down through the protocol stack 10 of the sending process to the physical layer 9 for transmission on the data path 7 to the receiving process 15. As the data 11 is passed down through the protocol stack 10, each protocol layer prepends a header (and possibly also appends a trailer) portion to convey information used by that protocol layer. For example, the data link layer 16 of the sending process wraps the information received from the network layer 17 in a data link header 18 and a data link layer trailer 20 before the message is passed to the physical layer 9 for transmission on the actual transmission path 7.

Fig. 2 shows the TCP/IP protocol stack. Some protocol layers in the TCP/IP protocol stack correspond with layers in the OSI protocol stack shown in Fig. 1. The detailed services and header formats of each layer in the TCP/IP protocol stack are described in many texts, for example "Internetworking with TCP/IP, Vol. 1: Principles, Protocols, and Architecture", Second Edi-

Petitioner Apple Inc. - Exhibit 1026, p. 828

tion, by Douglas E. Comer, published by Prentice-Hall, Englewood Cliffs, New Jersey, copyright 1991. The Transport Control Protocol (TCP) 22 corresponds to the Transport layer in the OSI reference model. The TCP protocol 22 provides a connection-oriented, end to end transport service with guaranteed, in-sequence packet delivery. In this way the TCP protocol 22 provides a reliable, transport layer connection.

The IP protocol 26 corresponds to the Network layer of the OSI reference model. The IP protocol 26 provides no guarantee of packet delivery to the upper layers. The hardware link level and access protocols 32 correspond to the Data link and Physical layers of the OSI reference model.

The Address Resolution Protocol (ARP) 28 is used to map IP layer addresses (referred to as "IP addresses") to addresses used by the hardware link level and access protocols 32 (referred to as "physical addresses" or "MAC addresses"). The ARP protocol layer in each network station typically contains a table of mappings between IP addresses and physical addresses (referred to as the "ARP cache"). When a mapping between an IP address and the corresponding physical address is not known, the ARP protocol 28 issues a broadcast packet (an "ARP request" packet) on the local network. The ARP request indicates an IP address for which a physical address is being requested. The ARP protocols 28 in each station connected to the local network examine the ARP request, and if a station recognizes the IP address indicated by the ARP request, it issues a response (an "ARP response" or "ARP reply" packet) to the requesting station indicating the responder's physical address. The requesting ARP protocol reports the received physical address to the local IP layer which then uses it to send datagrams directly to the responding station. As an alternative to having each station respond only for its own IP address, an ARP server may be used to respond for a set of IP addresses it stores internally, thus potentially eliminating the requirement of a broadcast request. In that case, the ARP request can be sent directly to the ARP server for physical addresses corresponding to any IP address mappings stored within the ARP server.

At system start up, each station on a network must determine an IP address for each of its network interfaces before it can communicate using TCP/IP. For example, a station may need to contact a server to dynamically obtain an IP address for one or more of its network interfaces. The station may use what is referred to as the Dynamic Host Configuration Protocol (DHCP) to issue a request for an IP address to a DHCP server. For example, a DHCP module broadcasts a DHCP request packet at system start up requesting allocation of an IP address for an indicated network interface. Upon receiving the DHCP request packet, the DHCP server allocates an IP address to the requesting station for use with the indicated network interface. The requesting station then stores the IP address in the response from the server as the IP address to associate with that network interface when communicating using TCP/IP.

Fig. 3 shows an example configuration of network nodes for which the presently disclosed system is applicable. In the example of Fig. 3, the tunnel server A is an initiator of the tunnel connection. As shown in Fig. 3, the term "tunnel relay" node is used to refer to a station which forwards data packets between transport layer connections (for example TCP connections).

For example, in the present system a tunnel relay may be dynamically configured to forward packets between transport layer connection 1 and transport layer connection 2. The tunnel relay replaces the header information of packets received over transport layer connection 1 with header information indicating transport layer connection 2. The tunnel relay can then forward the packet to a firewall, which may be conveniently programmed to pass packets received over transport layer connection 2 into a private network on the other side of the firewall. In the present system, the tunnel relay dynamically forms transport layer connections when a tunnel connection is established. Accordingly the tunnel relay is capable of performing dynamic load balancing or providing redundant service for fault tolerance over one or more tunnel servers at the time the tunnel connection is established.

Fig. 3 shows a Tunnel Server A 46 in a private network N1 48, physically connected with a first Firewall 50. The first Firewall 50 separates the private network N1 48 from a public network 52, for example the Internet. The first Firewall 50 is for example physically connected with a Tunnel Relay B 54, which in turn is virtually connected through the public network 52 with a Tunnel Relay C. The connection between Tunnel Relay B and Tunnel Relay C may for example span multiple intervening forwarding nodes such as routers or gateways through the public network 52.

The Tunnel Relay C is physically connected with a second Firewall 58, which separates the public network 52 from a private network N2 60. The second Firewall 58 is physically connected with a Tunnel Server D 62 on the private network N2 60. During operation of the elements shown in Fig. 3, the Tunnel Server D 62 provides routing of IP packets between the tunnel connection with Tunnel Server A 46 and other stations on the private network N2 60. In this way the Tunnel Server D 62 acts as a router between the tunnel connection and the private network N2 60.

During operation of the elements shown in Fig. 3, the present system establishes a tunnel connection between the private network N1 48 and the private network N2 60. The embodiment of Fig. 3 thus eliminates the need for a dedicated physical cable or line to provide secure communications between the private network 48 and the private network 60. The tunnel connection between Tunnel Server A 46 and Tunnel Server D 62 is

Petitioner Apple Inc. - Exhibit 1026, p. 829

composed of reliable, pair-wise transport layer connections between Tunnel Server A 46 (node "A"), Tunnel Relay B 54 (node "B"), Tunnel Relay C 56 (node "C"), and Tunnel Server D 62 (node "D"). For example, such pair-wise connections may be individual transport layer connections between each node A and node B, node B and node C, and node C and node D. In an alternative embodiment, as will be described below, a tunnel connection may alternatively be formed between a standalone PC in a public network and a tunnel server within a private network.

Fig. 4 and Fig. 5 show an example embodiment of steps performed during establishment of the tunnel connection between Tunnel Server A 46 (node "A") and Tunnel Server D 62 (node "D") as shown in Fig. 3. Prior to the steps shown in Fig. 4, node A selects a tunnel path to reach node D. The tunnel path includes the tunnel end points and any intervening tunnel relays. The tunnel path is for example predetermined by a system administrator for node A. Each tunnel relay along the tunnel path is capable of finding a next node in the tunnel path, for example based on a provided next node name (or "next node arc"), using a predetermined naming convention and service, for example the Domain Name System (DNS) of the TCP/IP protocol suite.

During the steps shown in Fig. 4, each of the nodes A, B and C perform the following steps:

- resolve the node name of the next node in the tunnel path, for example as found in a tunnel relay frame;

- establish a reliable transport layer (TCP) connection to the next node in the tunnel path;

- forward the tunnel relay frame down the newly formed reliable transport layer connection to the next node in the tunnel path.

As shown for example in Fig. 4, at step 70 node A establishes a reliable transport layer connection with node B. At step 72 node A identifies the next downstream node to node B by sending node B a tunnel relay frame over the reliable transport layer connection between node A and node B. The tunnel relay frame contains a string buffer describing all the nodes along the tunnel path (see below description of an example tunnel relay frame format). At step 74, responsive to the tunnel relay frame from node A, node B searches the string buffer in the relay frame to determine if the string buffer includes node B's node name. If node B finds its node name in the string buffer, it looks at the next node name in the string buffer to find the node name of the next node in the tunnel path.

Node B establishes a reliable transport layer connection with the next node in the tunnel path, for example node C. Node B further forms an association between the reliable transport layer connection between Node A and Node B, over which the relay frame was received, and the newly formed reliable transport layer connection between Node B and Node C, and as a result forwards subsequent packets received over the reliable transport layer connection with Node A onto the reliable transport layer connection with Node C, and vice versa. At step 76 node B forwards the tunnel relay frame on the newly formed reliable transport layer connection to node C.

At step 78, responsive to the relay frame forwarded from node B, node C determines that the next node in the tunnel path is the last node in the tunnel path, and accordingly is a tunnel server. Node C may actively determine whether alternative tunnel servers are available to form the tunnel connection. Node C may select one of the alternative available tunnel servers to form the tunnel connection in order to provide load balancing or fault tolerance. As a result node C may form a transport layer connections with one of several available tunnel servers, for example a tunnel server that is relatively underutilized at the time the tunnel connection is established. In the example embodiment, node C establishes a reliable transport layer connection with the next node along the tunnel path, in this case node D.

Node C further forms an association between the reliable transport layer connection between Node B and Node C, over which the relay frame was received, and the newly formed reliable transport layer connection between Node C and Node D, and as a result forwards subsequent packets received over the reliable transport layer connection with Node B to the reliable transport layer connection with Node D, and vice versa. At step 80 node C forwards the relay frame to node D on the newly formed reliable transport layer connection.

Fig. 5 shows an example of tunnel end point authentication and sharing of key exchange material provided by the present system. The present system supports passing authentication data and key exchange material through the reliable transport layer connections previously established on the tunnel path. The following are provided by use of a key exchange/authentication REQUEST frame and a key exchange/authentication RESPONSE frame:

a) mutual authentication of both endpoints of the tunnel connection;

b) establishment of shared session encryption keys and key lifetimes for encrypting/authenticating subsequent data sent through the tunnel connection;

d) agreement on a shared set of cryptographic transforms to be applied to subsequent data; and

e) exchange of any other connection-specific data between the tunnel endpoints, for example strength and type of cipher to be used, any compression of the data to be used, etc. This data can also be used

Petitioner Apple Inc. - Exhibit 1026, p. 830

by clients of this protocol to qualify the nature of the authenticated connection.

At step 90 a key exchange/authentication request frame is forwarded over the reliable transport layer connections formed along the tunnel path from node A to node D. At step 92, a key exchange/authentication response frame is forwarded from node D back to node A through the reliable transport layer connections. The attributes exchanged using the steps shown in Fig. 5 may be used for the lifetime of the tunnel connection. In an alternative embodiment the steps shown in Fig. 5 are repeated as needed for the tunnel end points to exchange sufficient key exchange material to agree upon a set of session parameters for use during the tunnel connection such as cryptographic keys, key durations, and choice of encryption/decryption algorithms.

Further in the disclosed system, the names used for authentication and access control with regard to node A and node D need not be the network layer address or physical address of the nodes. For example, in an alternative embodiment where the initiating node sending the tunnel relay frame is a stand-alone PC located within a public network, the user's name may be used for authentication and/or access control purposes. This provides a significant improvement over existing systems which base authorization on predetermined IP addresses.

Fig. 6 shows the format of an example embodiment of a tunnel relay frame. The tunnel frame formats shown in Figs. 6, 7, 8 and 9 are encapsulated within the data portion of a transport layer (TCP) frame when transmitted. Alternatively, another equivalent, connection-oriented transport layer protocol having guaranteed, in-sequence frame delivery may be used. The example TCP frame format, including TCP header fields, is conventional and not shown.

The field 100 contains a length of the frame. The field 102 contains a type of the frame, for example a type of RELAY. The field 104 contains a tunnel protocol version number. The field 106 contains an index into a string buffer field 112 at which a name of the originating node is located, for example a DNS host name of the node initially issuing the relay frame (node A in Fig. 3). The fields following the origin index field 106 contain indexes into the string buffer 112 at which names of nodes along the tunnel path are located. For example each index may be the offset of a DNS host name within the string buffer 112. In this way the field 108 contains the index of the name of the first node in the tunnel path, for example node B (Fig. 3). The field 110 contains the index of the name of the second node in the tunnel path, etc. The field 112 contains a string of node names of nodes in the tunnel path.

During operation of the present system, the initiating node, for example node A as shown in Fig. 3, transmits a tunnel relay frame such as the tunnel relay frame shown in Fig. 6. Node A sends the tunnel relay frame to the first station along the tunnel path, for example node B (Fig. 3), over a previously established reliable transport layer connection. Node B searches the string buffer in the tunnel relay frame to find its node name, for example its DNS host name. Node B finds its node name in the string buffer indexed by path index 0, and then uses the contents of path index 1 110 to determine the location within the string buffer 112 of the node name of the next node along the tunnel path. Node B uses this node name to establish a reliable transport layer connection with the next node along the tunnel path. Node B then forwards the relay frame to the next node. This process continues until the end node of the tunnel route, for example tunnel server D 62 (Fig. 3) is reached.

Fig. 7 shows the format of an example embodiment of a key exchange/key authentication request frame. The field 120 contains a length of the frame. The field 122 contains a type of the frame, for example a type of REQUEST indicating a key exchange/key authentication request frame. The field 124 contains a tunnel protocol version number. The field 126 contains an offset of the name of the entity initiating the tunnel connection, for example the name of a user on the node originally issuing the request frame. This name and key exchange material in the request frame are used by the receiving tunnel end point to authenticate the key exchange/authentication REQUEST. The name of the entity initiating the tunnel connection is also use to authorize any subsequent tunnel connection, based on predetermined security policies of the system. The field 128 contains an offset into the frame of the node name of the destination node, for example the end node of the tunnel shown as node D 62 in Fig. 3.

The field 130 contains an offset into the frame at which key exchange data as is stored, for example within the string buffer field 138. The key exchange data for example includes key exchange material used to determine a shared set of encryption parameters for the life of the tunnel connection such as cryptographic keys and any validity times associated with those keys. The key exchange data, as well as the field 132, further include information regarding any shared set of cryptographic transforms to be used and any other connection-specific parameters, such as strength and type of cipher to be used, type of compression of the data to be used, etc. The field 134 contains flags, for example indicating further information about the frame. The field 136 contains client data used in the tunnel end points to configure the local routing tables so that packets for nodes reachable through the virtual private network are sent through the pseudo network adapters. In an example embodiment, the string buffer 138 is encrypted using a public encryption key of the receiving tunnel end point.

During operation of the present system, one of the end nodes of the tunnel sends a key exchange/authentication REQUEST frame as shown in Fig. 7 to the other end node of the tunnel in order to perform key exchange and authentication as described in step 90 of Fig. 5.

Petitioner Apple Inc. - Exhibit 1026, p. 831

Fig. 8 shows the format of an example embodiment of a key exchange/key authentication response frame, referred to as a connection RESPONSE frame. The field 150 contains a length of the frame. The field 152 contains a type of the frame, for example a type of connection RESPONSE indicating a key exchange/key authentication request frame. The field 154 contains a tunnel protocol version number.

The field 156 contains an offset into the frame at which key exchange data as is stored, for example within the string buffer field 163. The key exchange data for example includes key exchange material to be used for encryption/decryption over the life of the tunnel connection and any validity times associated with that key exchange material. The key exchange data, as well as the field 158, further includes information regarding any shared set of cryptographic transforms to be applied to subsequent data and any other connection-specific parameters, such as strength and type of cipher to be used, any compression of the data to be used, etc. The field 160 contains flags, for example indicating other information about the frame. The client data field 162 contains data used by the pseudo network adapters in the tunnel end points to configure the local routing tables so that packets for nodes in the virtual private network are sent through the pseudo network adapters. The string buffer includes key exchange material. The string buffer is for example encrypted using a public encryption key of the receiving tunnel end point, in the this case the initiator of the tunnel connection.

During operation of the present system, one of the end nodes of the tunnel sends a key exchange/authentication RESPONSE frame as shown in Fig. 7 to the other end node of the tunnel in order to perform key exchange and authentication as described in step 92 of Fig. 5.

Fig. 9 shows the format of an example embodiment of an tunnel data frame used to communicate through a tunnel connection. Fig. 9 shows how an IP datagram may be encapsulated within a tunnel frame by the present system for secure communications through a virtual private network. The field 170 contains a length of the frame. The field 172 contains a type of the frame, for example a type of DATA indicating a tunnel data frame. The field 174 contains a tunnel protocol version number.

The fields 176, 178 and 182 contain information regarding the encapsulated datagram. The field 180 contains flags indicating information regarding the frame. The field 184 contains a value indicating the length of the optional padding 189 at the end of the frame. The frame format allows for optional padding in the event that the amount of data in the frame needs to be padded to an even block boundary for the purpose of being encrypted using a block cipher. The field 186 contains a value indicating the length of the digest field 187.

The data frame format includes a digital signature generated by the transmitting tunnel end point referred to as a "digest". The value of the digest ensures data integrity, for example by detecting invalid frames and replays of previously transmitted valid frames. The digest is the output of a conventional keyed cryptographic hash function applied to both the encapsulated datagram 190 and a monotonically increasing sequence number. The resulting hash output is passed as the value of the digest field 187. The sequence number is not included in the data frame. In the example embodiment, the sequence number is a counter maintained by the transmitter (for example node A in Fig. 3) of all data frames sent to the receiving node (for example node D in Fig. 3) since establishment of the tunnel connection.

In order to determine if the data frame is invalid or a duplicate, the receiving node decrypts the encapsulated datagram 190, and applies the keyed cryptographic hash function (agreed to by the tunnel end nodes during the steps shown in Fig. 5) to both the decrypted encapsulated datagram and the value of a counter indicating the number of data frames received from the transmitter since establishment of the tunnel connection. For example the keyed hash function is applied to the datagram concatenated to the counter value. If the resulting hash output matches the value of the digest field 187, then the encapsulated datagram 190 was received correctly and is not a duplicate. If the hash output does not match the value of the digest field 187, then the integrity check fails, and the tunnel connection is closed. The field 188 contains an encrypted network layer datagram, for example an encrypted IP datagram.

The encapsulated datagram may be encrypted using various encryption techniques. An example embodiment of the present system advantageously encrypts the datagram 190 using either a stream cipher or cipher block chaining encryption over all data transmitted during the life of the tunnel connection. This is enabled by the reliable nature of the transport layer connections within the tunnel connection. The specific type of encryption and any connection specific symmetric encryption keys used is determined using the steps shown in Fig. 5. The fields in the tunnel data frame other than the encapsulated datagram 188 are referred to as the tunnel data frame header fields.

Fig. 10 is a block diagram showing an example embodiment of a "close connection" frame. The field 190 contains the length of the frame. The field 191 contains a frame type, for example having a value equal to CLOSE. Field 192 contains a value equal to the current protocol version number of the tunnel protocol. The field 193 contains a status code indicating the reason the tunnel connection is being closed.

During operation of the present system, when end point of a tunnel connection determines that the tunnel connection should be closed, a close connection frame as shown in Fig. 10 is transmitted to the other end point of the tunnel connection. When a close connection close frame is received, the receiver closes the tunnel

Petitioner Apple Inc. - Exhibit 1026, p. 832

connection and no further data will be transmitted or received through the tunnel connection.

Fig. 11 is a state diagram showing an example embodiment of forming a tunnel connection in a node initiating a tunnel connection. In Fig. 11, Fig. 12, and Fig. 13, states are indicated by ovals and actions or events are indicated by rectangles. For example the tunnel server node A as shown in Fig. 3 may act as a tunnel connection initiator when establishing a tunnel connection with the tunnel server node D. Similarly the client system 247 in Fig. 14 may act as a tunnel connection initiator when establishing a tunnel connection with the tunnel server. The tunnel initiator begins in an idle state 194. Responsive to an input from a user indicating that a tunnel connection should be established, the tunnel initiator transitions from the idle state 194 to a TCP Open state 195. In the TCP Open state 195, the tunnel initiator establishes a reliable transport layer connection with a first node along the tunnel path. For example, the tunnel initiator opens a socket interface associated with a TCP connection to the first node along the tunnel path. In Fig. 3 node A opens a socket interface associated with a TCP connection with node B.

Following establishment of the reliable transport layer connection in the TCP Open state 195, the tunnel initiator enters a Send Relay state 197. In the Send Relay state 197, the tunnel initiator transmits a relay frame at 198 over the reliable transport layer connection. Following transmission of the relay frame, the tunnel initiator enters the connect state 199. If during transmission of the relay frame there is a transmission error, the tunnel initiator enters the Network Error state 215 followed by the Dying state 208. In the Dying state 208, the tunnel initiator disconnects the reliable transport layer connection formed in the TCP Open state 195, for example by disconnecting a TCP connection with Node B. Following the disconnection at 209, the tunnel initiator enters the Dead state 210. The tunnel initiator subsequently transitions back to the Idle state 194 at a point in time predetermined by system security configuration parameters.

In the Connect state 199, the tunnel initiator sends a key exchange/authentication REQUEST frame at 200 to the tunnel server. Following transmission of the key exchange/authentication REQUEST frame 200, the tunnel initiator enters the Response Wait state 201. The tunnel initiator remains in the Response Wait state 201 until it receives a key exchange/authentication RESPONSE frame 202 from the tunnel server. After the key exchange/authentication RESPONSE frame is received at 202, the tunnel initiator enters the Authorized state 203, in which it may send or receive tunnel data frames. Upon receipt of a CLOSE connection frame at 216 in the Authorized state 203, the tunnel initiator transitions to the Dying state 208.

Upon expiration of a session encryption key at 211, the tunnel initiator enters the Reconnect state 212, and sends a CLOSE connection frame at 213 and disconnects the TCP connection with the first node along the tunnel path at 214. Subsequently the tunnel initiator enters the TCP Open state 195.

If during the authorized state 203, a local user issues an End Session command at 204, or there is a detection of an authentication or cryptography error in a received data frame at 205, the tunnel initiator enters the Close state 206. During the Close state 206 the tunnel initiator sends a CLOSE connection frame at 207 to the tunnel server. The tunnel initiator then enters the Dying state at 208.

Figure 12 is a state diagram showing the states within an example embodiment of a tunnel server, for example node D in Fig. 3 or tunnel server 253 in Fig. 14. The tunnel server begins in an Accept Wait state 217. In the Accept Wait state 217, the tunnel server receives a request for a reliable transport layer connection, for example a TCP connection reguest 218 from the last node in the tunnel path prior to the tunnel server, for example Node C in Fig. 3. In response to a TCP connection request 218 the tunnel server accepts the request and establishes a socket interface associated with the resulting TCP connection with Node C.

Upon establishment of the TCP connection with the last node in the tunnel path prior to the tunnel server, the tunnel server enters the Receive Relay state 219. In the Receive Relay state 219, the tunnel server waits to receive a relay frame at 220, at which time the tunnel server enters the Connect Wait state 221. If there is some sort of network error 234 during receipt of the relay frame at 219, the tunnel server enters the Dying state 230. During the Dying state 230 the tunnel server disconnects at 231 the transport layer connection with the last node in the tunnel path prior to the tunnel server. After disconnecting the connection, the tunnel server enters the Dead state 232.

In the Connect Wait state 221, the tunnel server waits for receipt of a key exchange/authentication REQUEST frame at 222. Following receipt of the key exchange/authentication REQUEST frame at 222, the tunnel server determines whether the requested tunnel connection is authorized at step 223. The determination of whether the tunnel connection is authorized is based on a name of the tunnel initiator, and the key exchange material within the key exchange/authentication REQUEST frame.

If the requested tunnel connection is authorized the tunnel server sends a key exchange/authentication RESPONSE frame at 224 back to the tunnel initiator. If the requested tunnel connection is not authorized, the tunnel server enters the Close state 228, in which it sends a close connection frame at 229 to the tunnel client. Following transmission of the CLOSE connection frame at 229, the tunnel server enters the Dying state 230.

If the requested tunnel connection is determined to be authorized at step 223, the tunnel server enters the Authorized state 225. In the Authorized state, the tunnel

Petitioner Apple Inc. - Exhibit 1026, p. 833

server transmits and receives tunnel data frames between itself and the tunnel initiator. If during the Authorized state 225, the tunnel server receives a CLOSE connection frame at 233, the tunnel server transitions to the Dying state 230. If during the authorized state 225, the tunnel server receives an end session command from a user at 226, then the tunnel server transitions to the Close state 228, and transmits a close connection frame at 229 to the tunnel initiator. If the tunnel server in the Authorized state 225 detects an integrity failure in a received packet, the tunnel server transitions to the Close state 228. In the close state 228 the tunnel server sends a CLOSE connection frame at 229 and subsequently enters the Dying state 230.

Fig. 13 is a state diagram showing an example embodiment of a state machine within a tunnel relay node. The tunnel relay node begins in an Accept Wait state 235. When a request is received to form a reliable transport layer connection at 236, a reliable transport layer connection is accepted with the requesting node. For example, a TCP connection is accepted between the relay node and the preceding node in the tunnel path.

The relay node then transitions to the Receive Relay state 237. During the Receive Relay state 237, the relay node receives a relay frame at 238. Following receipt of the relay frame at 238, the relay node determines what forwarding address should be used to forward frames received from the TCP connection established responsive to the TCP connect event 236. If the next node in the tunnel path is a tunnel server, the forwarding address may be selected at 239 so as to choose an underutilized tunnel server from a group of available tunnel servers or to choose an operational server where others are not operational.

Following determination of the forwarding address or addresses in step 239, the relay node enters the Forward Connect state 240. In the Forward Connect state 240, the relay node establishes a reliable transport layer connection with the node or nodes indicated by the forwarding address or addresses determined in step 239.

Following establishment of the new connection at event 241, the tunnel relay enters the Forward state 242. During the Forward state 242, the relay node forwards all frames between the connection established at 236 and those connections established at 241. Upon detection of a network error or receipt of a frame indicating a closure of the tunnel connection at 243, the tunnel relay enters the Dying state 244. Following the Dying state 244, the relay node disconnects any connections established at event 241. The relay node then enters the Dead state 246.

Fig. 14 shows an example embodiment of a virtual private network 249 formed by a pseudo network adapter 248 and a tunnel connection between a tunnel client 247 and a tunnel server 253 across a public network 251. The tunnel server 253 and tunnel client 247 are for example network stations including a CPU or microprocessor, memory, and various I/O devices. The tunnel server 253 is shown physically connected to a private LAN 256 including a Network Node 1 257 and a Network Node 2 258, through a physical network adapter 254. The tunnel server 253 is further shown physically connected with a firewall 252 which separates the private LAN 256 from the public network 251. The firewall 252 is physically connected with the public network 251. The tunnel server 253 is further shown including a pseudo network adapter 255. The client system 247 is shown including a physical network adapter 250 physically connected to the public network 251.

During operation of the elements shown in Fig. 14, nodes within the virtual private network 249 appear to the tunnel client 247 as if they were physically connected to the client system through the pseudo network adapter 248. Data transmissions between the tunnel client and any nodes that appear to be within the virtual private network are passed through the pseudo network adapter 248. Data transmissions between the tunnel client 247 and the tunnel server 253 are physically accomplished using a tunnel connection between the tunnel client 247 and the tunnel server 253.

Fig. 15 shows elements in an example embodiment of a pseudo network adapter such as the pseudo network adapter 248 in Fig. 14. In an example embodiment the elements shown in Fig. 15 are implemented as software executing on the tunnel client 247 as shown in Fig. 14. In Fig. 15 there is shown a pseudo network adapter 259 including a virtual adapter driver interface 263, an encapsulation engine 264, an encryption engine 265, a decapsulation engine 268, and a decryption engine 266. Further shown in the pseudo network adapter 259 are an ARP server emulator 270 and a Dynamic Host Configuration Protocol (DHCP) server emulator.

The pseudo network adapter 259 is shown interfaced to a TCP/IP protocol stack 260, through the virtual adapter driver interface 260. The TCP/IP protocol stack 260 is shown interfaced to other services in an operating system 261, as well as a physical network adapter's driver 262. The physical network adapter's driver 262 is for example a device driver which controls the operation of a physical network adapter such as physical network adapter 250 as shown in Fig. 14.

During operation of the elements shown in Fig. 15, the pseudo network adapter 259 registers with the network layer in the TCP/IP stack 260 that it is able to reach the IP addresses of nodes within the virtual private network 249 as shown in Fig. 14. For example, the pseudo network adapter on the client system registers that it can reach the pseudo network adapter on the server. Subsequently, a message from the tunnel client addressed to a node reachable through the virtual private network will be passed by the TCP/IP stack to the pseudo network adapter 259. The pseudo network adapter 259 then encrypts the message, and encapsulates the message into a tunnel data frame. The pseudo network adapter 259 then passes the tunnel data frame

Petitioner Apple Inc. - Exhibit 1026, p. 834

back to the TCP/IP protocol stack 260 to be sent through to the physical network adapter in the tunnel server. The tunnel server passes the received data frame to the pseudo network adapter in the server, which de-encapsulates and decrypts the message.

Fig. 16 shows a more detailed example embodiment of a pseudo network adapter 280. The pseudo network adapter 280 includes a virtual network adapter driver interface 288. The transmit path 290 includes an encryption engine 292, and an encapsulation engine 294. The encapsulation engine 294 is interfaced with a TCP/IP transmit interface 312 within a TCP/IP protocol stack, for example a socket interface associated with the first relay node in the tunnel path, or with the remote tunnel end point if the tunnel path includes no relays.

In the example embodiment of Fig. 16, the pseudo network adapter 280 appears to the TCP/IP protocol stack 282 as an Ethernet adapter. Accordingly, ethernet packets 286 for a destination addresses understood by the TCP/IP protocol stack to be reachable through the virtual private network are passed from the TCP/IP protocol stack 282 to the virtual network adapter interface 288 and through the transmit path 290. Similarly, ethernet packets 284 received through the pseudo network adapter 280 are passed from the receive path 296 to the virtual network adapter interface 288 and on to the TCP/IP protocol stack 282.

Further shown in the pseudo network adapter 280 of Fig. 16 is a receive path 296 having a decryption engine 298 interfaced to the virtual network adapter interface 288 and a decapsulation engine 300. The decapsulation engine 300 in turn is interfaced to a TCP/IP receive function 314 in the TCP/IP protocol stack 282, for example a socket interface associated with the first relay in the tunnel path, or with the remote tunnel end point if the tunnel path includes no relays. The pseudo network adapter 280 further includes an ARP server emulator 304 and a DHCP server emulator 306. ARP and DHCP request packets 302 are passed to the ARP server emulator 304 and DHCP server emulator 306 respectively. When a received packet is passed from the receive path 296 to the TCP/IP stack 282, a receive event must be indicated to the TCP/IP stack 282, for example through an interface such the Network Device Interface Specification (NDIS), defined by Microsoft™ Corporation.

Also in Fig. 16 is shown is an operating system 310 coupled with the TCP/IP protocol stack 282. The TCP/IP protocol stack 282 is generally considered to be a component part of the operating system. The operating system 310 in Fig. 16 is accordingly the remaining operating system functions and procedures outside the TCP/IP protocol stack 282. A physical network adapter 308 is further shown operated by the TCP/IP protocol stack 282.

During operation of the elements shown in Fig. 16, a user passes data for transmission to the TCP/IP protocol stack 282, and indicates the IP address of the node to which the message is to be transmitted, for example through a socket interface to the TCP layer. The TCP/IP protocol stack 282 then determines whether the destination node is reachable through the virtual private network. If the message is for a node that is reachable through the virtual private network, the TCP/IP protocol stack 282 an ethernet packet 286 corresponding to the message to the pseudo network adapter 280. The pseudo network adapter 280 then passes the ethernet packet 286 through the transmit path, in which the ethernet packet is encrypted and encapsulated into a tunnel data frame. The tunnel data frame is passed back into the TCP/IP protocol stack 282 through the TCP/IP transmit function 312 to be transmitted to the tunnel server through the tunnel connection. In an example embodiment, a digest value is calculated for the tunnel data frame before encryption within the transmit path within the pseudo network adapter.

Further during operation of the elements shown in Fig. 16, when the TCP/IP protocol stack 282 receives a packet from the remote endpoint of the TCP/IP tunnel connection, for example the tunnel server, the packet is passed to the pseudo network adapter 280 responsive to a TCP receive event. The pseudo network adapter 280 then decapsulates the packet by removing the tunnel header. The pseudo network adapter further decrypts the decapsulated data and passes it back to the TCP/IP protocol stack 282. The data passed from the pseudo network adapter 280 appears to the TCP/IP protocol stack 282 as an ethernet packet received from an actual physical device, and is the data it contains is passed on to the appropriate user by the TCP/IP protocol stack 282 based on information in the ethernet packet header provided by the pseudo network adapter.

Fig. 17 is a flow chart showing steps performed by an example embodiment of a pseudo network adapter during packet transmission, such as in the transmit path 290 of Fig. 14. The TCP/IP protocol stack determines that the destination node of a packet to be transmitted is reachable through the virtual LAN based on the destination IP address of the packet and a network layer routing table. At step 320 the packet is passed to the pseudo network adapter from the TCP/IP protocol stack. As a result, a send routine in the pseudo adapter is triggered for example in the virtual network adapter interface 288 of Fig. 16.

At step 322 the pseudo network adapter send routine processes the Ethernet header of the packet provided by the TCP/IP stack, and removes it. At step 324, the send routine determines whether the packet is an ARP request packet. If the packet is an ARP request packet for an IP address of a node on the virtual LAN, such as the pseudo network adapter of the tunnel server, then step 324 is followed by step 326. Otherwise, step 324 is followed by step 330.

At step 326, the ARP server emulator in the pseudo network adapter generates an ARP reply packet. For example, if the ARP request were for a physical address

Petitioner Apple Inc. - Exhibit 1026, p. 835

corresponding to the IP address of the pseudo network adapter on the tunnel server, the ARP reply would indicate a predetermined, reserved physical address to be associated with that IP address. At step 328 the pseudo network adapter passes the ARP response to the virtual network adapter interface. The virtual network adapter interface then indicates a received packet to the TCP/IP protocol stack, for example using an NDIS interface. The TCP/IP protocol stack then processes the ARP response as if it had been received over an actual physical network.

At step 330 the send routine determines whether the packet is a DHCP request packet requesting an IP address for the pseudo network adapter. If so, then step 330 is followed by step 332. Otherwise, step 330 is followed by step 334.

At step 334, the DHCP server emulator in the pseudo network adapter generates a DHCP response. The format of DHCP is generally described in the DHCP RFC. At step 328 the pseudo network adapter passes the DHCP response to the virtual network adapter interface, for example indicating an IP address received from the tunnel server in the client data field of the key exchange/authentication RESPONSE frame. The virtual network adapter interface then indicates a received packet to the TCP/IP protocol stack. The TCP/IP protocol stack then processes the DHCP response as if it had been received over an actual physical network.

At step 334 the pseudo network adapter encrypts the message using an encryption engine such that only the receiver is capable of decrypting and reading the message. At step 336 the pseudo network adapter encapsulates the encrypted message into a tunnel data frame. At step 338 the pseudo network adapter transmits the tunnel data frame through the tunnel connection using the TCP/IP protocol stack.

Fig. 18 is a flow chart showing steps performed by an example embodiment of a pseudo network adapter during packet receipt, such as in the receive path 296 of Fig. 14.

At step 350, the pseudo network adapter is notified that a packet has been received over the tunnel connection. At step 352 the pseudo network adapter decapsulates the received message by removing the header fields of the tunnel data frame. At step 354 the pseudo network adapter decrypts the decapsulated datagram from the tunnel data frame. At step 356, in an example embodiment, the pseudo network adapter forms an Ethernet packet from the decapsulated message. At step 358 the pseudo network adapter indicates that an Ethernet packet has been received to the TCP/IP protocol stack through the virtual network adapter interface. This causes the TCP/IP protocol stack to behave as if it had received an Ethernet packet from an actual Ethernet adapter.

Fig. 19 shows the data flow within the transmit path in an example embodiment of a pseudo network adapter. At step 1 370, an application submits data to be transmitted to the TCP protocol layer 372 within the TCP/IP protocol stack. The application uses a conventional socket interface to the TCP protocol layer 372 to pass the data, and indicates the destination IP address the data is to be transmitted to. The TCP protocol layer 372 then passes the data to the IP protocol layer 374 within the TCP/IP protocol stack. At step 2 376, the TCP/IP protocol stack refers to the routing table 378 to determine which network interface should be used to reach the destination IP address.

Because in the example the destination IP address is of a node reachable through the virtual private network, the IP layer 374 determines from the routing table 378 that the destination IP address is reachable through pseudo network adapter. Accordingly at step 3 380 the TCP/IP protocol stack passes a packet containing the data to the pseudo network adapter 382.

At step 4 384, the pseudo network adapter 382 encrypts the data packets and encapsulates them into tunnel data frames.

The pseudo network adapter 382 then passes the tunnel data frames packets back to the TCP protocol layer 372 within the TCP/IP protocol stack through a conventional socket interface to the tunnel connection with the first node in the tunnel path.

The TCP protocol layer 372 then forms a TCP layer packet for each tunnel data frame, having the tunnel data frame as its data. The TCP frames are passed to the IP layer 374. At step 5 386 the routing table 378 is again searched, and this time the destination IP address is the IP address associated with the physical network adapter on the tunnel server, and accordingly is determined to be reachable over the physical network adapter 390. Accordingly at step 6 388 the device driver 390 for the physical network adapter is called to pass the packets to the physical network adapter. At step 7 392 the physical network adapter transmits the data onto the physical network 394.

Fig. 20 is a data flow diagram showing data flow in an example embodiment of packet receipt involving a pseudo network adapter. At step 1 410 data arrives over the physical network 412 and is received by the physical network adapter and passed to the physical network driver 414. The physical network driver 414 passes the data at step 2 418 through the IP layer 420 and TCP layer 422 to the pseudo network adapter 426 at step 3 424, for example through a conventional socket interface. At step 4 428 the pseudo network adapter 426 decrypts and decapsulates the received data and passes it back to the IP layer of the TCP/IP protocol stack, for example through the TDI (Transport Layer Dependent Interface API) of the TCP/IP stack. The data is then passed through the TCP/IP protocol stack and to the user associated with the destination IP address in the decapsulated datagrams at step 5 430.

Fig. 21 shows data flow in an example embodiment of packet transmission involving a pseudo network adapter. Fig. 21 shows an example embodiment for use

Petitioner Apple Inc. - Exhibit 1026, p. 836

on a Microsoft™ Windows 95™ PC platform. In Fig. 21 a user application 450 passes unencrypted data to an interface into the TCP layer of the TCP/IP protocol, for example the WinSock API 452. The user indicates a destination IP address associated with a node reachable through a virtual private network accessible through the pseudo network adapter.

The TCP layer 454 passes the data to the IP layer 456, which in turn passes the data to the Network Device Interface Specification Media Access Control (NDIS MAC) interface 458. The pseudo network adapter 459 has previously registered with the routing layer (IP) that it is able to reach a gateway address associated with the destination IP address for the user data. Accordingly the IP layer uses the NDIS MAC layer interface to invoke the virtual device driver interface 460 to the pseudo network adapter 459. The pseudo network adapter 459 includes a virtual device driver interface 460, an ARP server emulator 462, and a DHCP server emulator 464.

In the example embodiment of Fig. 19, the pseudo network adapter 459 passes the data to a tunnel application program 466. The tunnel application program 466 encrypts the IP packet received from the IP layer and encapsulates it into a tunnel data frame. The tunnel application then passes the tunnel data frame including the encrypted data to the WinSock interface 452, indicating a destination IP address of the remote tunnel end point. The tunnel data frame is then passed through the TCP layer 454, IP layer 456, NDIS MAC layer interface 458, and physical layer 468, and transmitted on the network 470. Since the resulting packets do not contain a destination IP address which the pseudo network adapter has registered to convey, these packets will not be diverted to the pseudo network adapter.

Fig. 22 is a data flow diagram showing data flow in an example embodiment of packet transmission involving a pseudo network adapter. The embodiment shown in Fig. 22 is for use on a UNIX platform. In Fig. 20 a user application 472 passes unencrypted data to a socket interface to the TCP/IP protocol stack in the UNIX socket layer 474, indicating a destination IP address of a node reachable through the virtual private network.

The UNIX socket layer 474 passes the data through the TCP layer 476 and the IP layer 478. The pseudo network adapter 480 has previously registered with the routing layer (IP) that it is able to reach a gateway associated with the destination IP address for the user data. Accordingly the IP layer 478 invokes the virtual device driver interface 482 to the pseudo network adapter 480. The IP layer 478 passes the data to the pseudo network adapter 480. The pseudo network adapter 480 includes a virtual device driver interface 482, and a DHCP server emulator 484.

In the example embodiment of Fig. 22, the pseudo network adapter 480 passes IP datagrams to be transmitted to a UNIX Daemon 486 associated with the tunnel connection. The UNIX Daemon 486 encrypts the IP packet(s) received from the IP layer 478 and encapsulates them into tunnel data frames. The UNIX Daemon 486 then passes the tunnel data frames to the UNIX socket layer 474, through a socket associated with the tunnel connection. The tunnel data frames are then processed by the TCP layer 476, IP layer 478, data link layer 488, and physical layer 490 to be transmitted on the network 492. Since the resulting packets are not addressed to an IP address which the pseudo network adapter 480 has registered to convey, the packets will not be diverted to the pseudo network adapter 480.

Fig. 23 is a flow chart showing steps to initialize a example embodiment of a virtual private network. The steps shown in Fig. 23 are performed for example in the tunnel client 247 as shown in Fig. 14. At step 500 a tunnel application program executing in the tunnel client sends a tunnel relay frame to the tunnel server. At step 502 the tunnel application program sends a tunnel key exchange/authentication REQUEST frame to the tunnel server. The tunnel application in the tunnel server ignores the contents of the client data field in the tunnel key exchange/authentication REQUEST frame. The tunnel application in the tunnel server fills in the client data field in the tunnel key exchange/authentication RESPONSE frame with Dynamic Host Configuration Protocol (DHCP) information, for example including the following information in standard DHCP format:

1) IP Address for tunnel client Pseudo Network Adapter
2) IP Address for tunnel server Pseudo Network Adapter
3) Routes to nodes on the private network physically connected to the tunnel server which are to be reachable over the tunnel connection.

At step 504 the tunnel application receives a tunnel key exchange/authentication RESPONSE frame from the tunnel server. The client data field 508 in the tunnel connection response is made available to the pseudo network adapter in the tunnel client. The tunnel application in the tunnel client tells the TCP/IP stack that the pseudo network adapter in the tunnel client is active. The pseudo network adapter in the tunnel client is active and ready to be initialized at step 510.

The tunnel client system is configured such that it must obtain an IP address for the tunnel client pseudo network adapter dynamically. Therefore the TCP/IP stack in the tunnel client broadcasts a DHCP request packet through the pseudo network adapter. Accordingly, at step 512 the pseudo network adapter in the client receives a conventional DHCP request packet from the TCP/IP stack requesting a dynamically allocated IP address to associate with the pseudo network adapter. The pseudo network adapter passes the DHCP request packet to the DHCP server emulator within the pseudo network adapter, which forms a DHCP response based on the client data 508 received from the tunnel applica-

Petitioner Apple Inc. - Exhibit 1026, p. 837

tion. The DHCP response includes the IP address for the client pseudo adapter provided by the tunnel server in the client data. At step 514 the pseudo network adapter passes the DHCP response to the TCP/IP stack.

At step 520, the tunnel application modifies the routing tables within the tunnel client TCP/IP stack to indicate that the routes to the nodes attached to the private network to which the tunnel server is attached all are reachable only through the pseudo network adapter in the tunnel server. The IP address of the pseudo network adapter in the tunnel server provided in the client data is in this way specified as a gateway to the nodes on the private network to which the tunnel server is attached. In this way those remote nodes are viewed by the TCP/IP stack as being reachable via the virtual private network through the client pseudo network adapter.

At step 516 the pseudo network adapter in the tunnel client receives an ARP request for a physical address associated with the IP address of the pseudo network adapter in the tunnel server. The pseudo network adapter passes the ARP request to the ARP server emulator, which forms an ARP reply indicating a reserved physical address to be associated with the IP address of the pseudo network adapter in the tunnel server. At step 518 the pseudo network adapter passes the ARP response to the TCP/IP stack in the tunnel client. In response to the ARP response, the TCP/IP stack determines that packets addressed to any node on the virtual private network must be initially transmitted through the pseudo network adapter.

In an example embodiment the present system reserves two physical addresses to be associated with the pseudo network adapter in the client and the pseudo network adapter in the server respectively. These reserved physical addresses are used in responses to ARP requests passed through the pseudo network adapter for physical addresses corresponding to the IP addresses for the pseudo network adapter in the client and the pseudo network adapter in the server respectively. The reserved physical addresses should have a high likelihood of not being used in any actual network interface.

While the invention has been described with reference to specific example embodiments, the description is not meant to be construed in a limiting sense. Various modifications of the disclosed embodiments, as well as other embodiments of the invention, will be apparent to persons skilled in the art upon reference to this description. Specifically, while various embodiments have been described using the TCP/IP protocol stack, the invention may advantageously be applied where other communications protocols are used. Also, while various flow charts have shown steps performed in an example order, various implementations may use altered orders of step in order to apply the invention. And further, while certain specific software and/or hardware platforms have been used in the description, the invention may be applied on other platforms with similar advantage. It is therefore contemplated that the appended claims will cover any such modifications or embodiments which fall within the scope of the invention.

Claims

1. A pseudo network adapter providing a virtual private network, comprising:

   an interface for capturing packets from a local communications protocol stack for transmission on said virtual private network, said interface appearing to said local communications protocol stack as a network adapter device driver for a network adapter connected to said virtual private network;
   a first server emulator, providing a first reply packet responsive to a first request packet captured by said interface for capturing packets from said local communications protocol stack for transmission on said virtual private network, said first request packet requesting a network layer address for said pseudo network adapter, said first reply indicating a network layer address for said pseudo network adapter; and
   a second server emulator, providing a second reply packet responsive to an second request packet captured by said interface for capturing packets from said local communications protocol stack for transmission on said virtual private network, said second request packet requesting a physical address corresponding to a network layer address of a second pseudo network adapter, said second pseudo network adapter located on a remote server node, said second reply indicating a predetermined, reserved physical address.

2. The pseudo network adapter of claim 1, further comprising a means for indicating to said local communications protocol stack that said predetermined, reserved physical address is reachable through said pseudo network adapter, wherein said means for indicating modifies a data structure in said local communications protocol stack indicating which nodes or networks are reachable through each network interface of the local system.

3. The pseudo network adapter of claim 1, further comprising a means for indicating to said local communications protocol stack that one or more nodes on a remote private network connected to said remote server node are reachable through a gateway node equal to said second pseudo network adapter on said remote server node.

Petitioner Apple Inc. - Exhibit 1026, p. 838

4. The pseudo network adapter of claim 1, further comprising:

a transmit path for processing data packets captured by said interface for capturing packets from said local communications protocol stack for transmission on said virtual private network;
an encryption engine, within said transmit path, for encrypting said data packets;
an encapsulation engine, within said transmit path, for encapsulating said encrypted data packets into tunnel data frames; and
a means for passing said tunnel data frames back to said local communications protocol stack for transmission to a physical network adapter on said remote server node.

5. The pseudo network adapter of claim 4, wherein said transmit path further includes means for storing a digest value in a digest field in each of said tunnel data frames, said digest value equal to an output of a keyed hash function applied to said data packet encapsulated within said tunnel data frame concatenated with a counter value equal to a total number of tunnel data frames previously transmitted to said remote server node.

6. The pseudo network adapter of claim 4, wherein said transmit path further includes means for processing an Ethernet header in each one of said captured data packets, said processing of said Ethernet header including removing said Ethernet header.

7. The pseudo network adapter of claim 1, further comprising:

an interface into a transport layer of said local communications protocol stack for capturing received data packets from said remote server node.

8. The pseudo network adapter of claim 7, further comprising:

a receive path for processing received data packets captured by said interface into said transport layer of said local communications protocol stack for capturing received data packets from said remote server node;
an decapsulation engine, within said receive path, for decapsulating said received data packets by removing a tunnel frame header;
an decryption engine, within said receive path, for decrypting said received data packets; and
a means for passing said received data packets back to said local communications protocol stack for delivery to a user.

9. A method for providing a pseudo network adapter for a virtual private network, comprising the steps of:

capturing packets from a local communications protocol stack for transmission on said virtual private network, said capturing through an interface appearing to said local communications stack as a network adapter device driver for a network adapter connected to said virtual private network;
issuing a first reply packet responsive to a first request packet captured by said interface for capturing packets from said local communications protocol stack for transmission on said virtual private network, said first request packet requesting a network layer address for said pseudo network adapter, said first reply indicating a network layer address for said pseudo network adapter; and
issuing a second reply packet responsive to a second request packet captured by said interface for capturing packets from said local communications protocol stack for transmission on said virtual private network, said second request packet requesting a physical address corresponding to a network layer address of a second pseudo network adapter, said second pseudo network adapter located on a remote server node, said ARP Reply indicating a predetermined, reserved physical address.

10. The method of claim 9, further comprising indicating to said local communications protocol stack that said predetermined, reserved physical address is reachable through said pseudo network adapter, wherein said step of indicating to said local communications protocol stack modifies a data structure in said local communications protocol stack indicating which nodes or networks are reachable through each network interface of the local system.

11. The method of claim 9, further comprising indicating to said local communications protocol stack that one or more nodes on a remote private network connected to said remote server node are reachable through a gateway node equal to said second pseudo network adapter on said remote server node, wherein said step of indicating to said local communications protocol stack that one or more nodes on said remote private network connected to said remote server node are reachable through a gateway node equal to said second pseudo network adapter on said remote server node modifies a network layer routing table in said local communications protocol stack.

12. The method of claim 9, further comprising:

Petitioner Apple Inc. - Exhibit 1026, p. 839

processing data packets captured by said interface for capturing packets from said local communications protocol stack for transmission on said virtual private network in a transmit data path;

encrypting said data packets in an encryption engine, within said transmit path;

encapsulating said encrypted data packets into tunnel data frames by an encapsulation engine, within said transmit path; and

passing said tunnel data frames back to said local communications protocol stack for transmission to a physical network adapter on said remote server node, wherein said transmit path further includes storing a digest value in a digest field in each of said tunnel data frames, said digest value equal to an output of a keyed hash function applied to said data packet encapsulated within said tunnel data frame concatenated with a counter value equal to a total number of tunnel data frames previously transmitted to said remote server node.

13. The method of claim 12, wherein said transmit path further includes processing an Ethernet header in each one of said captured data packets, said processing of said Ethernet header including removing said Ethernet header.

14. The method of claim 9, further comprising capturing received data packets from said remote server node through an interface into a transport layer of said local communications protocol stack, further comprising:

processing received data packets captured by said interface into said transport layer of said local communications protocol stack for capturing received data packets from said remote server node in a receive path;

decapsulating said received data packets by removing a tunnel frame header in an decapsulation engine, within said receive path;

decrypting said received data packets in a decryption engine within said receive path; and

passing said received data frames packets back to said local communications protocol stack for delivery to a user.

15. The method of claim 9, wherein said network layer address for said pseudo network adapter and said predetermined, reserved physical address is communicated to said pseudo network adapter from said remote server node as client data in a connection response frame.

Petitioner Apple Inc. - Exhibit 1026, p. 840

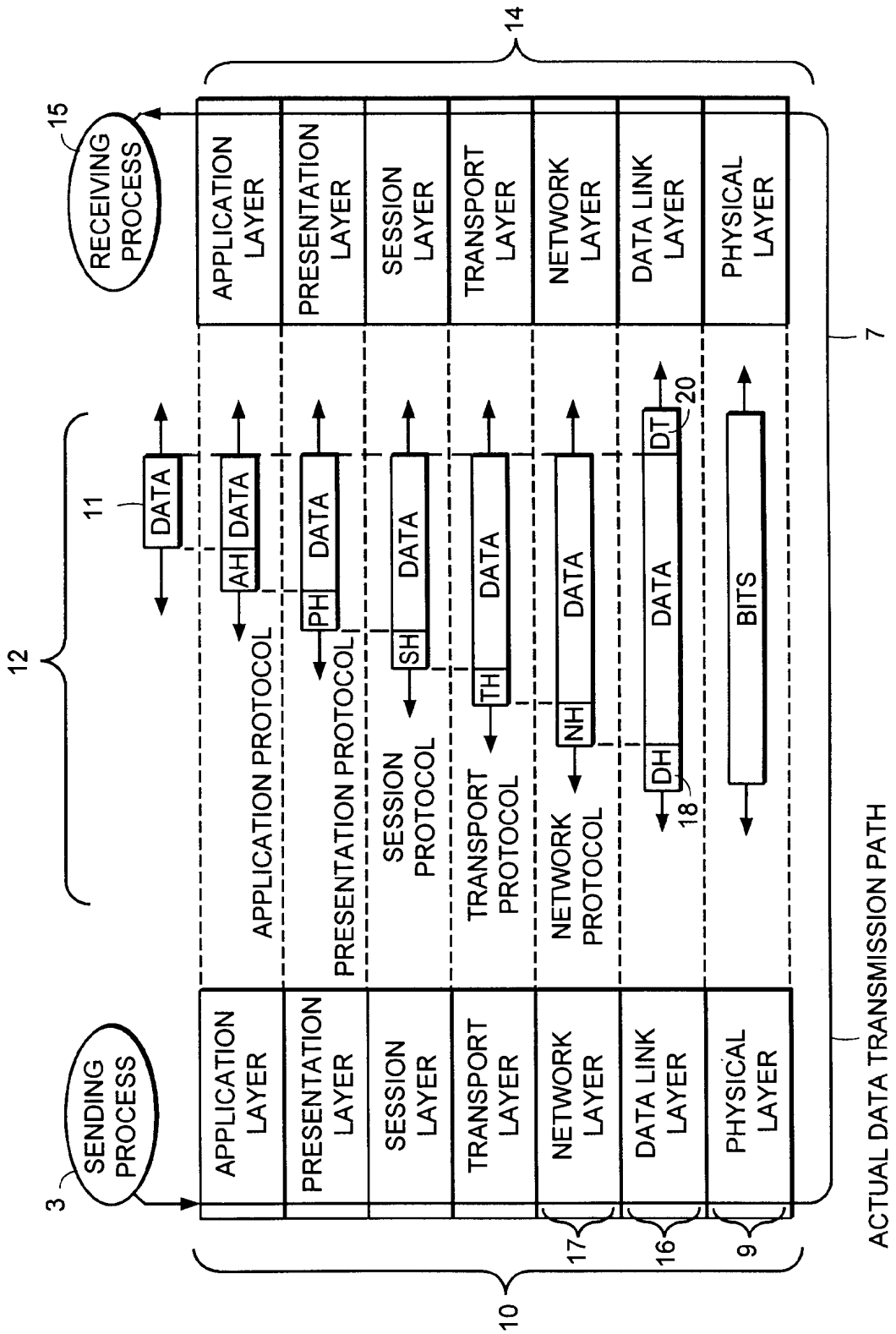


FIG. 1

Petitioner Apple Inc. - Exhibit 1026, p. 841

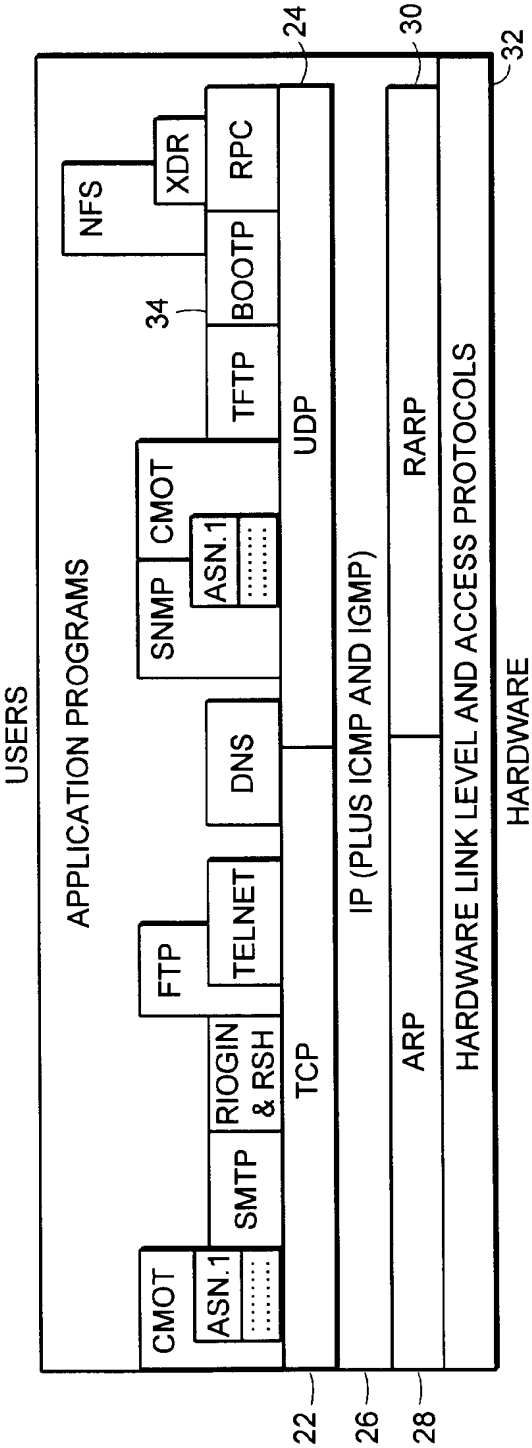


FIG. 2

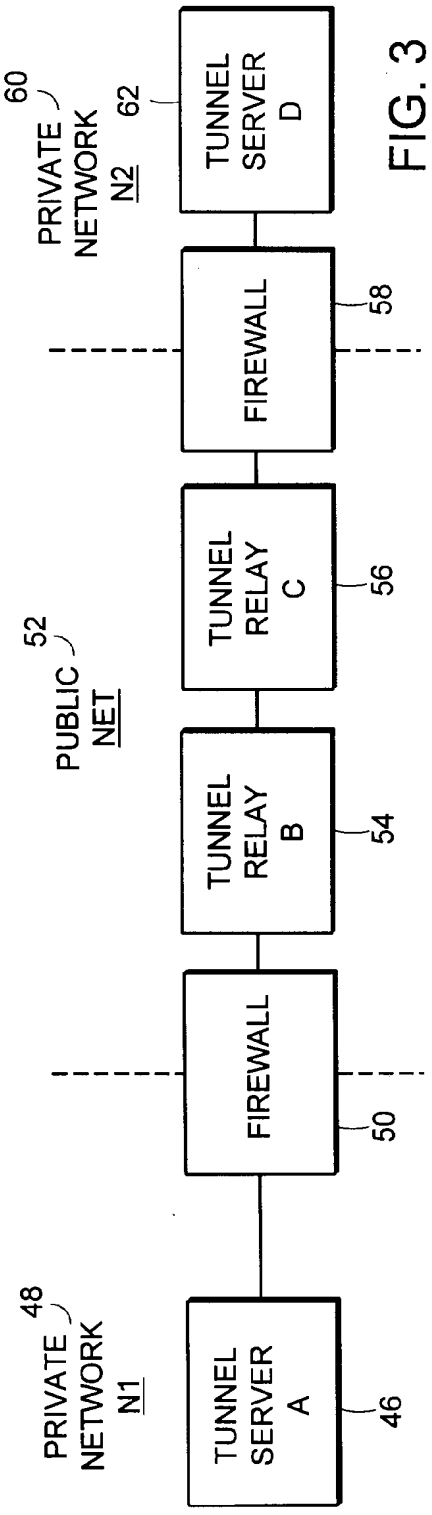


FIG. 3

Petitioner Apple Inc. - Exhibit 1026, p. 842

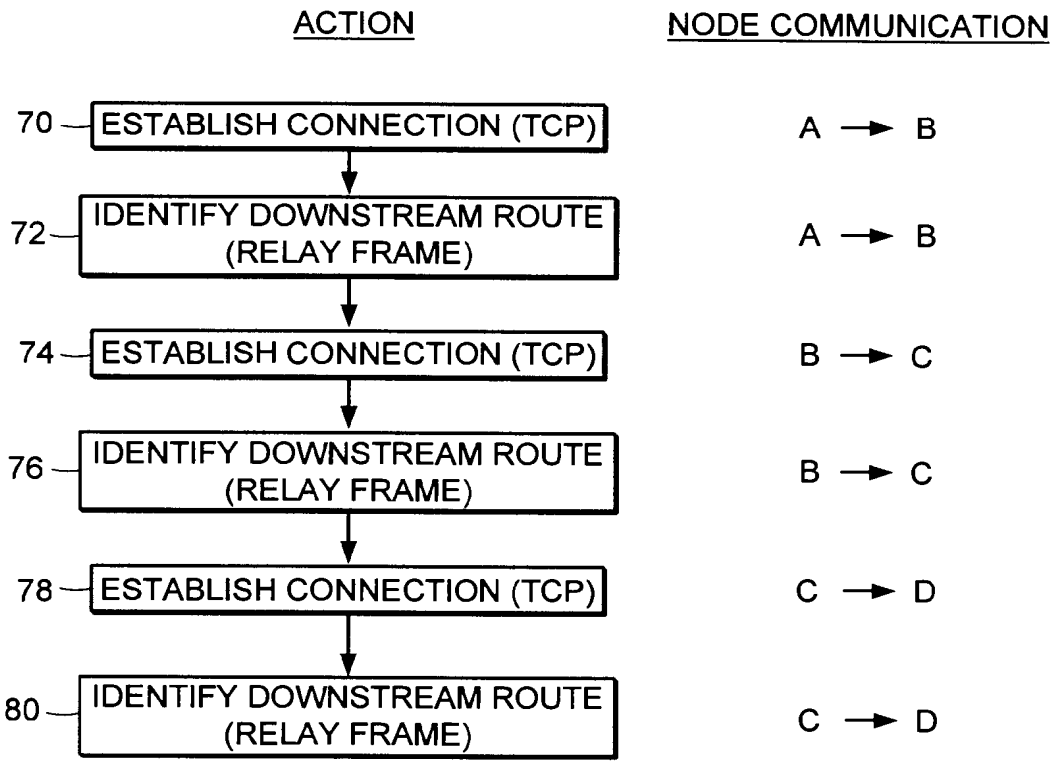


FIG. 4

Petitioner Apple Inc. - Exhibit 1026, p. 843

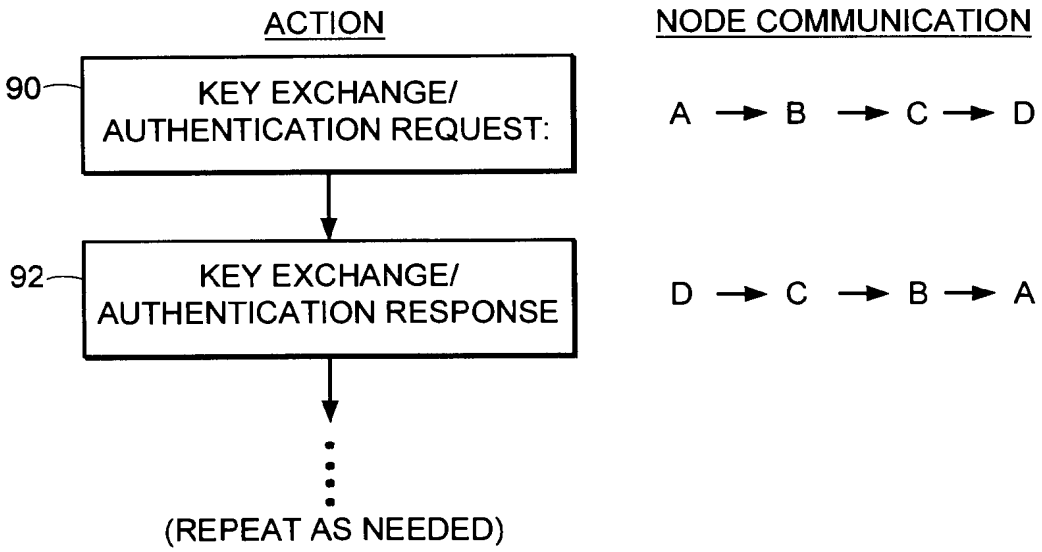


FIG. 5

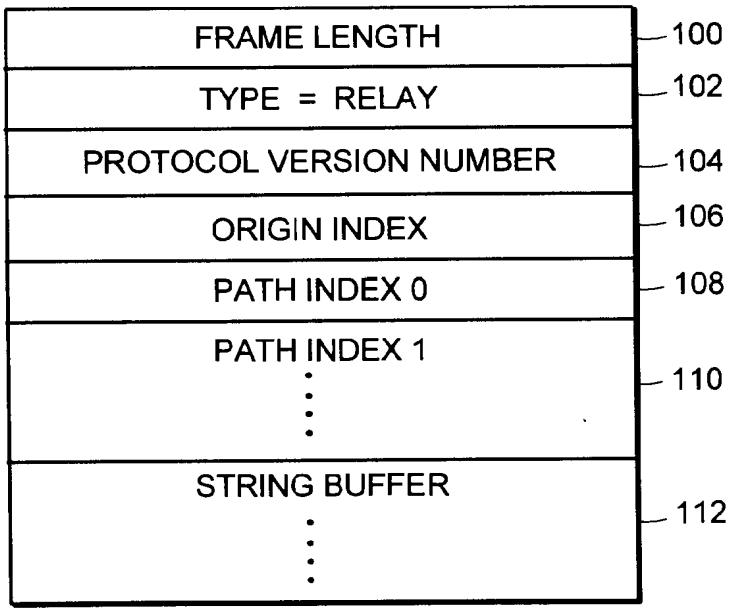


FIG. 6

Petitioner Apple Inc. - Exhibit 1026, p. 844

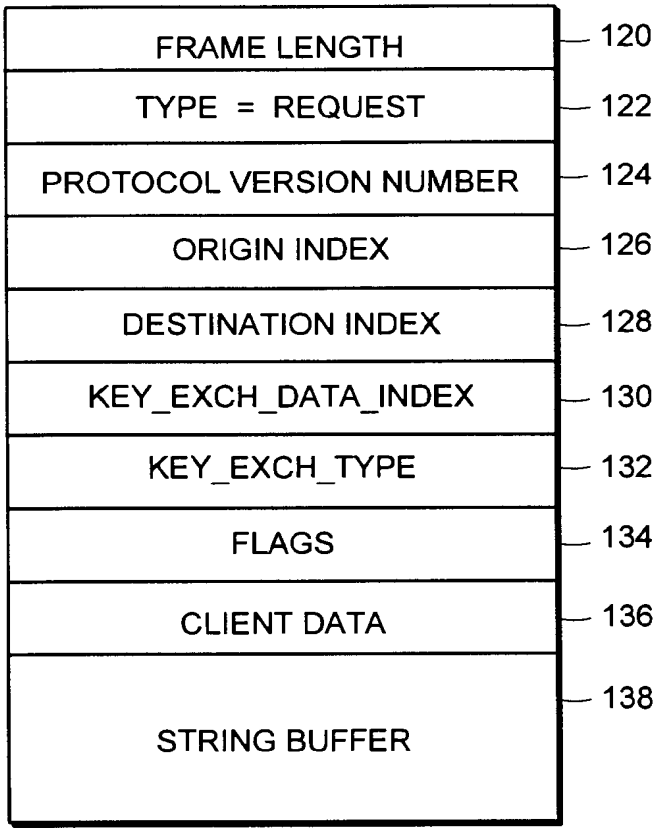


FIG. 7

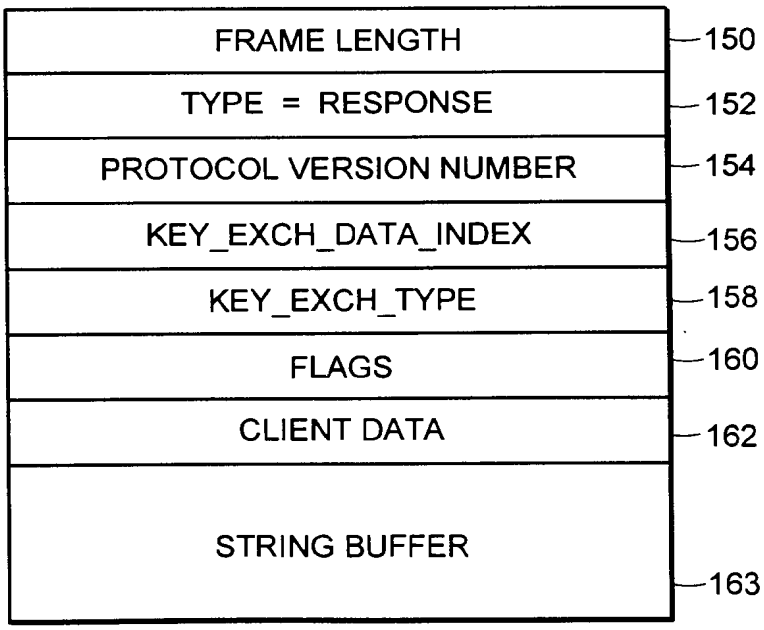


FIG. 8

Petitioner Apple Inc. - Exhibit 1026, p. 845

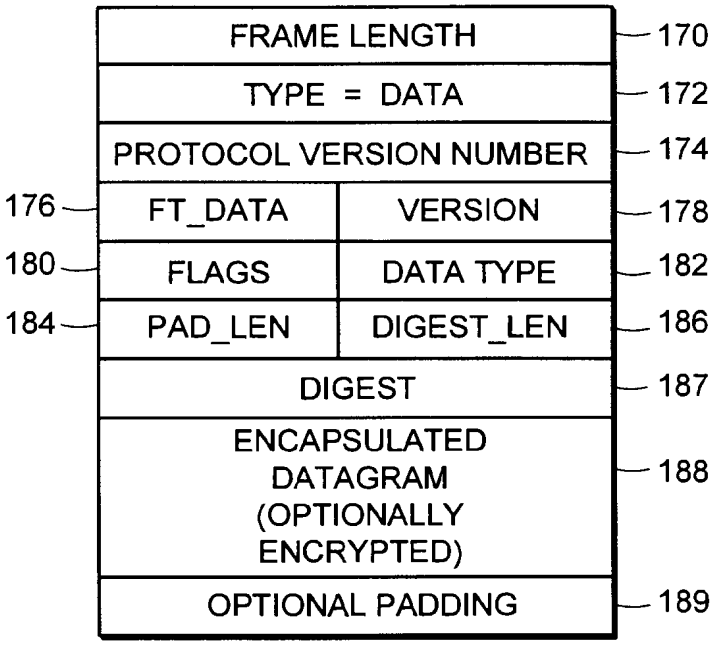


FIG. 9

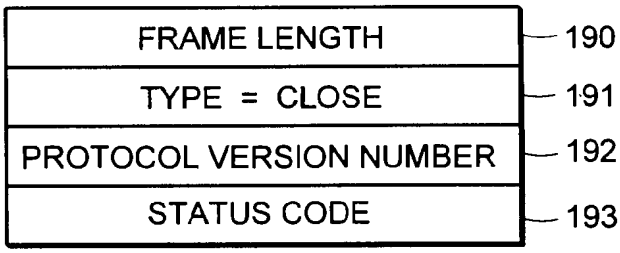


FIG. 10

Petitioner Apple Inc. - Exhibit 1026, p. 846

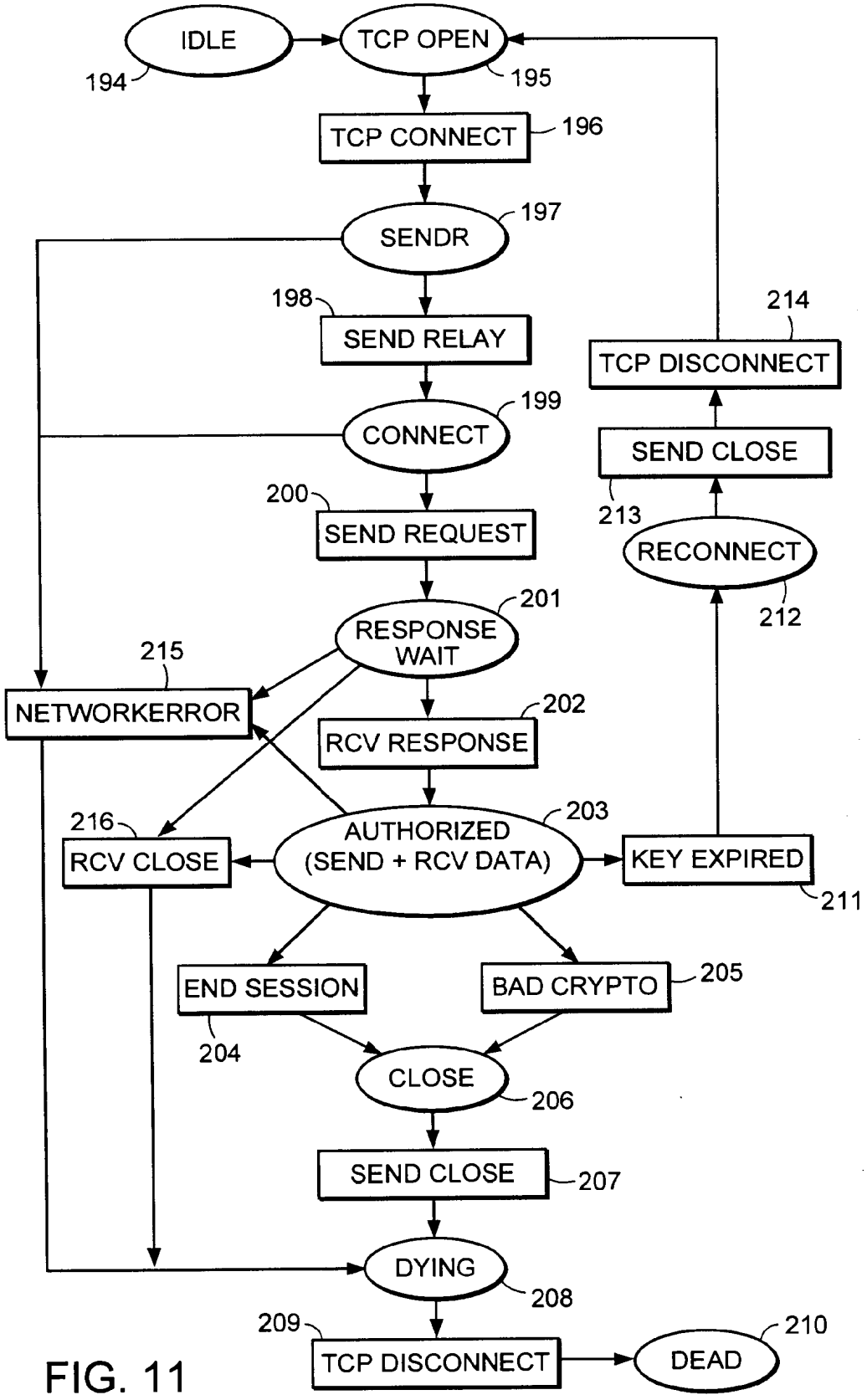


FIG. 11

Petitioner Apple Inc. - Exhibit 1026, p. 847

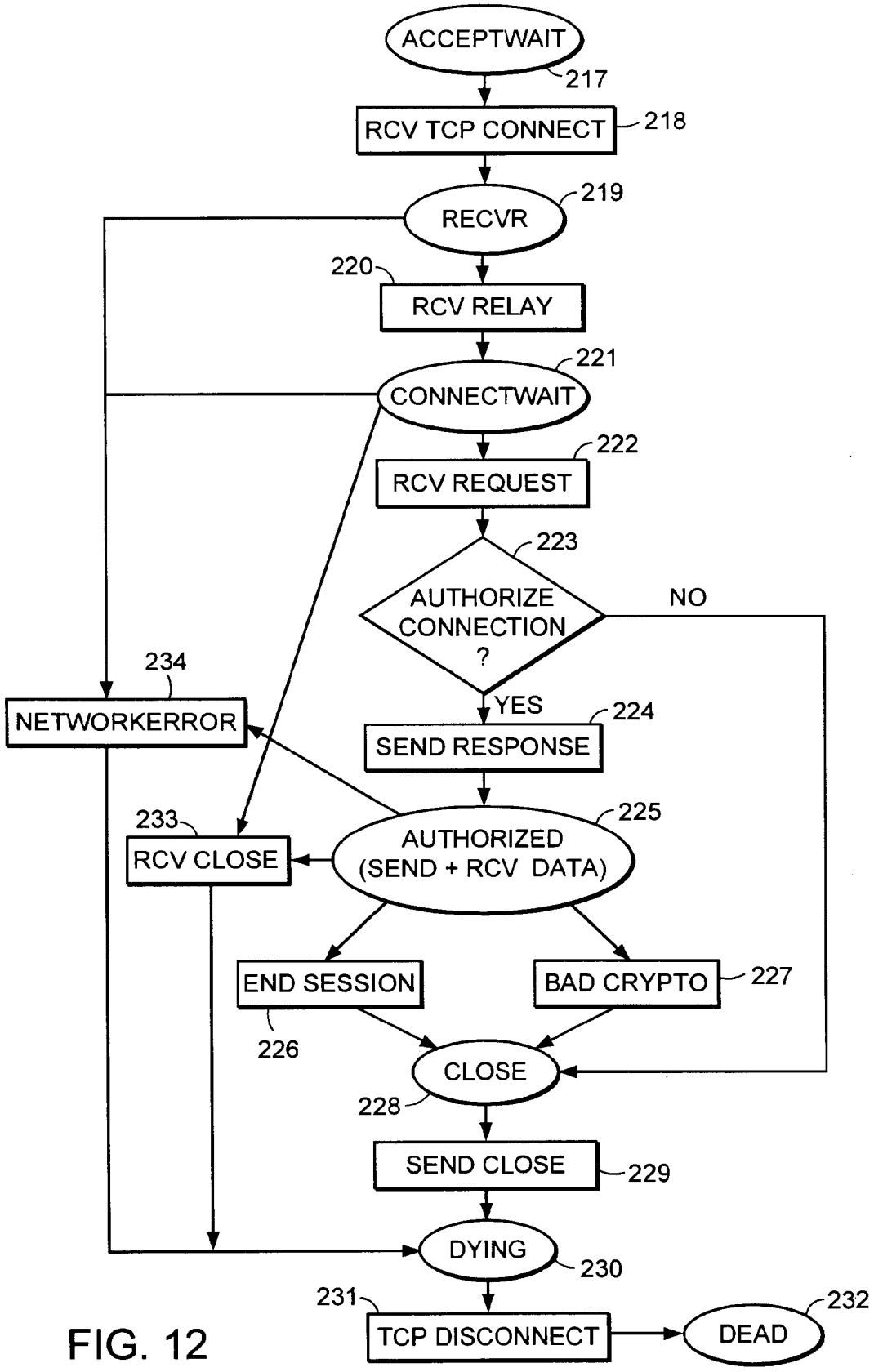


FIG. 12

Petitioner Apple Inc. - Exhibit 1026, p. 848

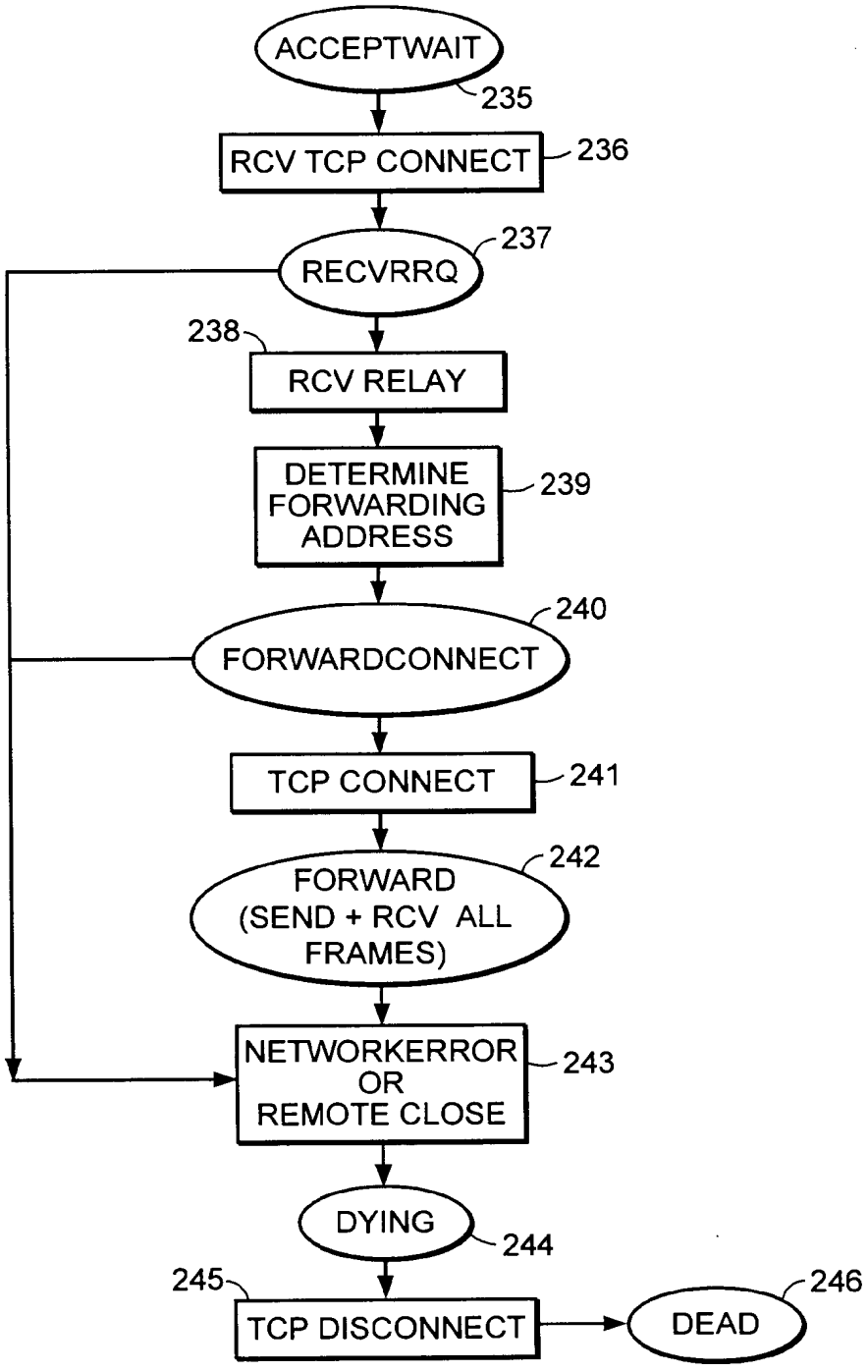


FIG. 13

Petitioner Apple Inc. - Exhibit 1026, p. 849

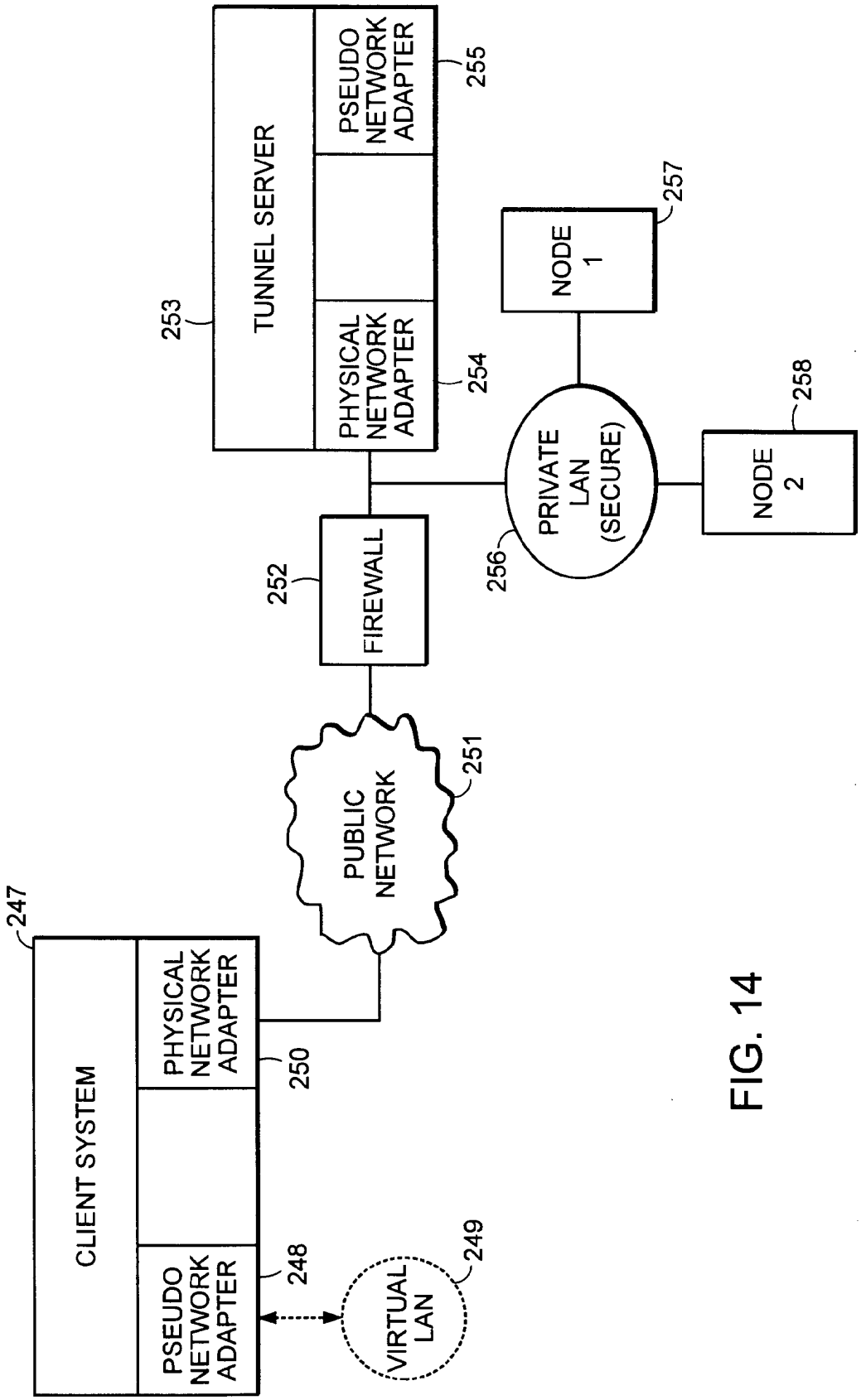


FIG. 14

Petitioner Apple Inc. - Exhibit 1026, p. 850

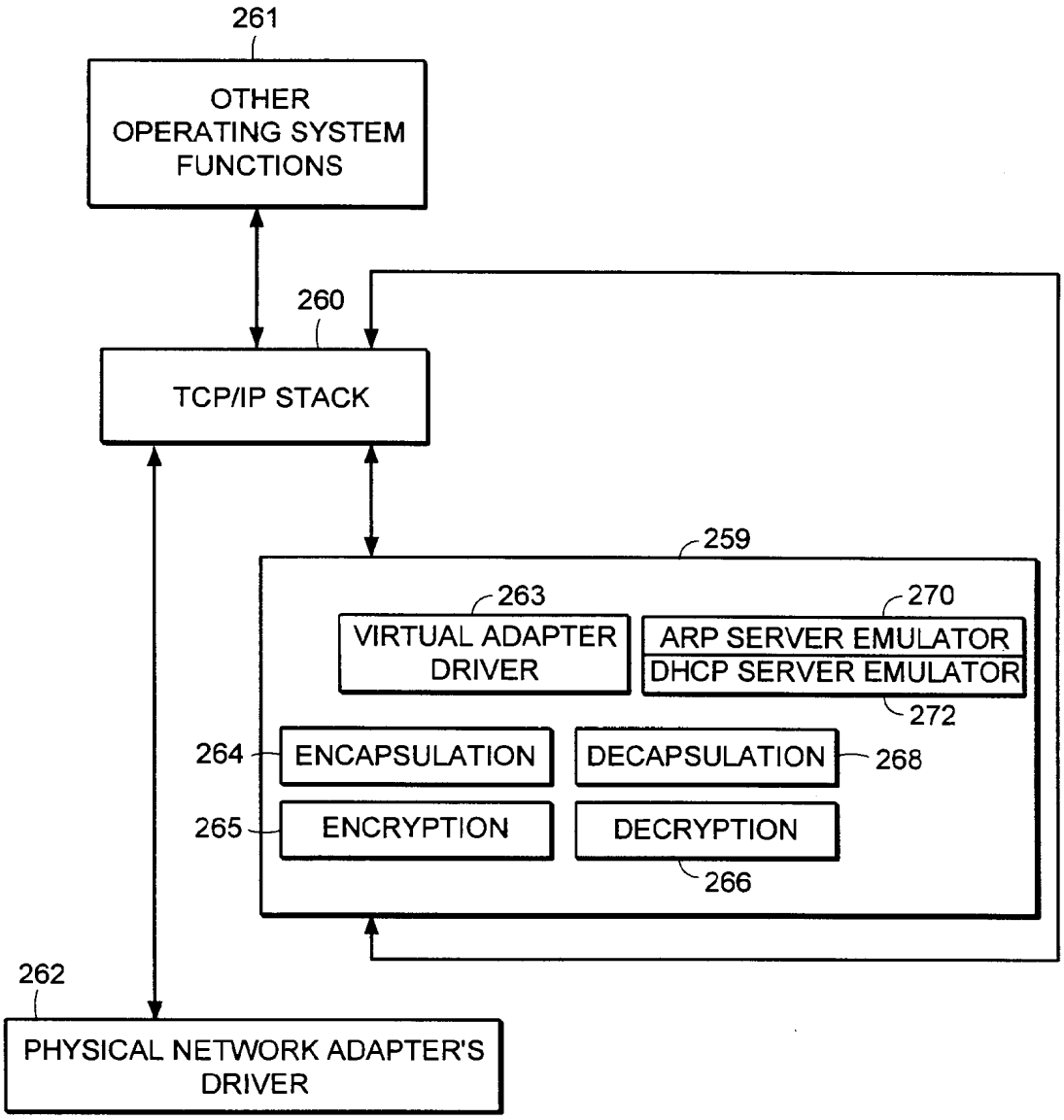


FIG. 15

Petitioner Apple Inc. - Exhibit 1026, p. 851

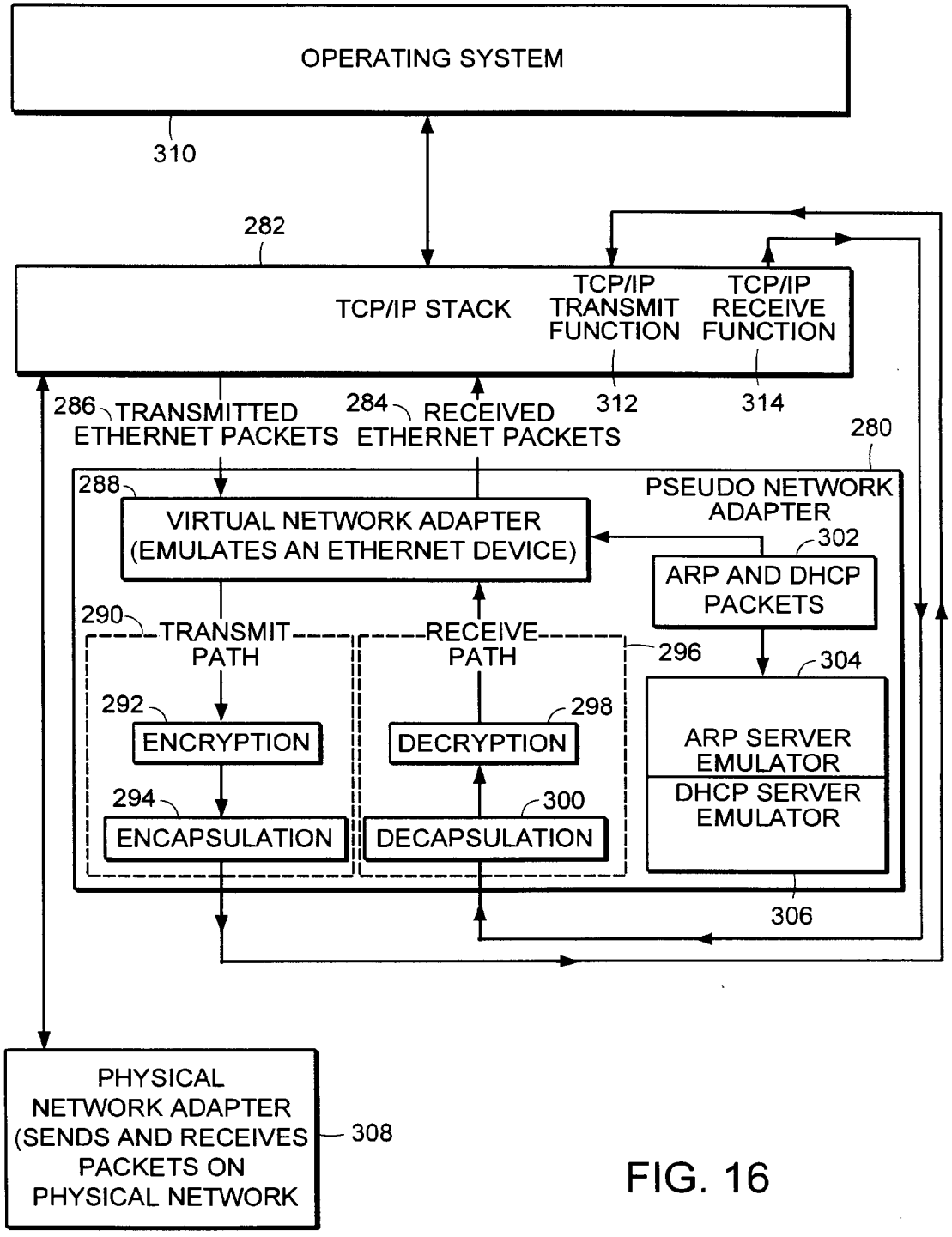


FIG. 16

Petitioner Apple Inc. - Exhibit 1026, p. 852

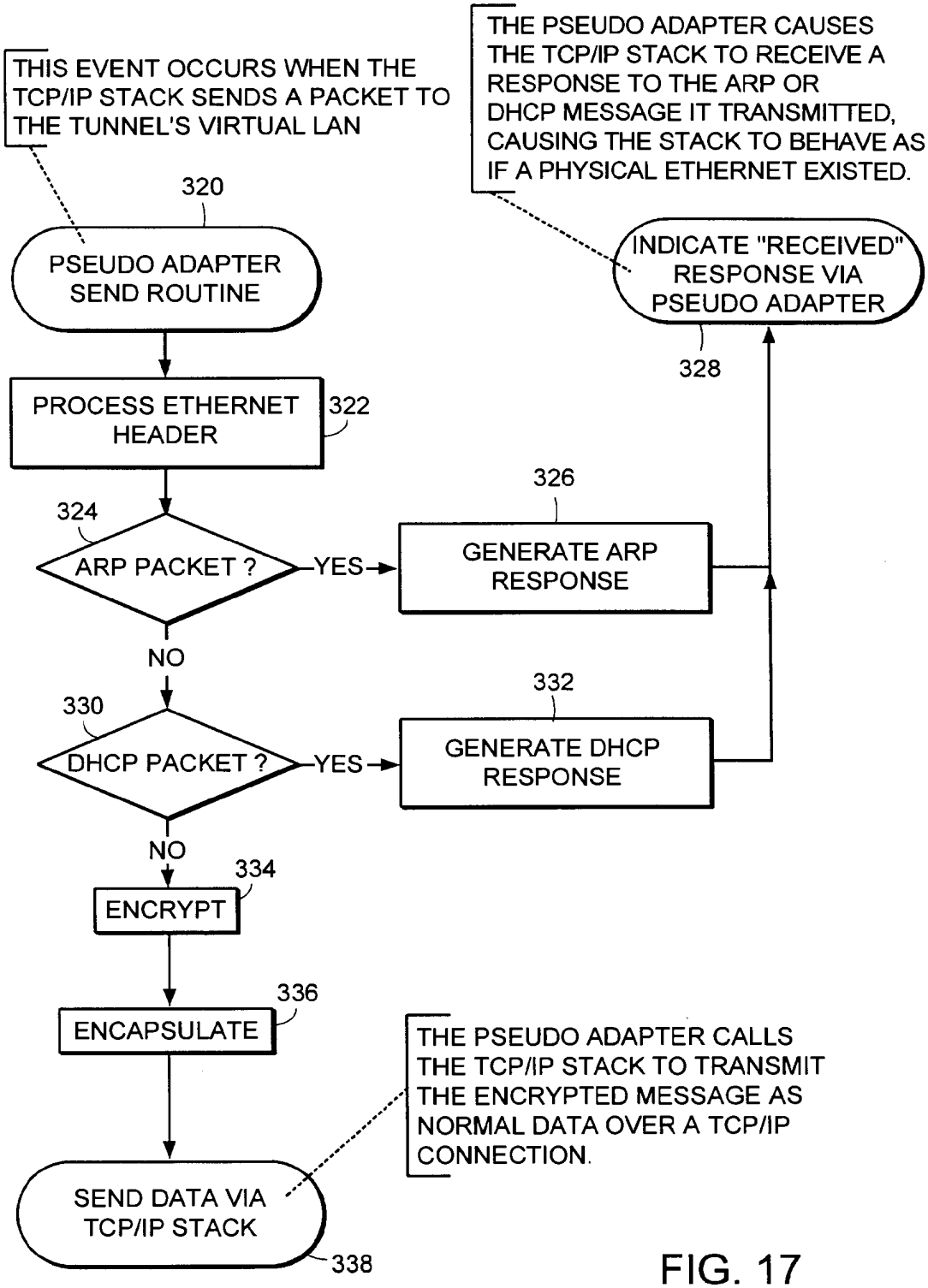


FIG. 17

Petitioner Apple Inc. - Exhibit 1026, p. 853

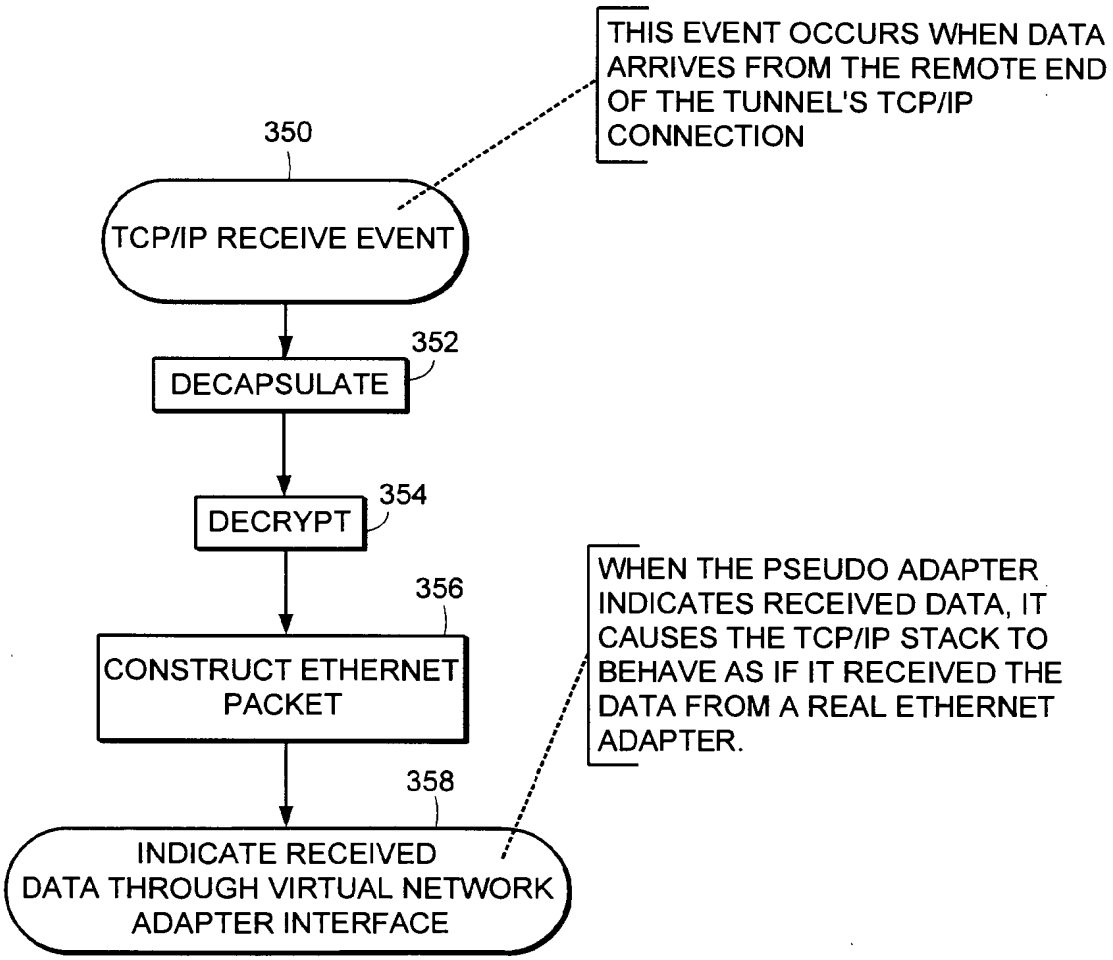


FIG. 18

Petitioner Apple Inc. - Exhibit 1026, p. 854

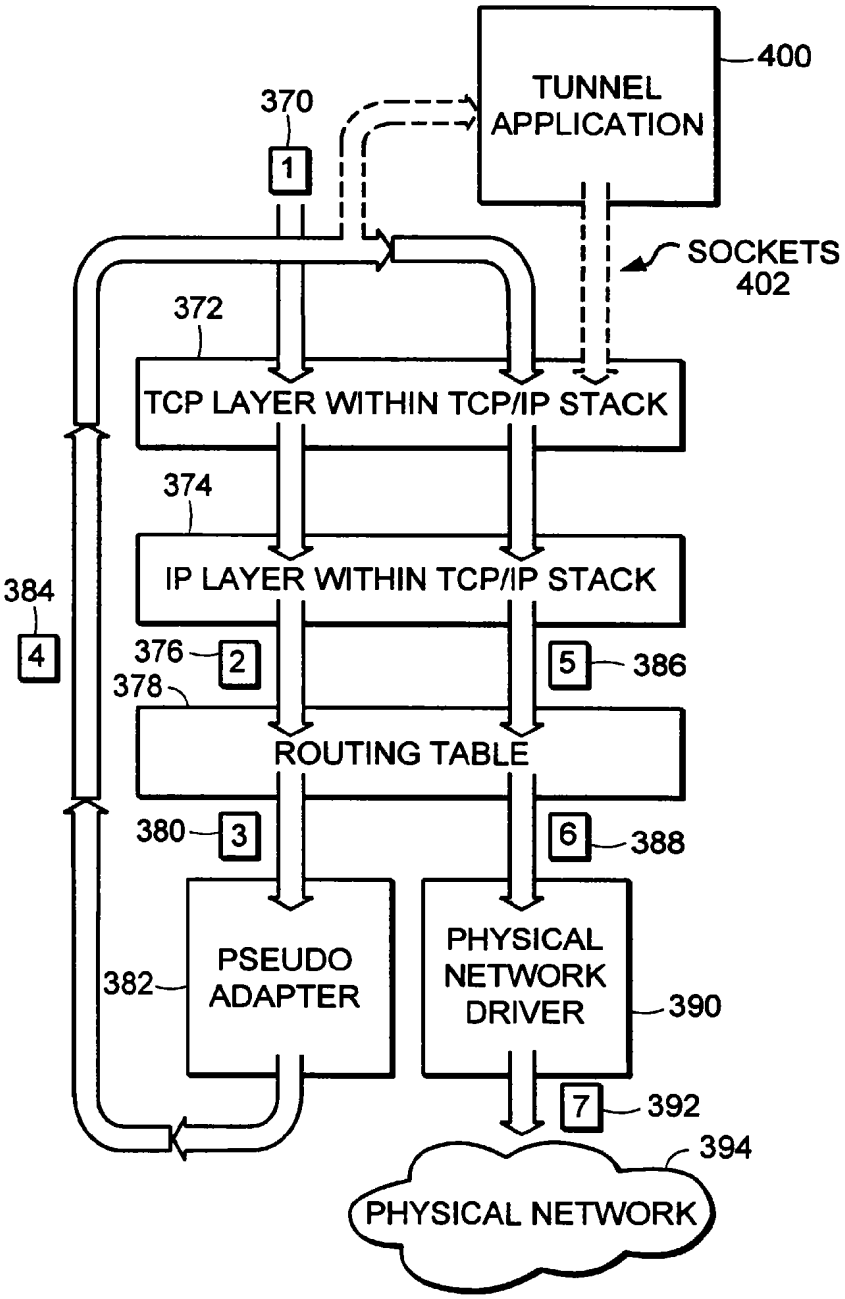


FIG. 19

Petitioner Apple Inc. - Exhibit 1026, p. 855

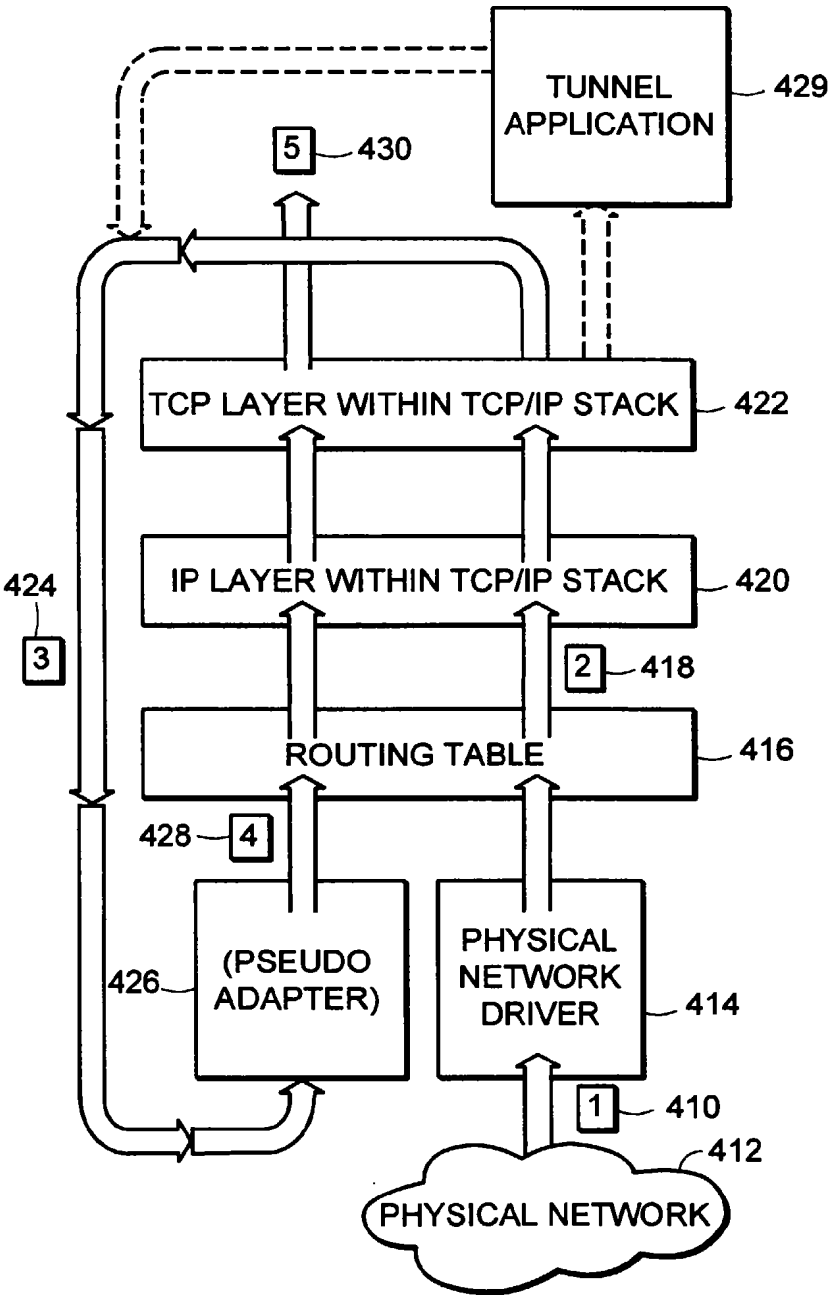


FIG. 20

Petitioner Apple Inc. - Exhibit 1026, p. 856

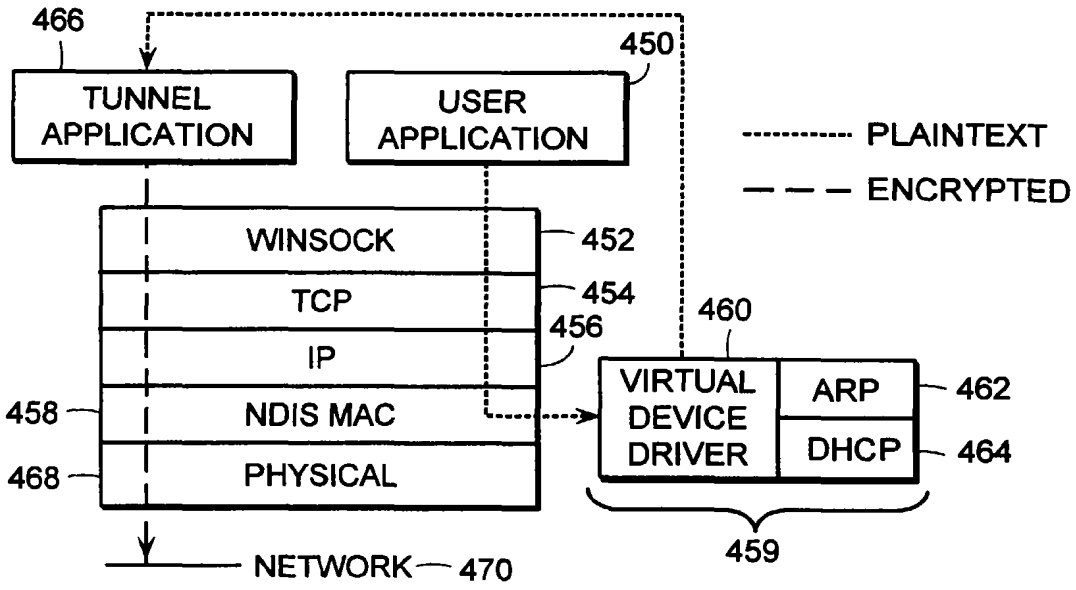


FIG. 21

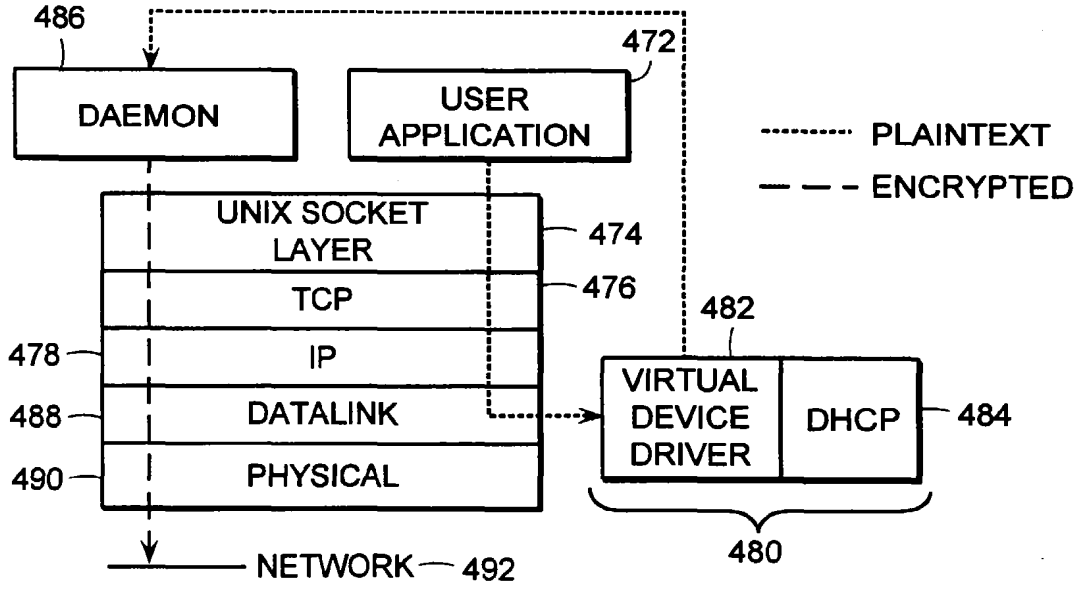


FIG. 22

Petitioner Apple Inc. - Exhibit 1026, p. 857

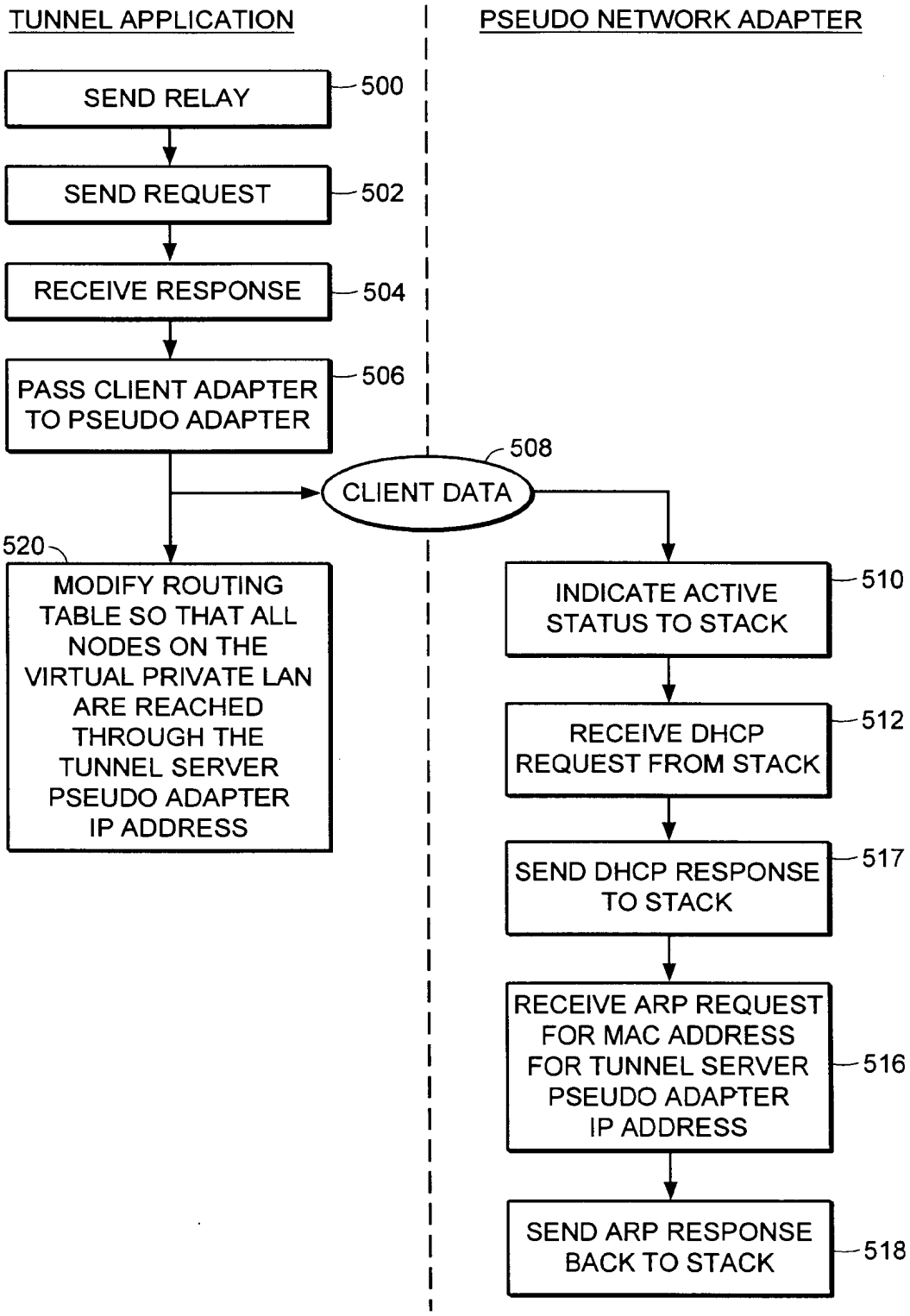


FIG. 23

Petitioner Apple Inc. - Exhibit 1026, p. 858

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 814 589 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.12.1997 Bulletin 1997/52

(51) Int. Cl.[6]: **H04L 29/06**

(21) Application number: **97109792.8**

(22) Date of filing: **16.06.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **19.06.1996 US 667524**

(71) Applicant: **AT&T Corp.**
New York, NY 10013-2412 (US)

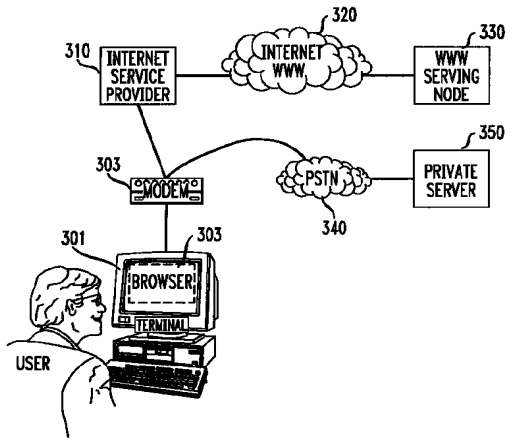
(72) Inventors:
- **Harwood, Jonathan P.**
Morganville, N.J. 07751 (US)
- **Kimmeth, Thomas**
Gladstone, N.J. 07977 (US)
- **Nusbaum, Kurt**
Downers Grove, Illinois 60515 (US)

(74) Representative:
KUHNEN, WACKER & PARTNER
Alois-Steinecker-Strasse 22
85354 Freising (DE)

(54) System and method for automated network reconfiguration

(57) A method is disclosed for providing an enhanced level of security for sensitive or proprietary information associated with information transactions in a public network, such as the Internet. In carrying out that method, an on-line information transaction is bifurcated between a generalized information access portion of such a transaction and an exchange of sensitive user information. With such a bifurcation, the generalized information access portion of the transaction, which generally would constitute the more substantial (in terms of network resources) portion of the transaction, would be handled via a non-secure network, usually a public network such as the Internet. The portion of the transaction involving sensitive user information, on the other hand, would be handled by a separate secure connection, such as a private network, or intranetwork. An important characteristic of this bifurcation arrangement is the provision of a means for automated reconfiguration of a user terminal as between accessing the Ageneralized information via the non-secure network and access to the secure communications network for the exchange of sensitive user information. Such an automated reconfiguration will be carried out without the necessity for any action on the part of the user, and indeed will be largely invisible to the user.

FIG. 3



EP 0 814 589 A2

Petitioner Apple Inc. - Exhibit 1026, p. 859

Description

FIELD OF THE INVENTION

This invention is related to the field of data communications, and more particularly to a method and means for establishing an automatic reconfiguration of a user terminal among alternative tasks.

BACKGROUND OF THE INVENTION

With the increasing popularity of personal computers over the last several years has come a striking growth in transaction-oriented computer-to-computer communications (as opposed to bulk-data transfers among such computers). For convenience herein such transaction-oriented computer-to-computer communications will be described by the shorthand term "information transaction". That growth in the use of computers for such information transactions has unquestionably been fueled by the existence of an international infrastructure for implementing such data communications, known as the Internet. And, driven by the burgeoning demand for such information transaction services, the Internet has itself experienced explosive growth in the amount of traffic handled.

At least partly in response to that demand, a new level of accessibility to various information sources has recently been introduced to the Internet, known as the World Wide Web ("WWW"). The WWW allows a user to access a universe of information which combines text, audio, graphics and animation within a hypermedia document. Links are contained within a WWW document which allow simple and rapid access to related documents. Using a system known as the HyperText Markup Language ("HTML"), pages of information in the WWW contain pointers to other pages, those pointers typically being a key word (commonly known as a hyperlink word). When a user selects one of those key words, a hyperlink is created to another information layer (which may be in the same, or a different information server), where typically additional detail related to that key word will be found.

In order to facilitate implementation of the WWW on the Internet, new software tools have been developed for user terminals, usually known as Web Browsers, which provide a user with a graphical user interface means for accessing information on the Web, and navigating among information layers therein. A commonly used such Web Browser is that provided by Netscape.

The substantial growth in the use of computer networks, and particularly the WWW, for such information transactions, has predictably led to significant commercialization of this communications medium. For example, with the WWW, a user is not only able to access numerous information sources, some public and some commercial, but is also able to access "catalogs" of merchandise, where individual items from such a catalog can be identified and ordered, and is able to carry out a number of banking and other financial transactions. As will be obvious, such commercial transactions will typically involve sensitive and proprietary information, such as credit card numbers and financial information of a user. Thus, with the growth of commercial activity in the Internet, has also come a heightened concern with security.

It is well known that there are persons with a high level of skill in the computer arts, commonly known as "hackers", who have both the ability and the will to intercept communications via the Internet. Such persons are thereby able to gain unauthorized access to various sensitive user information, potentially compromising or misappropriating such information.

The vulnerability of such sensitive user information to misuse when so transmitted via the Internet is a phenomena which has only recently received wide public attention. Unless such security concerns can be quickly addressed and alleviated, the commercial development of this new communications medium may be slowed or even stalled altogether.

SUMMARY OF THE INVENTION

Accordingly, it is an object of the invention to provide an acceptable level of security for sensitive or proprietary information associated with information transactions in a public network, such as the Internet. That object is realized through an arrangement whereby an on-line information transaction is bifurcated between a generalized information access portion of such a transaction and an exchange of sensitive user information. With such a bifurcation, the generalized information access portion of the transaction, which generally would constitute the more substantial (in terms of network resources) portion of the transaction would be handled via a non-secure network, usually a public network such as the Internet. The portion of the transaction involving sensitive user information, on the other hand, would be handled by a separate secure connection, such as a private network, or intranetwork. An important characteristic of this bifurcation arrangement is the provision of a means for automated reconfiguration of a user terminal as between accessing the generalized information via the non-secure network and access to the secure communications network for the exchange of sensitive user information. Such an automated reconfiguration will be carried out without the necessity for any action on the part of the user, and indeed will be largely invisible to the user. In a further embodiment of the invention, a transfer of data is provided from a public to a private network, wherein data selected by a user from a public net-

Petitioner Apple Inc. - Exhibit 1026, p. 860

work site may be arranged and displayed at a user terminal and, subject to further user selection/confirmation activity, thereafter transferred to a private network.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 depicts an illustrative case of information transactions carried out via a public network such as the Internet.

Figure 2 shows the architecture of a browser as would typically be applied for accessing a hypermedia web page.

Figure 3 illustrates the primary elements of the reconfigurable dual-path method of the invention.

Figure 4 depicts in flow chart form the basic jump capability of the methodology of the invention.

Figures 5A & 5B (generally designated collectively herein as "Figure 5") depict in flow chart form the "shopping cart" capability of the methodology of the invention.

Figure 6A & 6B (generally designated collectively herein as "Figure 6") depict in flow chart form the stored configuration capability of the methodology of the invention.

Figure 7A & 7B (generally designated collectively herein as "Figure 7") depict in flow chart form the off-line form capability of the methodology of the invention.

DETAILED DESCRIPTION

For clarity of explanation, the illustrative embodiment of the present invention is presented as comprising individual functional blocks. The functions these blocks represent may be provided through the use of either shared or dedicated hardware, including, but not limited to, hardware capable of executing software.

Figure 1 depicts an illustrative case of information transactions carried out via the Internet. As seen in the figure, an exemplary user obtains access to the Internet by First connecting, via a Terminal **110** having an associated Browser **111**, to an Internet Service Provider **112** selected by the user. That connection between the user and the Internet Service Provider will typically be made via the Public Switched Telephone Network (PSTN) from a modem associated with the user's Terminal to a network node in the Internet maintained by the selected Internet Service Provider.

Once the user has obtained access to the selected Internet Service Provider, an address is provided for connection to another user or other termination site and such a connection is made via the Internet to that destination location. As can be seen from the figure, communication via the Internet may be either user-to-user, as from Terminal **110** to Terminal **130**, or from a user to a node representing an information source accessed via the Internet, such as Public Site **120**.

It will of course be understood that the Internet provides service to a large number of users and includes a large number of such Public Sites, but the illustration provides the essential idea of the communication paths established for such Internet communication. It will also be understood that a number of service classifications are supported by the Internet, with the World Wide Web service, which represents a preferred embodiment for the public network aspect of the method of the invention, being one of the currently most heavily trafficked of such services.

The Web Browser, such as depicted at **111**, can be seen as a software application operating in conjunction with a user terminal (such as Terminal **110**) which provides an interface between such a user terminal and the particular functionality of the WWW information site. The architecture of such a browser is generally described in terms of three main components, as illustrated in Figure 2. At the top level is the Browser **201**, which enables the acquisition of information pages from a WWW server (beginning, in all cases, with the "home page" for that server), for display at a display device associated with the terminal. The Browser also provides the necessary interface for the terminal with the HTML functionality used by the server to provide access to other linked information layers.

The second level of the browser architecture is the TCP/IP Stack **202**, which handles the communications protocols used for connecting the terminal to the WWW server. The bottom level of this architecture is the Dialer **203**, which typically handles the function of providing dialing and setup digits to a modem, as illustrated at **204**, such a modem generally being a part of the terminal. Normally, upon receiving dialing and other setup information from the dialer, the modem would cause a connection to be made via the PSTN to the Internet Service Provider selected for that terminal.

After a connection is established in this manner to the Internet Service Provider, an address would be provided for the WWW information node sought to be contacted, a connection to that node made through the Internet, and the home page for that node caused to be displayed at the terminal's display device. A user would then select a key word in that home page, typically by clicking on the word with a mouse or similar device, and, upon transmission of that selection signal to the WWW server, a hyperlink would be created to the linked information layer and the open page of that layer would be caused to be displayed at the user terminal.

As explained above, serious questions have been raised in respect to the security of communications via the public Internet. (Note, that the discussion herein is focused on the Internet, and particularly the WWW functionality of the Internet, as a preferred embodiment of such public data communication networks generally, but the methodology of the invention will be applicable to any such network.) To address this problem, the methodology of the invention begins with a bifurcation of the information transaction between a user and the selected information transaction provider into a por-

Petitioner Apple Inc. - Exhibit 1026, p. 861

tion related to sensitive or proprietary user information, and other information comprising that transaction. With such a bifurcation, it becomes possible to provide substantial security for that proprietary information by use of an alternative communications path for that separated portion of the transaction via a private network, or intranetwork -- *i.e.*, a connection between a user's terminal and a secure serving node on that private network. It is anticipated that a coordination means will be established in respect to the management of information among the public and private network elements of the bifurcated information transaction.

In its basic form, this methodology may be carried out by the user terminal initiating a call via the Internet to a selected WWW node, and upon establishing connection to that node, proceeding with the desired information transaction up to the point where an exchange of sensitive or proprietary information were required. At that point the user terminal would be instructed by the WWW server to terminate that connection (*i.e.*, hangup) and to place a new call to an identified private network server for the necessary exchange of sensitive information.

However, in order to accomplish such a dual-path transaction, it is necessary that the browser at the user terminal be reconfigured to provide the dialing, authorization (*i.e.*, login and password), and other needed information for accessing the alternative private network, in order to implement the proprietary portion of the transaction. It will also usually be the case that, upon completion of that private-network transaction, the original dialer, stack and browser configurations will need to be restored, in order for the terminal to retain its normal Internet access functionality. Such a reconfiguration and subsequent restoral of the necessary parameters in the browser, stack and dialer is likely to be well beyond the capabilities of the average user.

Accordingly, as a further embodiment of the inventive methodology, an automated browser reconfiguration means is provided which interoperates with the browser. This browser reconfiguration means is described in detail hereafter and will be referred to as the "Bridging Software".

Figure 3 provides an illustration of the primary elements of the reconfigurable dual-path method of the invention. As seen in the figure, a first path comparable to the Internet link shown in Figure 1, between User Terminal **301** and WWW Serving Node **330** (via Browser **302**, Modem **303**, Internet Service Provider **310**, and Internet **320**) is provided. However, an alternative path is now provided from the output of Modem **303** to Private Server **350**. That path is illustrated as being via the PSTN, which is generally regarded as being highly secure, but an alternative dedicated or other more-secure path between the User Terminal **301** and the Private Server **350** could as well be provided. In keeping with the discussion above, Browser **302** shown in Figure 3 would also include the Bridging Software installed as a helper application for implementing the automatic reconfiguration of the Browser.

In the operation of this system, a user would normally make an initial connection to an Internet application, such as the application represented by WWW Serving Node **330**, which, *e.g.*, might be a shopping application, a financial transaction, or the provision of an enrollment form for off-line preparation. After conducting all, or some portion of an information transaction short of an exchange of sensitive or proprietary information, including a capture by the user's terminal of needed information from the public site, a user provides a signal indicative of an end to that portion of that transaction. During the course of the public portion of the information transaction, specially configured files are sent from the WWW serving node to the Bridging Software associated with Browser **302**. Such files contain instructions for the Bridging Software to store information-like products -- e.g., for selected items from a catalog, forms for enrollment, or non-secure portions of a financial transaction, and reconfiguration information for dialing and logging into the private portion of the transaction. The Bridging Software then hangs up the Internet connection, edits the user terminal's browser, stack and dialer files to reconfigure the terminal to connect to the private server. Prior to automatic redialing of the new private site for the user, the Bridging Software may be instructed by the application operating at WWW Server Node **330** to display items chosen for purchase, or to display a form for the end-user to complete off-line before dialing the private application. Upon connecting to the private application and completing the transaction as to the user sensitive information in a private environment, the Bridging Software then restores the end-user software to the dialing and authorization parameters required to dial to the public Internet.

A particularly advantageous application of the automated reconfiguration and information transfer methodology of the Bridging Software is that it adds value to certain WWW servers which do not possess the Common Gateway Interface ("CGI") capability -- *i.e.*, a provision of specialized functions on the server beyond just displaying HTML files, and are accordingly unable to accomplish any transactional processing in respect to items selected by a user. In effect, such a non-CGI server, on its own, can only serve as a "billboard" for the items represented in its database.

However, with the collection and redelivery process of the Bridging Software, a data capture and processing mechanism can be implemented for servers operating in a non-CGI environment -- such servers being incapable of more than the simple delivery of static data packets corresponding to available items. The data set enabled by the Bridging Software is a mechanism for augmenting such limited server capabilities by defining a flexible mechanism for the receipt, display, and delivery of arbitrary data from one site to another.

In such a scenario, the Bridging Software receives a "shopping cart" item list from the host as a data-set defined with a static MIME data packet associated with the Bridging Software. This information comprising the data-set may be updated, displayed to the user in a "read-only" fashion, or presented to the user for order selection.

Petitioner Apple Inc. - Exhibit 1026, p. 862

During the process of interacting with the WWW server, a user may trigger HTML links resulting in additional MIME packets for the Bridging Software being delivered to the client. These packets allow items to be added and/or removed from the specified data set or presented to the user for local confirmation. The user will interact with a pop-up screen provided by the Bridging Software which presents the items available with product information, such as part number, description, unit cost, etc. The user identifies those items which are to be placed into the "shopping cart" and the quantity of items desired. Upon completion of the form, the Bridging Software stores the order in a format suitable for subsequent delivery to the private server site.

An additional feature provided by the methodology of the Bridging Software is an automated mechanism for providing compatibility with user terminals not previously having the Bridging Software included with the terminal's browser. To that end, the Bridging Software located at an accessed public network site initially checks to see if the browser counterpart for that software is loaded at the calling user terminal. If yes, the heretofore described processes of the Bridging Software go forward. If not however, a request is sent through the public host to download the Bridging Software to the calling terminal. After such a download, a helper application loads the Bridging Software to the terminal's browser.

I. Illustrative Embodiments

A variety of browser reconfiguration applications are supported by the automated browser reconfiguration means of the invention. Four essentially diverse capabilities of this invention, which support such applications, are described hereafter as illustrative embodiments of the invention.

A. Basic Jump Capabilities

In this configuration, which is illustrated in flow chart form in Figure 4, an end-user is connected to a chosen WWW serving node (where a desired information product is made available) via a modem and an Internet browser associated with the user's terminal (**Step 401** of Figure 4). After conducting an information transaction with the selected WWW serving node for some interval (determined in relation to the specific application accessed), the user clicks on a hypertext link, or picture, to begin an automated process which will cause that public session to be terminated and a new connection established to an alternate private data network (**Step 402**).

In response to that user action, a data message containing parameter reconfiguration instructions is passed from the WWW server application to the Bridging Software at the user's terminal (**Step 403**). Upon receiving such instructions, the Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network (**Step 404**). This reconfiguration is fully automatic and transparent to the user, and includes parameters such as modem dial number, login, password, and TCP/IP addresses. At that point, the Bridging Software causes the modem to disconnect the current data network connection, shutting down the browser, and to then dial the alternate private data network (**Step 405**).

With the establishment of a connection to the private server on the alternate data network, the user interacts with the alternate data network application as appropriate (**Step 406**), and after an interval completes his activity with the alternate data network and provides an indication of such completion (**Step 407**). A data message containing parameter reconfiguration instructions is then passed from the alternate data network application to the Bridging Software (**Step 408**).

At that point, the Bridging Software again edits the user's on-line communications software parameters, reconfiguring them to dial the original public data network, or another preselected network (**Step 409**). As with the first reconfiguration, this configuration is automatic and includes parameters such as modem dial number, login, password, and TCP/IP addresses. The Bridging Software automatically causes the current private data network to be disconnected by the modem (**Step 410**), and if appropriate, causes the original public data network to be redialed (**Step 411**). When such a reconnection to the public data network is established, the end-user would then continue his application in the public data network.

B. "Shopping Cart" Capability

With this configuration, illustrated in flow chart form in Figure 5, a user begins by establishing a connection to a WWW application (assuming for the moment that the application is non-CGI enabled) at a serving node for that application, using the Internet browser and modem associated with the user's terminal (**Step 501** of Figure 5). Upon finding an item in that application to be saved, or remembered for later consideration, or purchase, the user clicks on a hypertext link, or picture, representing that item (**Step 502**). That application then sends a data message to the Bridging Software containing information about the items selected (**Step 503**) and such information is stored by the Bridging Soft-

Petitioner Apple Inc. - Exhibit 1026, p. 863

ware in the "shopping cart" file in the user's terminal (**Step 504**). Such selection download and storage steps (*i.e.*, steps 502, 503 & 504) are repeated for as many items as the user chooses to select. At any point after the Bridging Software has received the first set of item selection information, the user can instruct the Bridging Software to cause those selected items about which such information has been received to be displayed locally (at the user's terminal), where the user may review or edit (including deletion if desired) the collection of items theretofore selected. The application may also control display characteristics such as color and font for such locally displayed items. Note that in the case of a CGI-enabled application, the application itself will keep track of the items selected by the user and only download the totality of the selected items at the end of the selection process, and accordingly, the described local display option will not be applicable to such a CGI-enabled application.

At the point of completion of his "shopping", the user clicks on a hyper-text link or picture to "check out" (**Step 505**), which will begin a process of causing a jump to an alternate data network for the completion of sensitive portions of the transaction. To that end, a data message containing parameter reconfiguration instructions is passed from the WWW application to the Bridging Software (**Step 506**). It is to be noted that, as a security measure, information such as the new dial number, IP address, home page, configuration data (*e.g.*, login, password, DNS address) may be passed over the public network in encrypted form.

Upon receiving such reconfiguration instructions, the Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network (**Step 507**). This reconfiguration is fully automatic and transparent to the user, and includes parameters such as modem dial number, login, password, and TCP/IP addresses. At that point, the Bridging Software causes the modem to disconnect the current data network connection, shutting down the browser, and to then dial the alternate data network (**Step 508**).

The Bridging Software passes the stored "shopping cart" data captured from the WWW application to the alternate network application (**Step 509**), where that data may be displayed for the user, permitting the user to confirm and/or modify the data (**Step 510**). The user interacts with the alternate data network application as appropriate, and after an interval completes his activity with the alternate data network (**Step 511**) and thus, by providing an appropriate completion signal to the application, completing the private portion of the information transaction (**Step 512**). A data message containing parameter reconfiguration instructions is then passed from the alternate data network application to the Bridging Software (**Step 513**).

The Bridging Software, at this point, again edits the user's on-line communications software parameters, reconfiguring them to dial the original (or another pre-defined) data network (**Step 514**). As with the first reconfiguration, this configuration is automatic and includes parameters such as modem dial number, login, password, and TCP/IP addresses. The Bridging Software automatically causes the current private data network to be disconnected by the modem (**Step 515**), and if appropriate, causes the original public data network to be redialed (**Step 516**). When such a reconnection is established to the point in the public data network where the user had left off to handle the secured aspects of his information transaction, the user would then continue his application in the public data network.

C. Stored Configuration Capabilities

For this configuration, depicted in flow chart form in Figure 6, an end-user is connected to a chosen WWW serving node (where a desired information product is made available) via a modem and an Internet browser associated with the user's terminal (**Step 601** of Figure 6). The user selects a hypertext link or picture associated with the WWW application by clicking on such link or picture (**Step 602**). A data message containing parameter reconfiguration instructions and an application icon (related to the selected hypertext link or picture) is passed from the WWW application to the Bridging Software (**Step 603**).

The Bridging Software creates an icon for display at the user's terminal, and saves a Bridging Software configuration file that is associated with that icon (**Step 604**). Such Bridging Software actions are automatic and multiple selections may he captured in this manner. At this point the user may continue the on-line session, or, if all desired selections have been made, a signal is provided from the user that the session should be discontinued (**Step 605**). The Bridging Software then automatically disconnects the current data network connection (**Step 606**).

After disconnecting from the WWW application, and following an interval determined by the user, a new application is selected by the user by clicking on the appropriate new icon displayed at the user's terminal (**Step 607**). The Bridging Software receives the reconfiguration instructions from the file associated with the selected icon (**Step 608**).

The Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network (**Step 609**). The Bridging Software then automatically starts the user's Internet browser software and causes the alternate network application to be dialed by the modem associated with that terminal (**Step 610**). Upon establishing a connection to the alternate network, the user interacts with that application and completes the transaction to the user's satisfaction (**Step 611**). After a signal is sent to the alternate network indicating such completion of the user's activity (**Step 612**), a data message containing parameter reconfiguration instructions is passed from the alternate data network application to the Bridging Software (**Step 613**). That Software then causes the user's

Petitioner Apple Inc. - Exhibit 1026, p. 864

terminal configuration parameters to be reset (**Step 614**) and the alternate data network to be automatically disconnected (**Step 615**).

D. Off-Line Form Capability

In this configuration, depicted in flow chart form in Figure 7, an end-user is connected to a chosen WWW serving node (where a desired information product is made available) via a modem and an Internet browser associated with the user's terminal (**Step 701** of Figure 7). The user selects a hypertext link or picture associated with an off-line form application -- an exemplary such form being an HTML-based form -- by clicking on such link or picture (**Step 702**). A data message containing parameter reconfiguration instructions for the Bridging Software, the selected off-line-form application, and an optional icon (related to the selected hypertext link or picture) is passed from the WWW application to the Bridging Software (**Step 703**). Note that the selected off-line form may be for either single or multiple use.

In the case of a delayed or multiple use of the selected form, the Bridging Software may create an icon for display at the user's terminal, and will save a Bridging Software configuration file that is associated with that icon (**Step 704**). The form in question is also saved on the user's terminal. Such Bridging Software actions are automatic. At this point the user may continue the on-line session, or, if all desired selections have been made, a signal is provided from the user that the session should be discontinued (**Step 705**). The Bridging Software then automatically disconnects the current data network connection (**Step 706**).

After disconnecting from the WWW application, two cases are to be considered as to the further processing of the selected form: (1) an immediate single use of the form and (2) either a delayed or multiple use of the form. In the first case, the Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network. The Bridging Software then automatically starts the user's Internet browser software which is caused to display the off-line form. The user then completes the off-line form and chooses a "Submit Form" button displayed at his terminal.

In the second case, the Bridging Software will have created an icon for display at the user's terminal and saved a Bridging Software configuration file associated with that icon. Following an interval determined by the user, the off-line-form application is started by the user by clicking on the new form icon displayed at the user's terminal (**Step 707**). The Bridging Software receives the reconfiguration instructions from the file associated with the selected icon (**Step 708**).

The Bridging Software edits the user's on-line communications software parameters, reconfiguring that software to dial the alternate data network (**Step 709**). The Bridging Software then automatically starts the user's Internet browser software which is caused to display the off-line form (**Step 710**). The user then completes the off-line form and chooses a "Submit Form" button displayed at his terminal (**Step 711**).

In either the first or second case, following activation of the "Submit Form" button, the alternate network application is then caused to be dialed by the Bridging Software. Upon establishing a connection to the alternate network, the form data is passed to the alternate network (**Step 712**). The user then interacts with that application and completes the application (**Step 713**). After a signal is sent to the alternate network indicating such completion of the user's activity (**Step 714**),a data message containing parameter reconfiguration instructions is passed from the alternate data network application to the Bridging Software (**Step 715**). That Software then causes the user's terminal configuration parameters to be reset (**Step 716**) and the alternate data network to be automatically disconnected (**Step 717**).

CONCLUSION

A system and method has been described for the automatic switching of an information transaction between two or more alternate networks. This functionality, which incorporates a reconfiguration means designated herein as the Bridging Software, supports the movement of application specific data from one on-line environment to another. Among potential applications of this process for passing data between different environments are: selected items for purchase ("shopping cart"), captured data from forms, and other server captured data such as web pages visited.

The Bridging Software reconfiguration means is intended to work with various Web Browser software implementations, including the Netscape Personal Edition (NPE) Software for Windows 3.1 and 3.11, and which represents a working embodiment for the invention. The Bridging Software installs itself as a helper application within the browser application and utilizes a special MIME type configuration file to pass reconfiguration and "shopping cart" information from the server to the client software.

When an application requires a user to re-connect to a private application, a reconfiguration file is passed to the Bridging Software helper application via a CGI script or simple hyper-text link. The helper application disconnects the current data connection, reconfigures the dial parameters (dial #, login password, DNS address, and home page) and initiates the dial program so the end-user can access the private application.

When the end-user connects to the private application, the Bridging Software reconfiguration means provides the new "private server" application with data collected from the "public server", and the application resumes in a private,

Petitioner Apple Inc. - Exhibit 1026, p. 865

secure environment.

The Bridging Software allows both short term and long term storage of dial configurations. Configurations passed to the Bridging Software can be designated as single use configurations and discarded after the application has terminated, or saved and displayed to the end-user as a dial choice by the Bridging Software.

Although the present embodiment of the invention has been described in detail, it should be understood that various changes, alterations and substitutions can be made therein without departing from the spirit and scope of the invention as defined by the appended claims. In particular, it is noted that, while the invention has been primarily described in terms of a preferred embodiment based on an automatic reconfiguration between a public and a private data network, any the methodology of the invention will be equally applicable to any set of alternate networks.

Claims

1. A method for managing a transaction via a communications path between a terminal device and a serving node in a data network, said method comprising the steps of:

   establishing an initial communications path via a first connection between said terminal device and a serving node in a first data network;
   receiving information from said serving node in said first data network for effecting a reconfiguration of said communications path for said transaction from said first connection in said first data network to a second connection in a second data network; and
   automatically connecting said terminal device to a serving node in said second data network via said second connection.

2. A method for managing a transaction via a communications path between a terminal device and a serving node in a data network, said method comprising the steps of:

   establishing an initial communications path via a first connection between said terminal device and a serving node in a first data network;
   selecting at least one information item from a data base of said information items provided at said serving node in said first data network;
   causing said selected information items to be downloaded to said terminal device via said first connection;
   receiving information from said serving node in said first data network for effecting a reconfiguration of said communications path for said transaction from said first connection in said first data network to a second connection in a second data network; and
   automatically connecting said terminal device to a serving node in said second data network via said second connection.

3. A method for managing a transaction via a communications path between a terminal device and a serving node in a data network, said method comprising the steps of:

   establishing an initial communications path via a first connection between said terminal device and a serving node in a first data network;
   identifying at least one data network application from a data base of said data network applications provided at said serving node in said first data network;
   receiving information from said serving node in said first data network for reconfiguring said terminal device for implementation of a communication path via an alternate connection between said terminal device and at least one of said identified data network applications in a second data network; and
   in response to a selection signal from a user, automatically connecting said terminal device to a selected one of said identified data network applications via said alternate connection.

4. A method for managing a transaction via a communications path between a terminal device and a serving node in a data network, said method comprising the steps of:

   establishing an initial communications path via a first connection between said terminal device and a serving node in a first data network;
   selecting an off-line form application from a data base provided at said serving node in said first data network;
   receiving information from said serving node in said first data network for reconfiguring said terminal device for implementation of a communication path via a second connection between said terminal device and said

Petitioner Apple Inc. - Exhibit 1026, p. 866

selected off-line form application in a second data network; and

in response to, a selection signal from a user, automatically connecting said terminal device to said selected off-line form application.

5. The method for managing a transaction of Claim 1 or 2 including the further step of recognizing a signal to reconfigure said communications path from said first connection to said second connection.

6. The method for managing a transaction of Claim 3 wherein said selected data network application is operated at a serving node in said second data network.

7. The method for managing a transaction of Claim 4 wherein said selected off-line form application is operated at a serving node in said second data network.

8. The method for managing a transaction of one of the Claims 1, 2, 6 or 7 wherein said serving nodes in said first and said second data networks are manifested in a common node.

9. The method for managing a transaction of Claim 1 or 2 wherein said step of receiving information includes the further step of effecting said reconfiguration of said communications path.

10. The method for managing a transaction of Claim 1 or 2 wherein said step of automatically connecting includes the step of automatically disconnecting said first connection prior to implementation of said second connection.

11. The method for managing a transaction of Claim 1 or 2 including the further steps of:

automatically disconnecting said second connection in response to a user signal; and

reconfiguring said terminal device to enable, in response to user instruction, an implementation of a connection via an identified data network.

12. The method for managing a transaction of Claim 11 wherein said step of automatically reconfiguring said terminal device includes the step of effecting said implementation of said connection via said identified data network.

13. The method for managing a transaction of Claim 2 wherein said step of causing said selected information items to be downloaded includes the further step of causing said selected information items to be displayed at said terminal device.

14. The method for managing a transaction of Claim 13 wherein said displayed selected items can be edited by a user at said terminal device.

15. The method for managing a transaction of Claim 13 wherein display characteristics for said displayed selected items can be controlled at said terminal device.

16. The method for managing a transaction of Claim 2 wherein said step of automatically connecting includes the step of uploading said selected information items from said terminal device to said service provider via said second connection.

17. The method for managing a transaction of Claim 3 including the further steps of:

automatically disconnecting said alternate connection in response to a user signal; and

reconfiguring said terminal device to enable implementation of a pre-selected connection between said terminal device and an identified data network.

18. The method for managing a transaction of Claim 17 wherein said step of automatically reconfiguring said terminal device includes the further step of effecting said implementation of said pre-selected connection.

19. The method for managing a transaction of Claim 4 including the further step of downloading from said serving node in said first data network to said terminal device of an off-line form related to said off-line form application.

20. The method for managing a transaction of Claim 4 including the further step of uploading said downloaded off-line

Petitioner Apple Inc. - Exhibit 1026, p. 867

form from said terminal device to said selected off-line form application, after processing by a user.

21. The method for managing a transaction of Claim 4 including the further steps of:

automatically disconnecting said connection to said selected off-line form application in response to a user signal; and
reconfiguring said terminal device to enable implementation of a pre-selected connection between said terminal device and an identified data network.

22. The method for managing a transaction of Claim 21 wherein said step of automatically reconfiguring said terminal device includes the further step of effecting said implementation of said pre-selected connection.

23. A method for managing connections between a terminal device and at least one information source/processor wherein at least two of said connections are implemented via separate communications networks, comprising the steps of:

recognizing a signal for connection to an information source/processor via a communications network other than a communications network for which a predetermined connection is configured;
causing said terminal device to implement a connection to said information source/processor via said other communications network; and
upon termination of said information source/processor connection via said other communications network, automatically reconfiguring a connection criteria in said terminal device to enable said terminal device to implement, in response to user instruction, a connection via an alternative one of said communications networks.

24. The method for managing connections of Claim 23 wherein said recognizing step occurs at a point when said terminal device is connected to a given source/processor.

25. The method for managing connections of Claim 23 wherein information items may be selected by a user at said terminal device from said given source/processor, and including the further step of causing said selected information items to be downloaded from said source/processor to said terminal device.

26. The method for managing connections of Claim 25 wherein said step of effecting connection includes the further step of uploading said selected information items from said terminal device to said other information source/processor.

27. The method for managing connections of Claim 26 wherein said selected information items are processed by said user at said terminal device prior to uploading to said other information source/processor.

28. The method for managing connections of Claim 24 including the further step of causing said given source/processor to download to said terminal device configuration data for enabling said step of effecting connection to said other information source/processor.

29. The method for managing connections of Claim 24 including the further step of causing said other source/processor to download to said terminal device configuration data for enabling said step of automatically restoring a prior connection criteria in said terminal device.

30. A method for enhancing security of certain data in an on-line information transaction comprising the steps of:

bifurcating said information transaction into a first portion comprising said certain data and a remaining portion, wherein said remaining portion is carried out via a public on-line communications connection between a terminal device and a public information server;
causing said first portion to be carried out via a secure private on-line communications connection between said terminal device and a private information server; and
automatically reconfiguring network access means in said terminal device to switch between said public connection and said private connection.

Petitioner Apple Inc. - Exhibit 1026, p. 868

FIG. 1

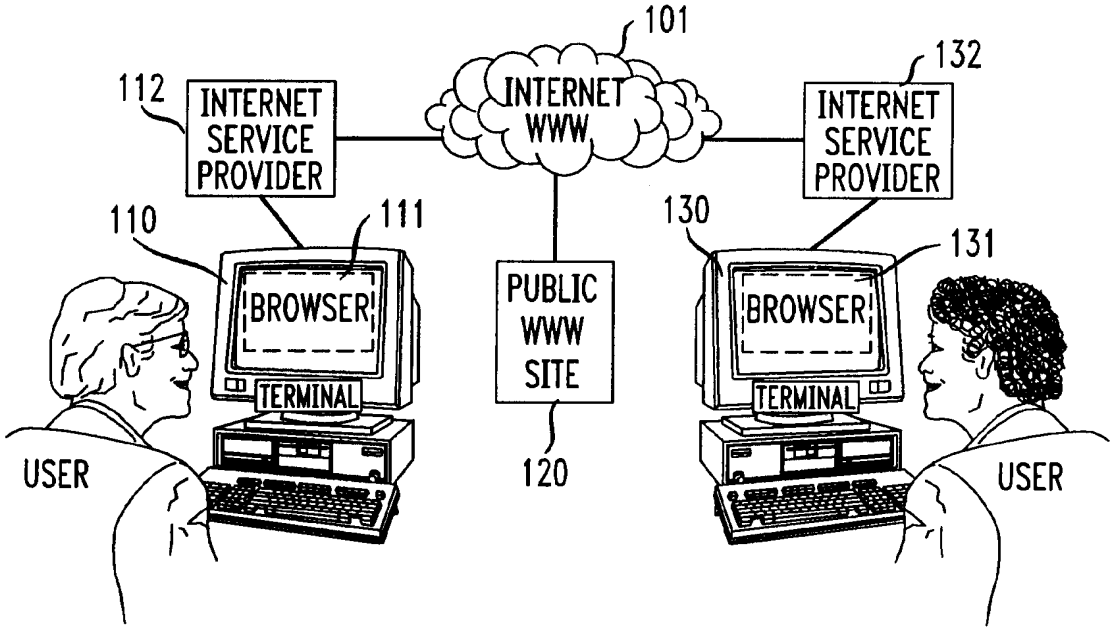
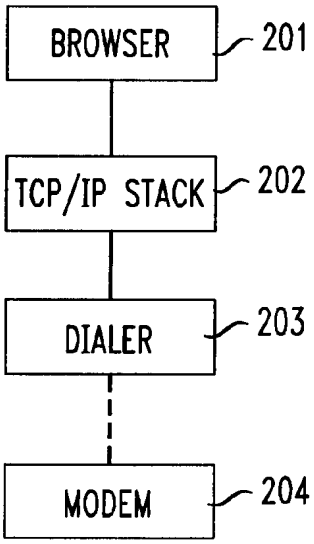
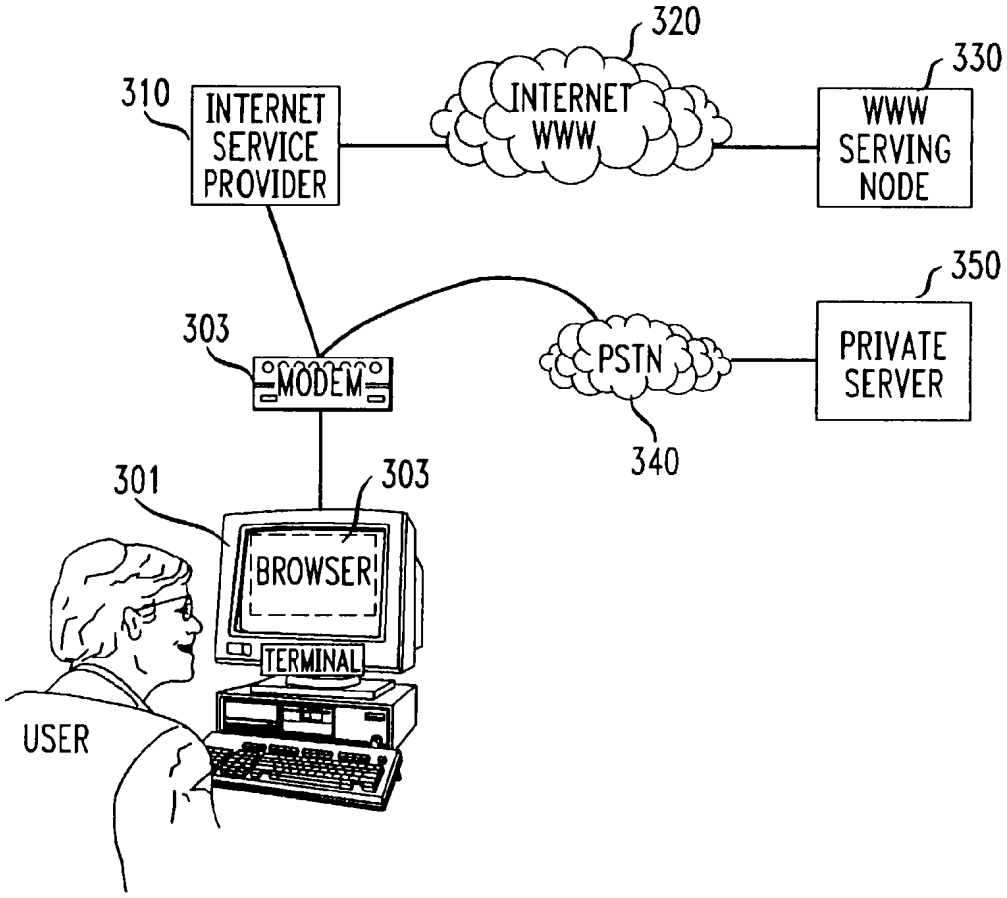


FIG. 2



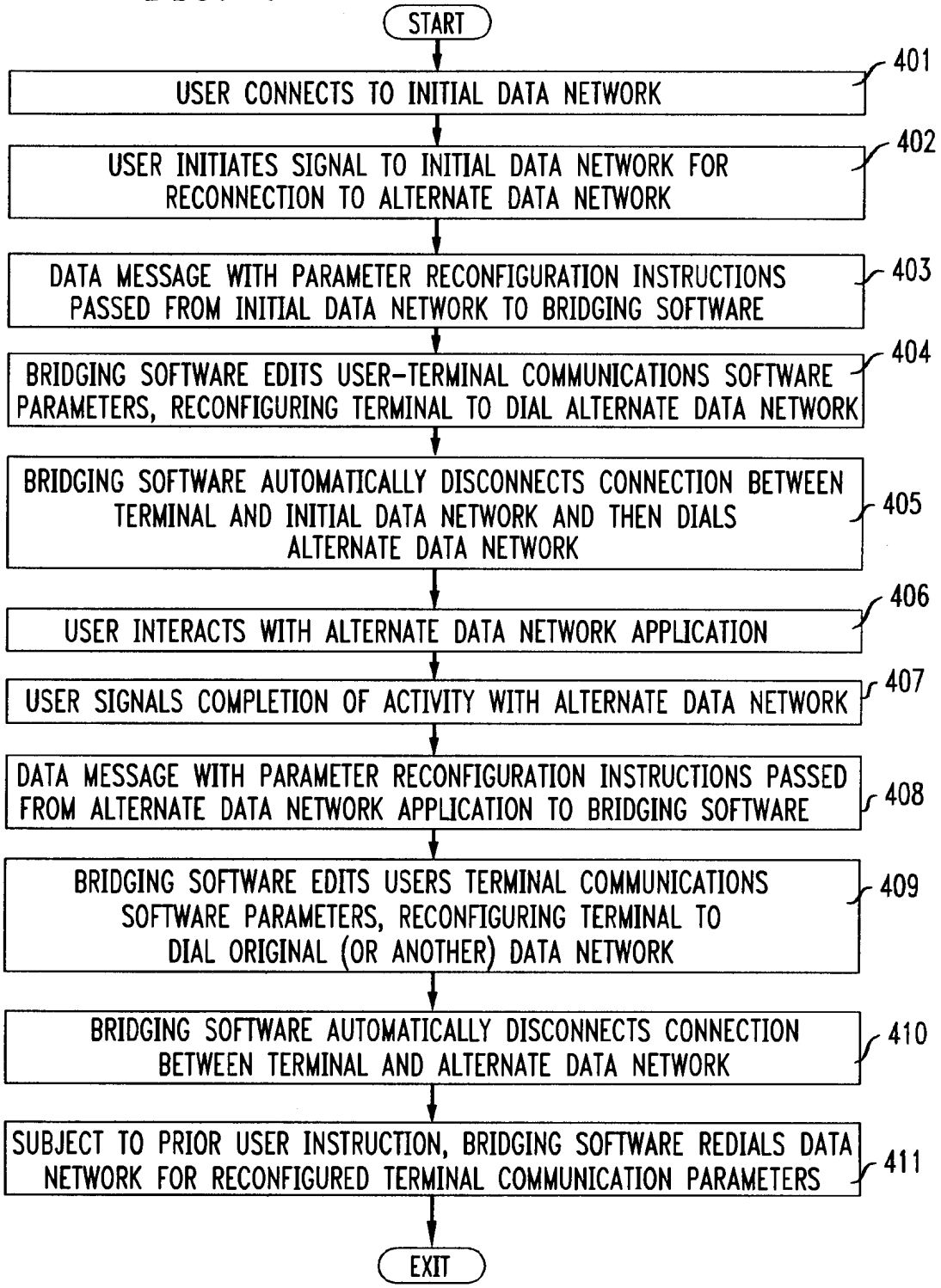
Petitioner Apple Inc. - Exhibit 1026, p. 869

FIG. 3



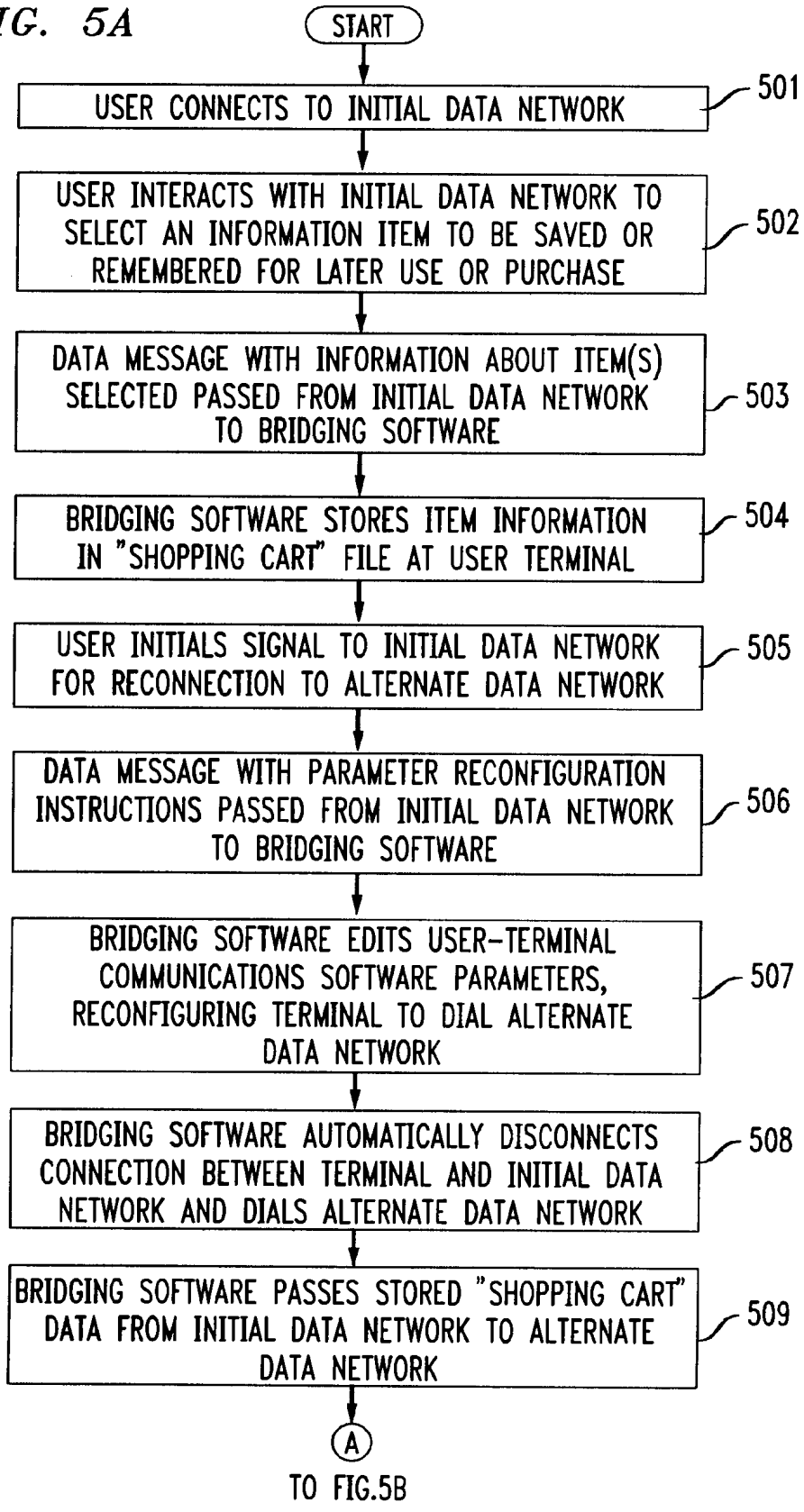
Petitioner Apple Inc. - Exhibit 1026, p. 870

FIG. 4



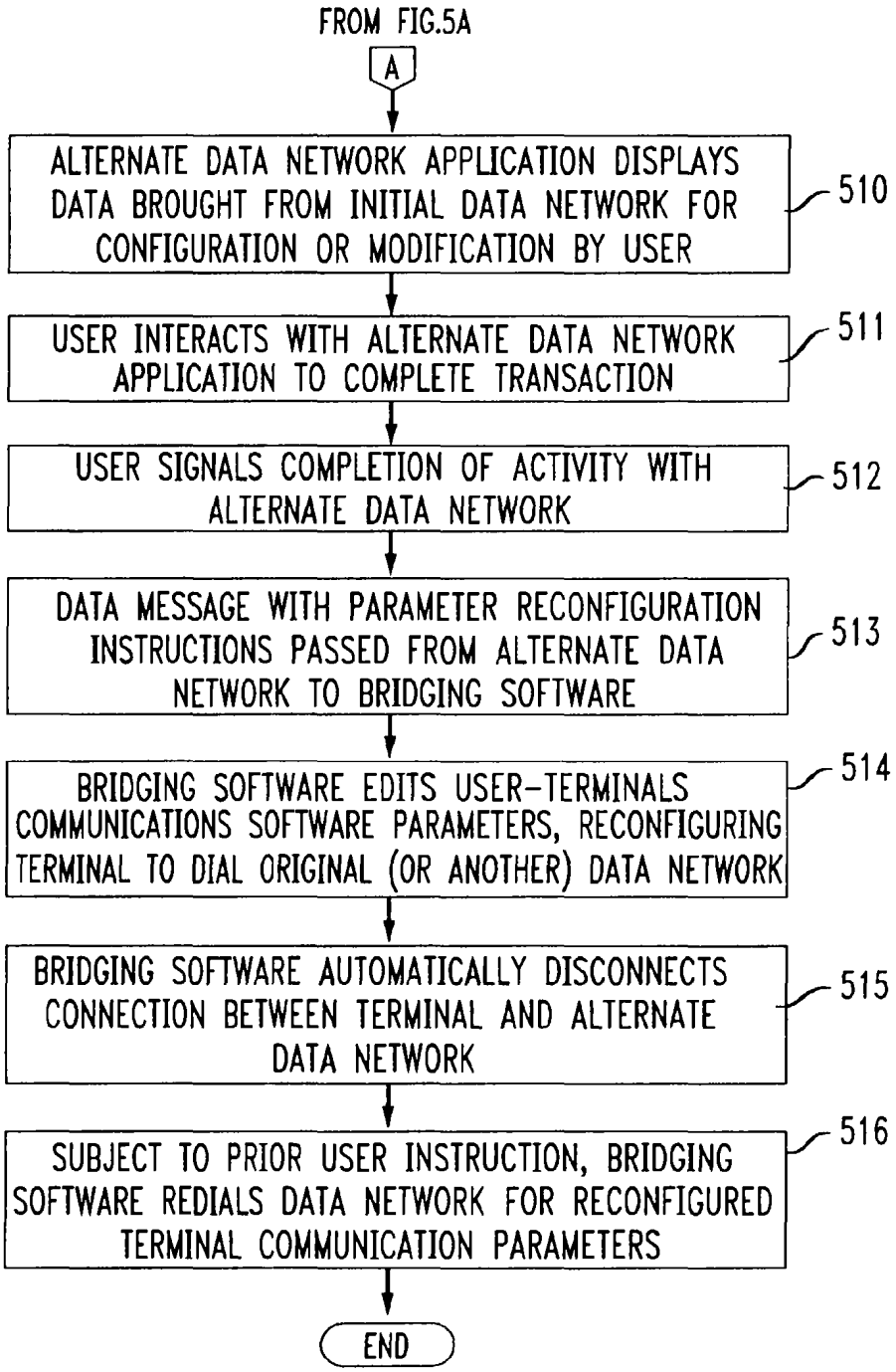
Petitioner Apple Inc. - Exhibit 1026, p. 871

FIG. 5A



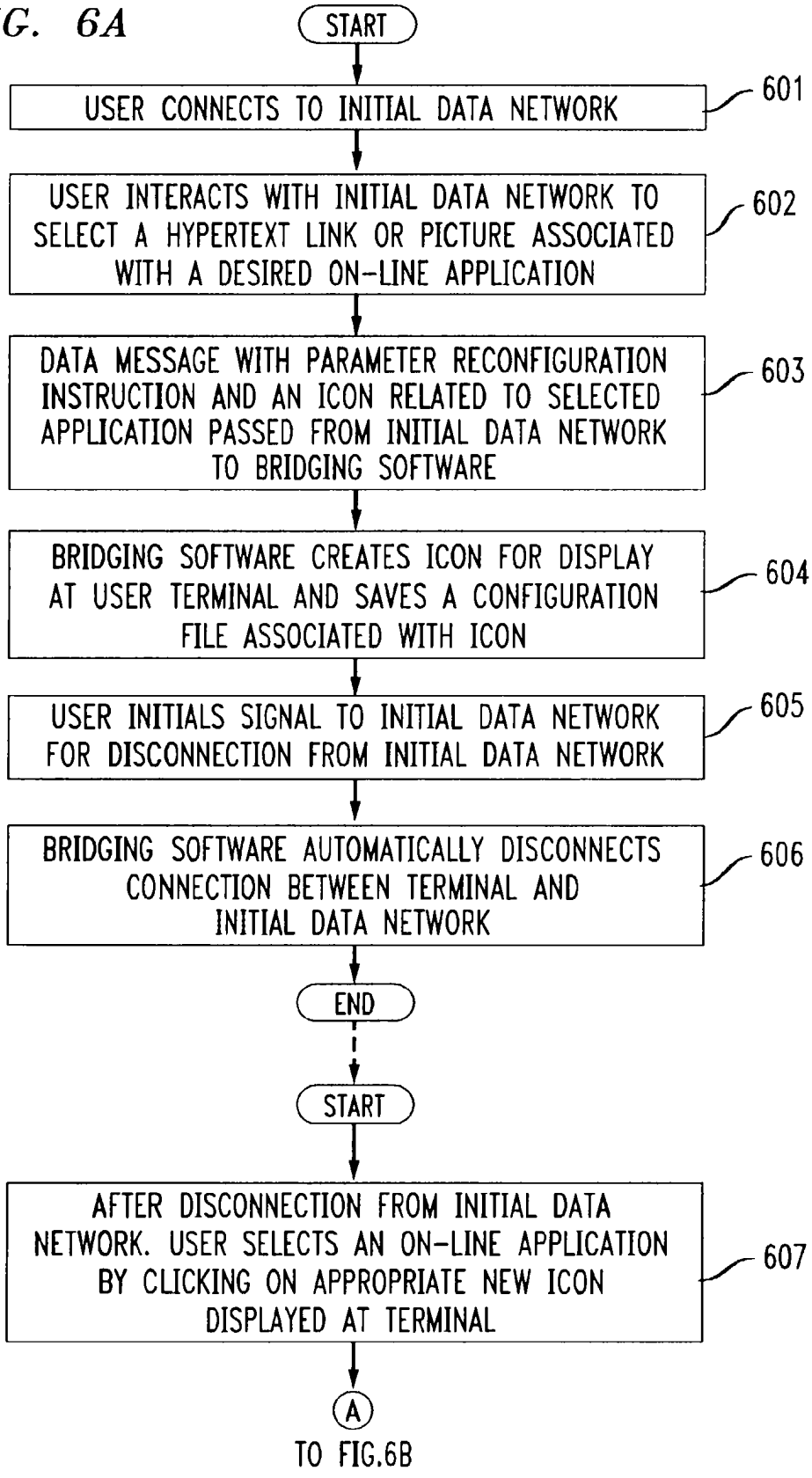
Petitioner Apple Inc. - Exhibit 1026, p. 872

FIG. 5B



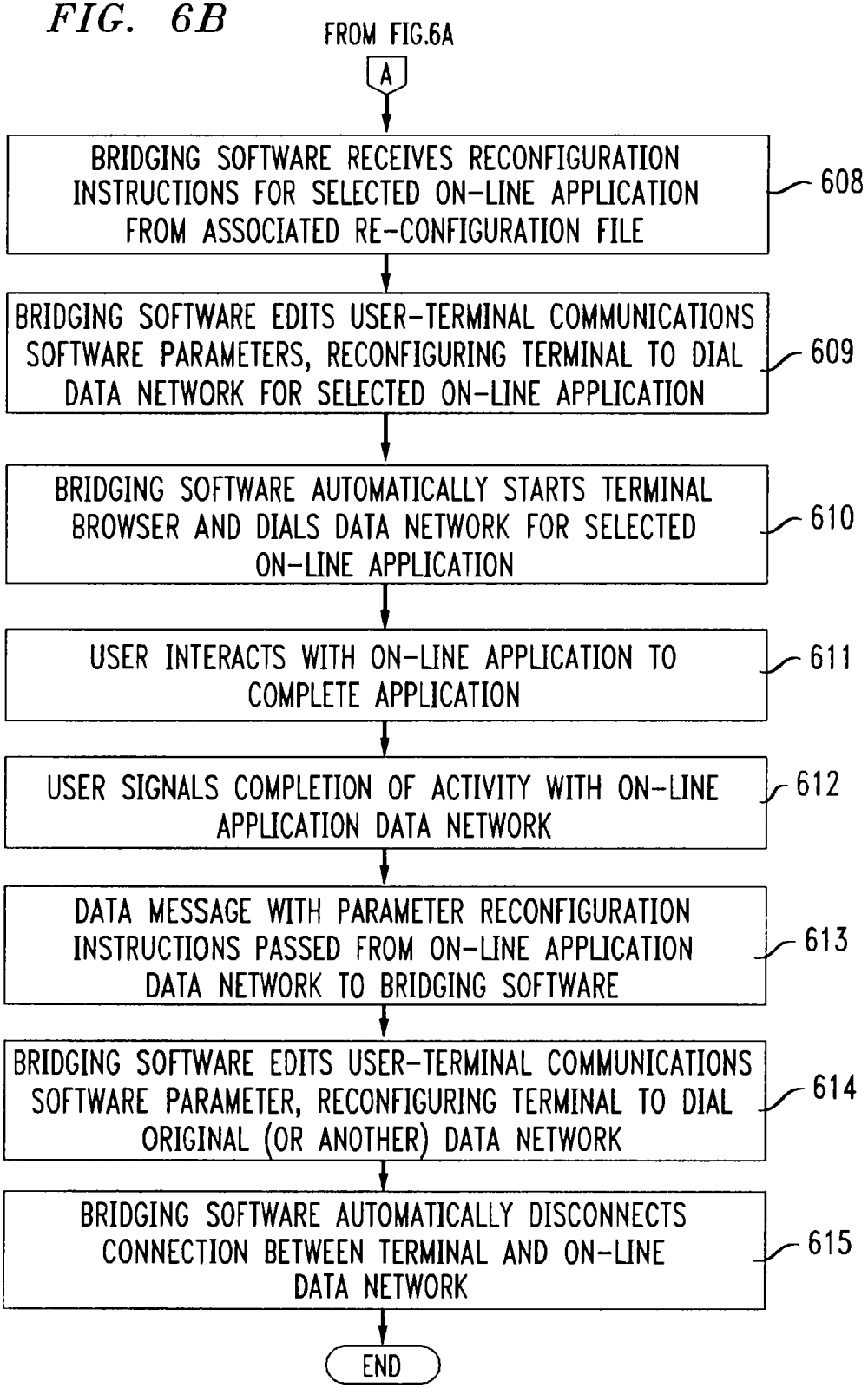
Petitioner Apple Inc. - Exhibit 1026, p. 873

FIG. 6A



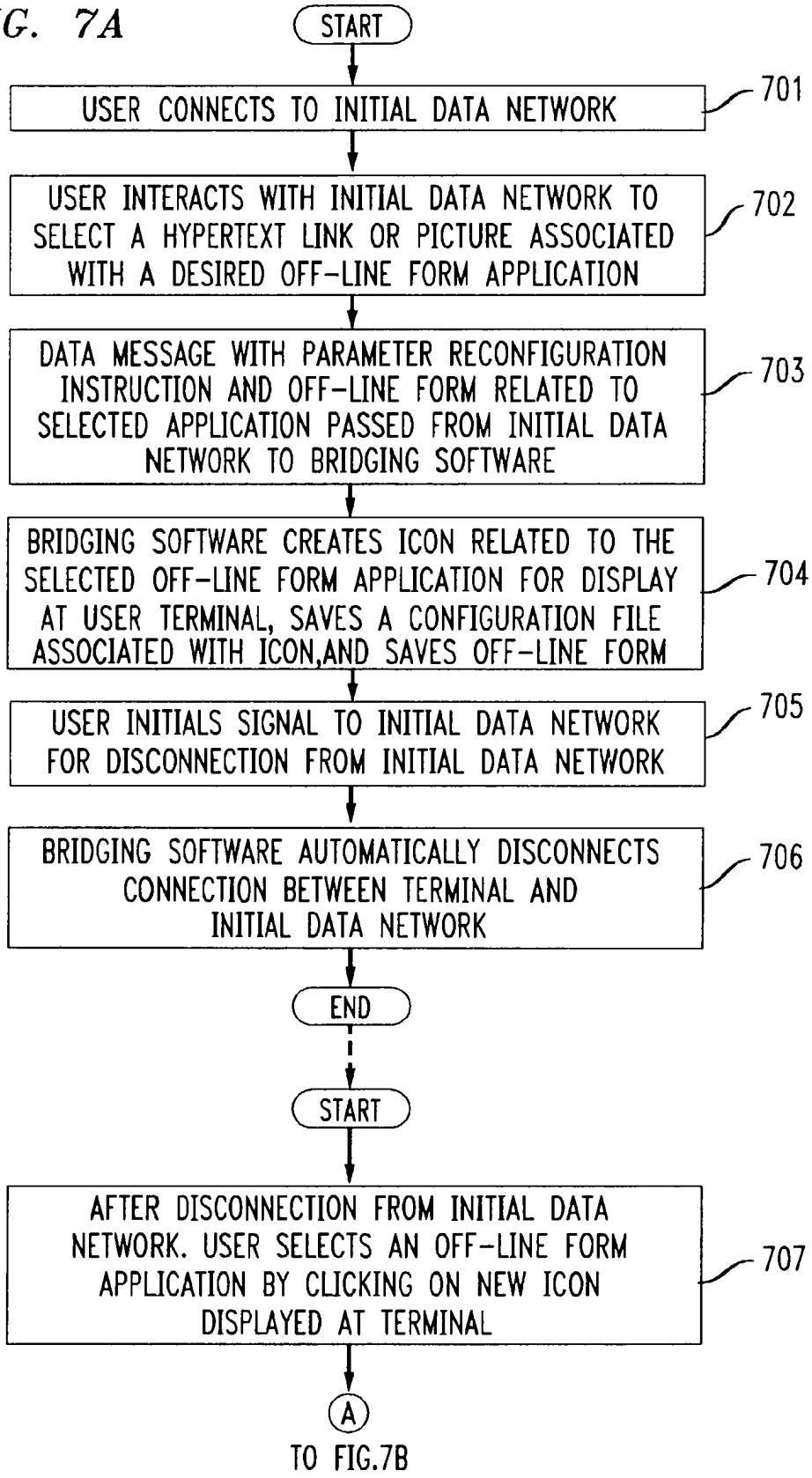
Petitioner Apple Inc. - Exhibit 1026, p. 874

FIG. 6B



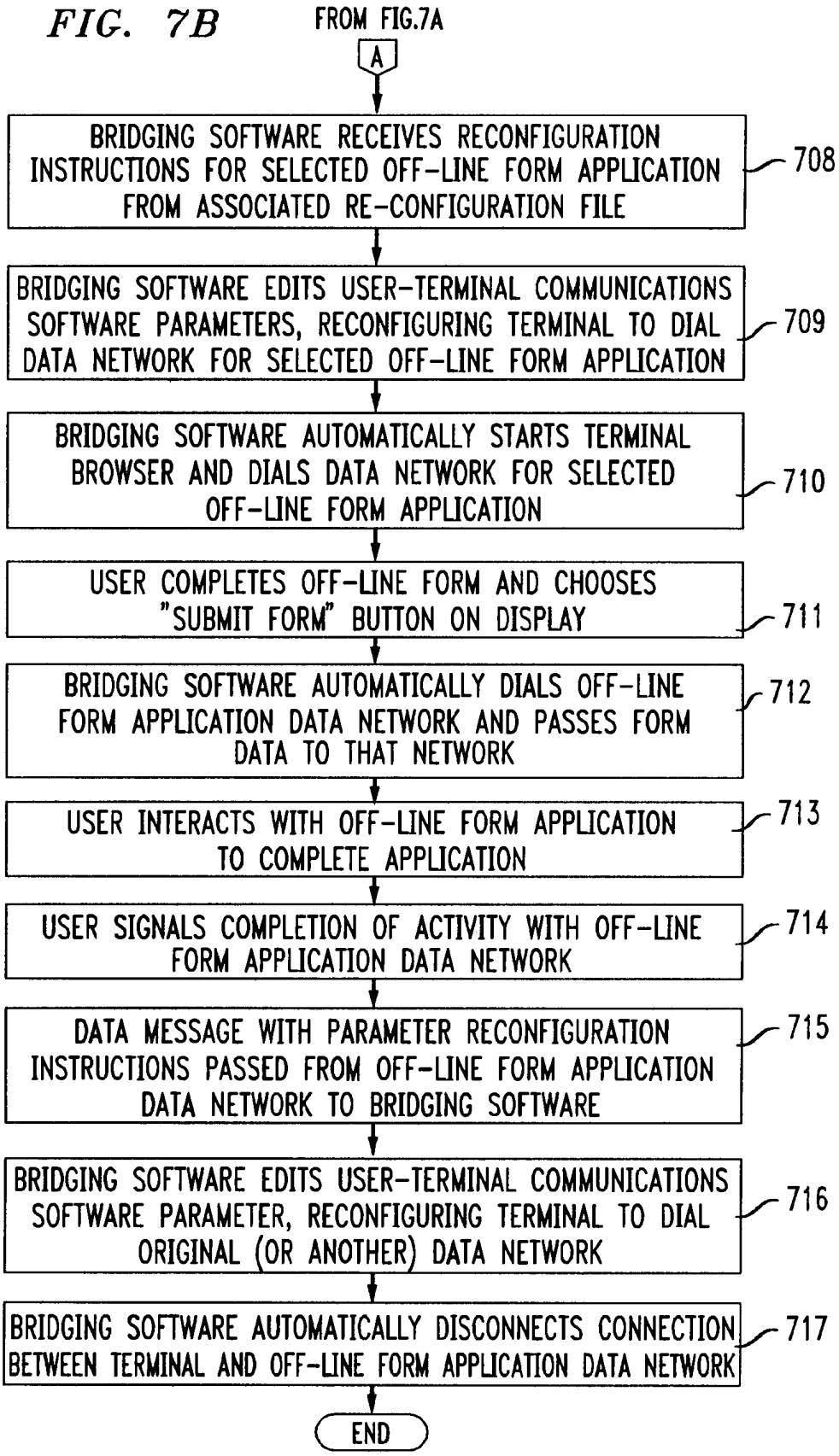
Petitioner Apple Inc. - Exhibit 1026, p. 875

FIG. 7A



Petitioner Apple Inc. - Exhibit 1026, p. 876

FIG. 7B



Petitioner Apple Inc. - Exhibit 1026, p. 877

(12) UK Patent Application (19) GB (11) 2 317 792 (13) A

(43) Date of A Publication 01.04.1998

(21) Application No 9719816.2

(22) Date of Filing 17.09.1997

(30) Priority Data
(31) 08715343 (32) 18.09.1996 (33) US
08715668 18.09.1996

(71) Applicant(s)
Secure Computing Corporation

(Incorporated in USA - Delaware)

2675 Long Lake Road, Roseville,
Minnesota 55113-2536, United States of America

(72) Inventor(s)
Spence Minear
Edward B Stockwell
Troy De Jongh

(74) Agent and/or Address for Service
Beresford & Co
2-5 Warwick Court, High Holborn, LONDON,
WC1R 5DJ, United Kingdom

(51) INT CL^6
H04L 9/00

(52) UK CL (Edition P)
H4P PPEB
U1S S2124 S2209

(56) Documents Cited
WO 97/26735 A1 WO 97/26734 A1 WO 97/26731 A1
WO 97/23972 A1 WO 97/13340 A1

(58) Field of Search
UK CL (Edition P) **H4P PDCSA PDCSC PPEB**
INT CL^6 **H04L 9/00 9/32 29/06 29/08**
Online: WPI, INSPEC

(54) **Virtual Private Network for encrypted firewall**

(57) A system (10) for regulating the flow of messages through a firewall (18) having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer where if the message is not encrypted, it passes the unencrypted message up the network protocol stack to an application level proxy (50), and if the message is encrypted, it decrypts the message and passes the decrypted message up the network protocol stack to the application level proxy. The step of decrypting the message includes the step of executing a process at the IP layer to decrypt the message.

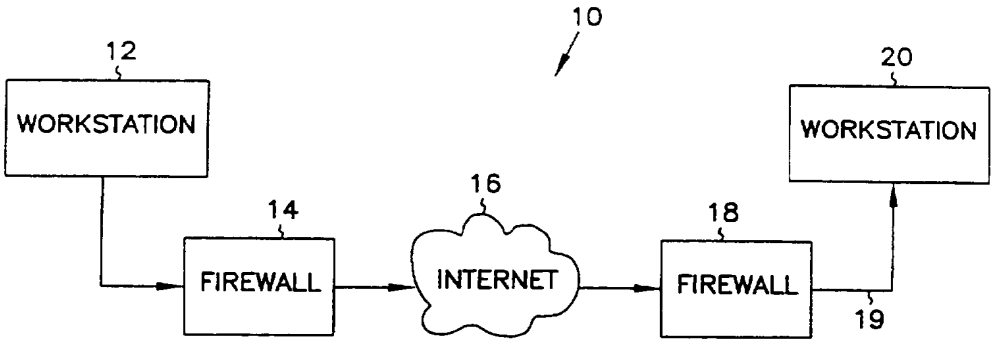


FIG. 1

GB 2 317 792 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

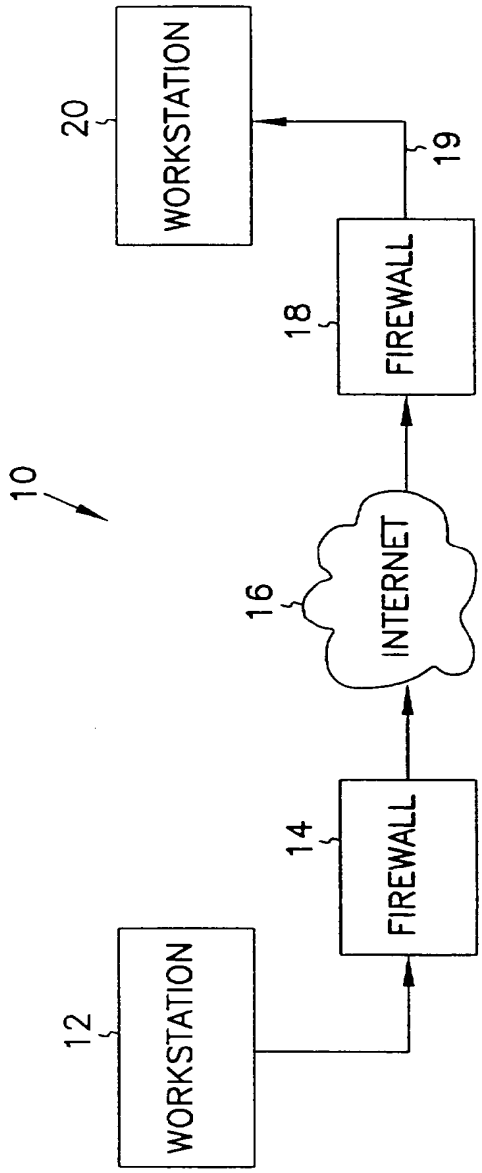

10
12
WORKSTATION
14
FIREWALL
16
INTERNET
18
FIREWALL
19
20
WORKSTATION

FIG. 1

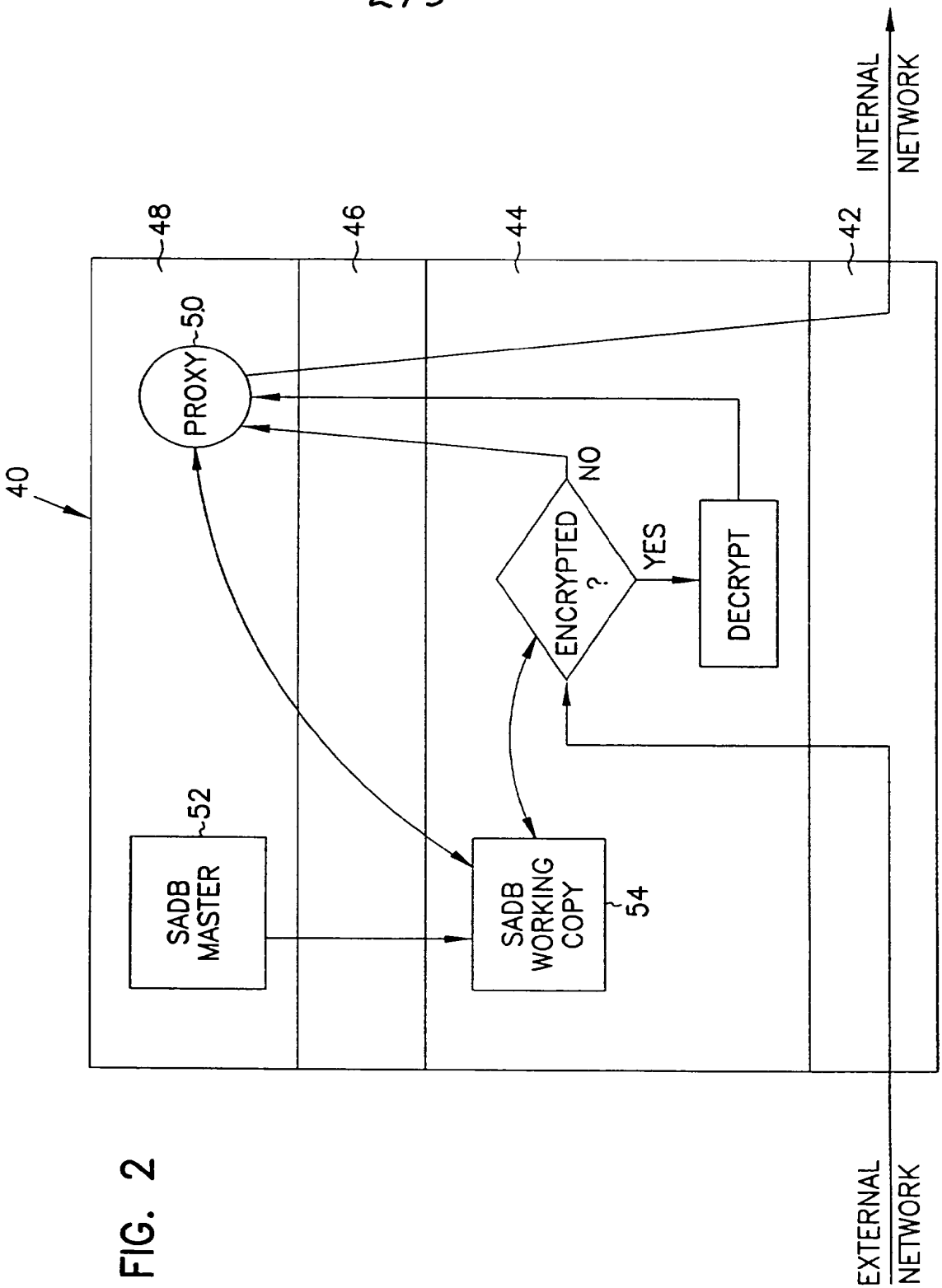

40
48
46
44
42
INTERNAL NETWORK
PROXY
50
NO
ENCRYPTED ?
YES
DECRYPT
SADB MASTER
52
SADB WORKING COPY
54
EXTERNAL NETWORK

FIG. 2

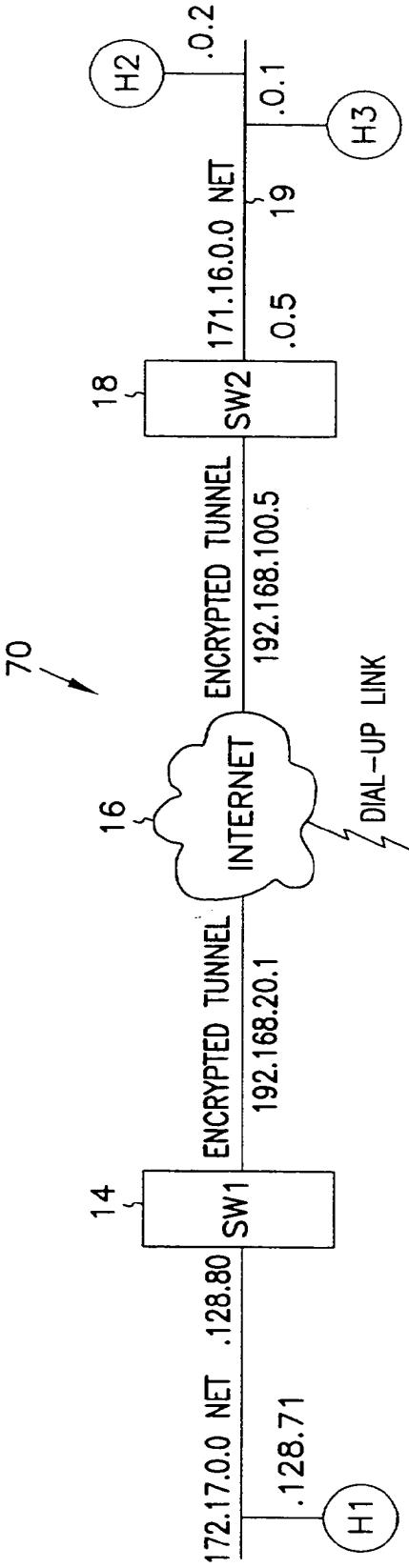

70
16
INTERNET
ENCRYPTED TUNNEL
192.168.100.5
ENCRYPTED TUNNEL
192.168.20.1
DIAL-UP LINK
L1
14
SW1
18
SW2
172.17.0.0 NET
.128.80
.128.71
H1
171.16.0.0 NET
19
.0.5
.0.2
.0.1
H2
H3

FIG. 3

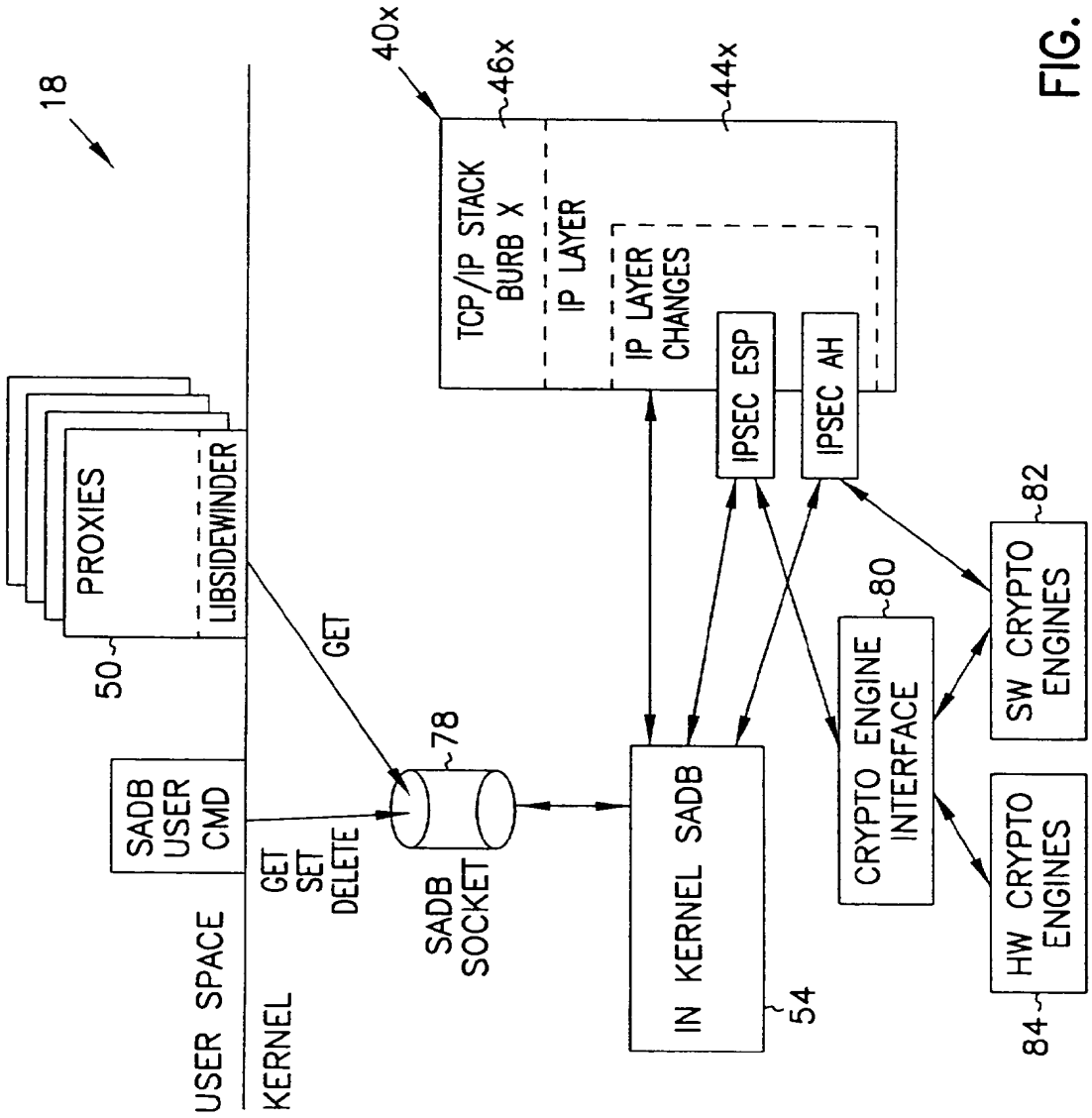

18
40x
46x
44x
TCP/IP STACK
BURB X
IP LAYER
IP LAYER
CHANGES
IPSEC ESP
IPSEC AH
PROXIES
LIBSIDEWINDER
50
GET
78
SADB
USER
CMD
GET
SET
DELETE
SADB
SOCKET
IN KERNEL SADB
54
CRYPTO ENGINE
INTERFACE
80
SW CRYPTO
ENGINES
82
HW CRYPTO
ENGINES
84
USER SPACE
KERNEL

FIG. 4

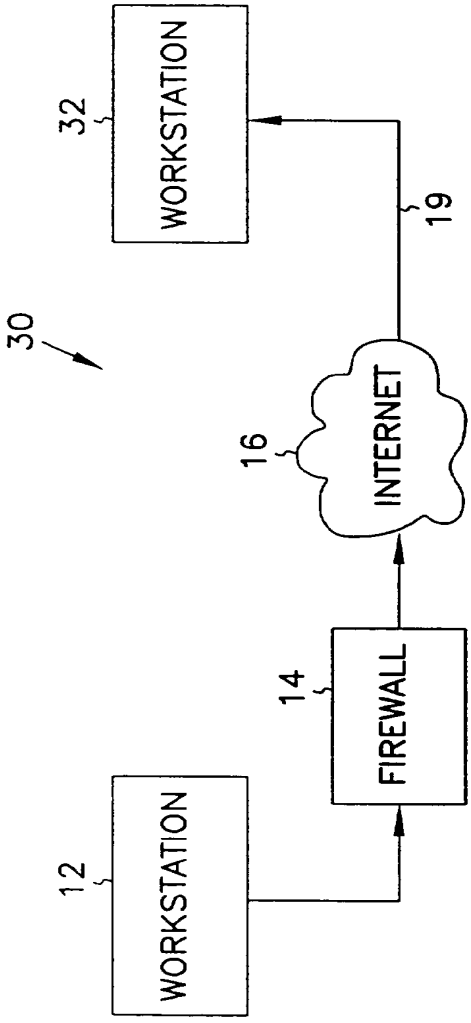

30
WORKSTATION
12
FIREWALL
14
INTERNET
16
19
WORKSTATION
32

FIG. 5

VIRTUAL PRIVATE NETWORK ON APPLICATION GATEWAY

Background of the Invention

Field of the Invention

The present invention pertains generally to network communications, and in particular to a system and method for securely transferring information between firewalls over an unprotected network.

Background Information

Firewalls have become an increasingly important part of network design. Firewalls provide protection of valuable resources on a private network while allowing communication and access with systems located on an unprotected network such as the Internet. In addition, they operate to block attacks on a private network arriving from the unprotected network by providing a single connection with limited services. A well designed firewall limits the security problems of an Internet connection to a single firewall computer system. This allows an organization to focus their network security efforts on the definition of the security policy enforced by the firewall. An example of a firewall is given in "SYSTEM AND METHOD FOR PROVIDING SECURE INTERNETWORK SERVICES" by Boebert et al. (PCT Published Application No. WO 96/13113, published on May 2, 1996), the description of which is hereby incorporated by reference. Another description of a firewall is provided by Dan Thomsen in "Type Enforcement: the new security model", *Proceedings: Multimedia: Full-Service Impact on Business, Education, and the Home*, SPIE Vol. 2617, p. 143, August 1996. Yet another such system is described in "SYSTEM AND METHOD FOR ACHIEVING NETWORK SEPARATION" by Gooderum et al. (PCT Published Application No. WO 97/29413, published on August 14, 1997), the description of which is hereby incorporated by reference. All the above systems are examples of application level gateways. Application level gateways use proxies or other such mechanisms operating at the application layer to process traffic through the firewall. As such, they can review not only the

message traffic but also message content. In addition, they provide authentication and identification services, access control and auditing.

Data to be transferred on unprotected networks like the Internet is susceptible to electronic eavesdropping and accidental (or deliberate) corruption. Although a firewall can protect data within a private network from attacks launched from the unprotected network, even that data is vulnerable to both eavesdropping and corruption when transferred from the private network to an external machine. To address this danger, the Internet Engineering Task Force (IETF) developed a standard for protecting data transferred between firewalls over an unprotected network. The Internet Protocol Security (IPSEC) standard calls for encrypting data before it leaves the first firewall, and then decrypting the data when it is received by the second firewall. The decrypted data is then delivered to its destination, usually a user workstation connected to the second firewall. For this reason IPSEC encryption is sometimes called *firewall-to-firewall encryption* (FFE) and the connection between a workstation connected to the first firewall and a client or server connected to the second firewall is termed a *virtual private network*, or VPN.

The two main components of IPSEC security are data encryption and sender authentication. Data encryption increases the cost and time required for the eavesdropping party to read the transmitted data. Sender authentication ensures that the destination system can verify whether or not the encrypted data was actually sent from the workstation that it was supposed to be sent from. The IPSEC standard defines an encapsulated payload (ESP) as the mechanism used to transfer encrypted data. The standard defines an authentication header (AH) as the mechanism for establishing the sending workstation's identity.

Through the proper use of encryption, the problems of eavesdropping and corruption can be avoided; in effect, a protected connection is established from the internal network connected to one firewall through to an internal network connected to the second firewall. In addition, IPSEC can be used to provide a protected connection to an external computing system such as a portable personal computer.

IPSEC encryption and decryption work within the IP layer of the network protocol stack. This means that all communication between two IP addresses will be protected because all interfirewall communication must go through the IP layer. Such an approach is preferable over encryption and decryption at higher levels in the network protocol stack since when encryption is performed at layers higher than the IP layer more work is required to ensure that all supported communication is properly protected. In addition, since IPSEC encryption is handled below the Transport layer, IPSEC can encrypt data sent by any application. IPSEC therefore becomes a transparent add-on to such protocols as TCP and UDP.

Since, however, IPSEC decryption occurs at the IP layer, it can be difficult to port IPSEC to an application level gateway while still maintaining control at the proxy over authentication, message content, access control and auditing. Although the IPSEC specification in RFC 1825 suggests the use of a mandatory access control mechanism in a multi-level secure (MLS) network to compare a security level associated with the message with the security level of the receiving process, such an approach provides only limited utility in an application level gateway environment. In fact, implementations on application level gateways to date have simply relied on the fact that the message was IPSEC-encrypted as assurance that the message is legitimate and have simply decoded and forwarded the message to its destination. This creates, however, a potential chink in the firewall by assuming that the encrypted communication has access to all services.

What is needed is a method of handling IPSEC messages within an application level gateway which overcomes the above deficiencies. The method should allow control over access by an IPSEC connection to individual services within the internal network.

Summary of the Invention

The present invention is a system and method for regulating the flow of messages through a firewall having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer, the method

comprising the steps of determining, at the IP layer, if a message is encrypted, if the message is not encrypted, passing the unencrypted message up the network protocol stack to an application level proxy, and if the message is encrypted, decrypting the message and passing the decrypted message up the network protocol stack to the application level proxy, wherein the step of decrypting the message includes the step of executing a procedure at the IP layer to decrypt the message.

According to another aspect of the present invention, a system and method is described for authenticating the sender of a message within a computer system having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer, the method comprising the steps of determining, at the IP layer, if the message is encrypted, if the message is encrypted, decrypting the message, wherein the step of decrypting the message includes the step of executing a procedure at the IP layer to decrypt the message, passing the decrypted message up the network protocol stack to an application level proxy, determining an authentication protocol appropriate for the message, and executing the authentication protocol to authenticate the sender of the message.

Brief Description of the Drawings

In the following detailed description of example embodiments of the invention, reference is made to the accompanying drawings which form a part hereof, and which is shown by way of illustration only, specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

In the drawings, where like numerals refer to like components throughout the several views:

Figure 1 is a functional block diagram of an application level gateway-implemented firewall-to-firewall encryption scheme according to the present invention;

Figure 2 is a block diagram showing access control checking of both encrypted and unencrypted messages in network protocol stack according to the present invention;

Figure 3 is a block diagram of a representative application level gateway-implemented firewall-to-firewall encryption scheme;

Figure 4 is a block diagram of one embodiment of a network-separated protocol stack implementing IPSEC according to the present invention; and

Figure 5 is a functional block diagram of a firewall-to-workstation encryption scheme according to the present invention.

Description of the Preferred Embodiments

In the following detailed description of the preferred embodiment, references made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific preferred embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that structural, logical, physical, architectural, and electrical changes may be made without departing from the spirit and scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims and their equivalents.

A system 10 which can be used for firewall-to-firewall encryption (FFE) is shown in Figure 1. In Figure 1, system 10 includes a workstation 12 communicating through a firewall 14 to an unprotected network 16 such as the Internet. System 10 also includes a workstation 20 communicating through a firewall 18 to unprotected network 16. In one embodiment, firewall 18 is an application level gateway.

As noted above, IPSEC encryption and decryption work within the IP layer of the network protocol stack. This means that all communications between two IP addresses will be protected because all interfirewall communication must pass through the IP layer. IPSEC takes the standard

Internet packet and converts it into a carrier packet. The carrier packet is designed to do two things: to conceal the contents of the original packet (encryption) and to provide a mechanism by which the receiving firewall can verify the source of the packet (authentication). In one embodiment of the present invention, each IPSEC carrier packet includes both an authentication header used to authenticate the sending machine and an encapsulated payload containing encrypted data. The authentication header and the encapsulated payload features of IPSEC can, however, be used independently. As required in RFC 1825, DES-CBC is provided for use in encrypting the encapsulated payload while the authentication header uses keyed MD5.

To use IPSEC, you must create a *security association* (SA) for each destination IP address. In one embodiment, each SA contains the following information:

- Security Parameters Index (SPI) - The index used to find a SA on receipt of an IPSEC datagram.
- Destination IP address - The address used to find the SA and trigger use of IPSEC processing on output.
- The peer SPI - The SPI value to put on a IPSEC datagram on output.
- The peer IP address - The destination IP address to be put into the packet header if IPSEC Tunnel mode is used.
- The Encryption Security Payload (ESP) algorithm to be used.
- The ESP key to used for decryption of input datagrams.
- The ESP key to used for encryption of output datagrams.
- The authentication (AH) algorithm to be used.
- The AH key to be used for validation of input packets.
- The AH key to be used for generation of the authentication data for output datagrams.

The combination of a given Security Parameter Index and Destination IP address uniquely identifies a particular "Security Association." In one

embodiment, the sending firewall uses the sending userid and Destination Address to select an appropriate Security Association (and hence SPI value). The receiving firewall uses the combination of SPI value and Source address to obtain the appropriate Security Association.

A security association is normally one-way. An authenticated communications session between two firewalls will normally have two Security Parameter Indexes in use (one in each direction). The combination of a particular Security Parameter Index and a particular Destination Address uniquely identifies the Security Association.

More information on the specifics of an IPSEC FFE implementation can be obtained from the standards developed by the IPSEC work group and documented in *Security Architecture for IP* (RFC 1825) and in RFC's 1826-1829.

When a datagram is received from unprotected network 16 or is to be transmitted to a destination across unprotected network 16, the firewall must be able to determine the algorithms, keys, etc. that must be used to process the datagram correctly. In one embodiment, this information is obtained via a security association lookup. In one such embodiment, the lookup routine is passed several arguments: the source IP address if the datagram is being received from network 16 or the destination IP address if the datagram is to be transmitted across network 16, the SPI, and a flag that is used to indicate whether the lookup is being done to receive or transmit a datagram.

When an IPSEC datagram is received by firewall 18 from unprotected network 16, the SPI and source IP address are determined by looking in the datagram. In one embodiment a Security Association Database (SADB) stored within firewall 18 is searched for the entry with a matching SPI. In one such embodiment, security associations can be set up based on network address as well as a more granular host address. This allows the network administrator to create a security association between two firewalls with only a couple of lines in a configuration file on each machine. For such embodiments, the entry in the Security Association Database that has both the matching SPI and the longest

address match is selected as the SA entry. In another such embodiment, each SA has a prefix length value associated with the address. An address match on a SA entry means that the addresses match for the number of bits specified by the prefix length value.

There are two exceptions to this search process. First, when an SA entry is set marked as being dynamic it implies that the user of this SA may not have a fixed IP address. In this case the match is fully determined by the SPI value. Thus it is necessary that the SPI values for such SA entries be unique in the SADB. The second exception is for SA entries marked as tunnel mode entries. In this case it is normally the case that the sending entity will hide its source address so that all that is visible on the public wire is the destination address. In this case, like in the case where the SA entries are for dynamic IP addresses, the search is done exclusively on the basis of the SPI.

When transmitting a datagram across unprotected network 16 the SADB is searched using only the destination address as an input. In this case the entry which has the longest address match is selected and returned to the calling routine.

In one embodiment, if firewall 18 receives datagrams which are identified as either an IP_PROTO_IPSEC_ESP or IP_PROTO_IPSEC_AH protocol datagram, there must be a corresponding SA in the SADB or else firewall 18 will drop the packet and an audit message will be generated. Such an occurrence might indicate a possible attack or it might simply be a symptom of an erroneous key entry in the Security Association Database.

In a system such as system 10, application level gateway firewall 18 acts as a buffer between unprotected network 16 and workstations such as workstation 20. Messages coming from unprotected network 16 are reviewed and a determination is made as to whether execution of an authentication and identification protocol is warranted. In contrast to previous systems, system 10 also performs this same determination on IPSEC-encrypted messages. If desired, the same authentication and identification can be made on messages to be transferred from workstation 20 to unprotected network 16. Figure 2

illustrates one way of authenticating both encrypted and unencrypted messages in a system such as system 10.

In the system of Figure 2 a network protocol stack 40 includes a physical layer 42, an Internet protocol (IP) layer 44, a Transport layer 46 and an application layer 48. Such a protocol stack exists, for instance on application level gateway firewall 18 of Figure 1. An application executing in application layer 48 can communicate to an application executing on another system by preparing a message and transmitting it through one of the existing transport services executing on transport layer 46. Transport layer 46 in turn uses a process executing in IP layer 44 to continue the transfer. Physical layer 42 provides the software needed to transfer data through the communication hardware (e.g., a network interface card or a modem). As noted above, IPSEC executes within IP layer 44. Encryption and authentication is transparent to the host as long as the network administrator has the Security Association Database correctly configured and a key management mechanism is in place on the firewall.

In application level gateway firewall 18, a proxy 50 operating within application layer 48 processes messages transferred between internal and external networks. All network-to-network traffic must pass through one of the proxies within application layer 48 before being the transfer across networks is allowed. A message arriving from external network 16 is examined at IP layer 44 and an SADB is queried to determine if the source address and SPI are associated with an SA. In the embodiment shown in Figure 2, an SADB Master copy 52 is maintained in persistent memory at application layer 48 while a copy 54 of SADB is maintained in volatile memory within the kernel. If the message is supposed to be encrypted, the message is decrypted based on the algorithm and key associated with the particular SA and the message is transferred up through transport layer 46 to proxy 50. Proxy 50 examines the source and destination addresses and the type of service desired and decides whether authentication of the sender is warranted. If so, proxy 50 initiates an authentication protocol. The protocol may be as simple as requesting a user

name and password or it may include a challenge/response authentication process. Proxy 50 also looks to see whether the message coming in was encrypted or not and may factor that into whether a particular type of authentication is needed. In Telnet, for instance, user name/password authentication may be sufficient for an FFE link while the security policy may dictate that a more stringent challenge/response protocol is needed for unencrypted links. In that case, proxy 50 will be a Telnet proxy and it will base its authentication protocol on whether the link was encrypted or not.

Since IPSEC executes within IP layer 44 there is no need for host firewalls to update their applications. Users that already have IPSEC available on their own host machine will, however, have to request that the firewall administrator set up SA's in the SADB for their traffic.

In the embodiment shown in Figure 2, a working copy 54 of the Security Association Database consisting of all currently active SA's is kept resident in memory for ready access by IP layer processing as datagrams are received and transmitted. In addition, a working master copy 52 of the SADB is maintained in a file in nonvolatile memory. During system startup and initialization processing the content of all of the required SA's in master SADB 52 is added to the working copy 54 stored in kernel memory.

In one embodiment, firewall 18 maintains different levels of security on internal and external network interfaces. It is desirable for a firewall to have different levels of security on both the internal and external interfaces. In one embodiment, firewall 18 supports three different levels, numbered 0 through 2. These levels provide a simple policy mechanism that controls permission for both in-bound and out-bound packets.

- Level 0 - do not allow any in-bound or out-bound traffic unless there is a security association between the source and destination.

- Level 1 - Allow both in-bound and out-bound non-IPSEC traffic but force the use of IPSEC if a SA exists for the address. (To support this firewall 18 must look for a SA for each in-bound datagram.)
- Level 2 - allow NULL security associations to exist. NULL associations are just like normal security associations, except no encryption or authentication transform is performed on in-bound or out-bound packets that correspond to this NULL association. With Level 2 enabled, the machine will still receive unprotected traffic, but it will not transmit unless Level 1 is enabled.

The default protection level established when the Security Association Database (SADB) is initialized at boot time is 1 for in-bound traffic and 2 for out-bound traffic.

An Access Control List, or ACL, is a list of rules that regulate the flow of Internet connections through a firewall. These rules control how a firewall's servers and proxies will react to connection attempts. When a server or proxy receives an incoming connection, it performs an ACL check on that connection.

An ACL check compares a set of parameters associated with the connection against a list of ACL rules. The rules determine whether the connection is allowed or denied. A rule can also have one or more side effects. A side effect causes the proxy to change its behavior in some fashion. For example, a common side effect is to redirect the destination IP address to an alternate machine. In addition to IP connection attempts, ACL checks can also made on the console logins and on logins made from serial ports. Finally, ACL checks can also be made on behalf of IP access devices, such as a Cisco box, through the use of the industry standard TACACS+ protocol.

In one embodiment, the ACL is managed by an acld daemon running in the kernel of firewalls 10 and 30. The acld daemon receives two types of requests, one to query the ACL and one to administer it. In one such embodiment, the ACL is stored in a relational database such as the Oracle database for fast access. By using such a database, query execution is asynchronous and many queries can be executing concurrently. In addition, these types of databases are designed to manipulate long lists of rules quickly

and efficiently. These qualities ensure that a given query cannot hang up the process that issued the query for any appreciable time (> 1-2 seconds).

In one such embodiment, the database can hold up to 100,000 users and up to 10,000 hosts but can be scaled up to the capacity of the underlying database engine. The results of an ACL check is cached, allowing repeated checks to be turned around very quickly.

Applications on firewalls 10 and 30 can query acld to determine if a given connection attempt should be allowed to succeed. In one embodiment, the types of applications (i.e. "agents") that can make ACL queries can be divided into four classes:

1) Proxies. These allow connections to pass through firewall 10 or 30 in order to provide access to a remote service. They include tnauthp (authenticated telnet proxy), pftp (FTP proxy), httpp (HTTP proxy), and tcpgsp (TCP generic service proxy).

2) Servers. These provide a service on the firewall itself. They include ftpd and httpd.

3) Login agents. Login agent is a program on the firewall that can create a Unix shell. It is not considered a server because it cannot receive IP connections. One example is /usr/bin/login when used to create a dialup session or a console session on firewall 10 or 30. Another example is the command *srole*.

4) Network Access Servers (NAS). NAS is a remote IP access device, typically a dialup box manufactured by such companies as Cisco or Bridge. The NAS usually provides dialup telnet service and may also provide SLIP or PPP service.

Proxies, servers, login agents, and NASes make queries to acld to determine if a given connection attempt should be allowed to succeed. All of the agents except NAS make their queries directly. NAS, because it is remote, must communicate via an auxiliary daemon that typically uses an industry standard protocol such as RADIUS or TACACS+. The auxiliary daemon (e.g., tacradd) in turn forwards the query to local acld.

As a side effect of the query, acld tells the agent if authentication is needed. If no authentication is needed, the connection proceeds immediately. Otherwise acld provides (as another side effect) a list of allowed authentication methods that the user can choose from. The agent can present a menu of choices or simply pick the first authentication method by default. Typical authentication methods include plain password, SNK DSS, SDI SecurID, LOCKout DES, and LOCKout FORTEZZA. In one embodiment, the list of allowed authentication methods varies depending on the host name, user name, time of day, or any combination thereof.

In the case of a Level 0 policy, it would be safe to assume that all incoming traffic is encrypted or authenticated. In the case of Levels 1 through 2, a determination must be made whether or not a security association exists for a given peer. Otherwise an application may believe that in-bound traffic has been authenticated when it really has not. (That is why it is necessary to look for an SA on input of each non-IPSEC datagram.)

In one embodiment, a flag which accompanies the message as it is sent from IP layer 44 to proxy 50 indicates whether the incoming message was or was not encrypted. In another embodiment, proxy 50 accesses Security Association Database 54 (the table in the kernel can be queried via an SADB routing socket (PF-SADB)) to determine whether or not a security association exists for a given peer.. The SADB socket is much like a routing socket found in the stock BSD 4.4 kernel (protocol family PF-ROUTE) except that PF-SADB sockets are used to maintain the Security Association Database (SADB) instead of the routing table. Because the private keys used for encryption, decryption, and keyed authentication are stored in this table, access must be strictly prohibited and allowed to only administrators and key management daemons. Care must be taken when allowing user-level daemons access to `/dev/mem` or `/dev/kmem` as well, since the keys are stored in kernel memory and could be exposed with some creative hacking.

In one embodiment, a command-line tool called `sadb` is used to support the generation and maintenance of in-kernel version 54 of SADB. The primary

interface between this tool and the SADB is the PF-SADB socket. The kernel provides socket processing to receive client requests to add, update, or change entries in in-kernel SADB 54. As noted above, the default protection level established when the Security Association Database (SADB) is initialized at boot time is 1 for in-bound traffic and 2 for out-bound traffic. This may be changed by the use of the `sadb` command.

The existing `sadb` command was derived from the NIST implementation of IPSEC. As noted above, this tool is much like `route` in that it uses a special socket to pass data structures in and out of the kernel. There are three commands recognized by the `sadb` command: *get*, *set*, *delete*. The following simple shell script supports adding and removing a single SA entry to SADB 54. It shows one embodiment of a parameter order for adding a SA to the SADB.

```
# ! /bin/sh
if [ $# -ne 1 ]
then
     echo "usage: $0 <on>|<off>" >&2
     exit 1
fi
ONOFF=$1

addsa ()
{
IPADDRESS=$2
PEERADDRESS=0.0.0.0
PREFIXLEN=0                 # Num of bits, 0 => full 32
bit match
LOCALADDRESS=0.0.0.0
REALADDRESS=0.0.0.0
PORT=0
PROTOCOL=0
UID=0
DESALG=1                    # 1 = DES-CBC
IVLEN=4                     # bytes
DESKEY=0b0b0b0b0b0b0b0b
DESKEYLEN=8                 # bytes
AHALG=1                     # 1 = MD5
AHKEY=30313233343536373031323334353637
AHKEYLEN=16                 # bytes
LOCAL_SPI=$1
```

```
PEER_SPI=$1
TUNNEL_MODE=0
AHRESULTLEN=4
COMBINED_MODE=1          # On output, 1 = ESP, then
AH; 0 = AH, then ESP
DYNAMIC_FLAG=0

if [ "$ONOFF" = "on"
then
     ./sadb add dst $IPADDRESS $PREFIXLEN $LOCAL_SPI
$UID $PEERADDRESS $PEER_SPI $TUNNEL_MODE $LOCALADDRESS
$REALADDRESS $PROTOCOL $PORT $DESALG $IVLEN $DESKEYLEN
$DESKEY $DESKEYLEN $DESKEY $AHALG $AHKEYLEN $AHKEY
$AHKEYLEN $AHKEY $AHRESULTLEN $COMBINED_MODE
$DYNAMIC_FLAG
else
     ./sadb delete dst $IPADDRESS $LOCAL-SPI
fi
}

#    Get down to work:
addsa 500 172.17.128.115          # number6.sctc.com
```

The current status of in-kernel SADB 54 can be obtained with the `sadb` command. The get option allows dumping the entire SADB or a single entry. In one embodiment, the complete dump approach uses `/dev/kmem` to find the information. The information may be presented as follows:

```
# sadb get dst

Local-SPI Address-Family Destination-Addr
Preflx_length UID
     Peer-Address Peer-SPI Transport-Type
     Local-Address Real-Address
     Protocol Port
     ESP_Alg_ID ESP_IVEC_Length
          ESP_Enc_Key_length ESP_Enc_ESP_Key
          ESP_Dec_Key_length ESP_Dec_ESP_Key
     AH_Alg_ID AH_Data_Length
          AH_Gen_Key_Length AH_Gen_Key
          AH_Check_Key_Length AH_Check_Key
     Combined_Mode  Dynamic_Flag
```

```
-------------------------------------------------------
-
500 INET: number6.sctc.com 0 0
      0.0.0.0   500 Transport(0) 0
      0.0.0.0 0.0.0.0
      None None
      DES/CBC-RFC1829(1) 4
            8 0b0b0b0b0b0b0b0b
            8 0b0b0b0b0b0b0b0b
      MD5-RFC1828(1) 4
            16 30313233343536373031323334353637
            16 30313233343536373031323334353637
      ESP+AH(1) 0
501 INET: spokes.sctc.com 0 0
      0.0.0.0   501 Transport(0) 0
      0.0.0.0.0.0.0.0
      None None
      DES/CBC-RFC1829(1) 4
            8 0b0b0b0b0b0b0b0b
            8 0b0b0b0b0b0b0b0b
      MD5-RFC1828(1) 4
            16 30313233343536373031323334353637
            16 30313233343536373031323334353637
      ESP+AH(1) 0

End of list.
```

When a new entry is added to in-kernel SADB 54, the add process first checks to see that no existing entry will match the values provided in the new entry. If no match is found then the entry is added to the end of the existing SADB list.

To illustrate the use and administration of an FFE, we'll go through an example using FFE 70 in Figure 3. Firewalls 14 and 18 are both application level gateway firewalls implemented according to the present invention. Workstations H2 and H3 both want to communicate with Hl. For the administrator of firewalls 14 and 18, this is easy to accomplish. The administrator sets up a line something like this (we'll only show the IP address part and SPI parts of the SA, since they're the trickiest values to configure. Also, assume that we are using tunnel mode):

```
#  Hypothetical SW1 Config File
```

```
#
#  Fields are laid out in the following manner:
#  srcaddrornet= localSPI= peeraddr= peerSPI=
realsrcaddr= localaddr= key=

# The following entry sets up a tunnel between hosts
behind SW1
# and hosts behind SW2.
src=172.16.0.0 localSPI=666 peer=192.168.100.5
peerSPI=777 \
     realsrcaddr=192.168.100.5 localaddrs=0.0.0.0
     key=0xdeadbeeffadebabe

#  Hypothetical SW2 Config File
#
#  Fields are laid out in the following manner:
#  srcaddrornet= localSPI= peeraddr= peerSPI=
     realsrcaddr= localaddr= key=

#  The following entry sets up a tunnel between hosts
behind SW1 and
#  hosts behind SW2.
src=172.17.0.0 localSPI=777 peer=192.168.20.1
peerSPI=666 \
     realsrcaddr=192.168.20.1 localaddr=0.0.0.0 \
     key=Oxdeadbeeffadebabe
```

With this setup, all traffic is encrypted using one key, no matter who is talking to whom. For example, traffic from H2 to Hl as well as traffic from H3 to Hl will be encrypted with one key. Although this setup is small and simple, it may not be enough.

What happens if H2 cannot trust H3? In this case, the administrator can set up security associations at the host level. In this case, we have to rely on the SPI field of the SA, since the receiving firewall cannot tell from the datagram header which host behind the sending firewall sent the packet. Since the SPI is stored in IPSEC datagrams, we can do a lookup to obtain its value. Below are the sample configuration files for both firewalls again, but this time, each host combination communicates with a different key. Moreover, H2 excludes H3 from communications with Hl, and H3 excludes H2 in the same way.

```
#  Hypothetical SW1 Config File
#
#  Fields are laid out in the following manner:
#  srcaddrornet= localSPI= peeraddr= peerSPI=
realsrcaddr= localaddr= key=

# The following entry sets up a secure link between H2
and H1
src=172.16.0.2 localSPI=666 peer=192.168.100.5
peerSPI=777 \
     realsrcaddr=192.168.100.5
localaddrs=178.17.128.71 \
     key=0x0a0a0a0a0a0a0a0a

# The following entry sets up a secure link between H3
and H1
src=172.16.0.1 localSPI=555 peer=192.168.100.5
peerSPI=888 \
     realsrcaddr=192.168.100.5
localaddrs=178.17.128.71 \
     key=0x0b0b0b0b0b0b0b0b

#  Hypothetical SW2 Config File
#
#  Fields are laid out in the following manner:
#  srcaddrornet= localSPI= peeraddr= peerSPI=
realsrcaddr= localaddr= key=

# The following entry sets up a secure link between H2
and H1
src=172.17.128.71 localSPI=777 peer=192.168.20.1
peerSPI=666 \
     realsrcaddr=192.168.20.1 localaddrs=172.16.0.2 \
     key=0x0a0a0a0a0a0a0a0a

# The following entry sets up a secure link between H3
and H1
src=172.17.128.71 localSPI=888 peer=192.168.20.1
peerSPI=555 \
     realsrcaddr=192.168.20.1 localaddrs=172.16.0.1 \
     key=0x0b0b0b0b0b0b0b0b
```

Figure 4 is a block diagram showing in more detail one embodiment of an IPSEC-enabled application level gateway firewall 18. Application level gateway firewall 18 provides access control checking of both encrypted and

unencrypted messages in a more secure environment due to its network-separated architecture. Network separation divides a system into a set of independent regions or burbs, with a domain and a protocol stack assigned to each burb. Each protocol stack 40x has its own independent set of data structures, including routing information and protocol information. A given socket will be bound to a single protocol stack at creation time and no data can pass between protocol stacks 40 without going through proxy space. A proxy 50 therefore acts as the go-between for transfers between domains. Because of this, a malicious attacker who gains control of one of the regions is prevented from being able to compromise processes executing in other regions. Network separation and its application to an application level gateway is described in "SYSTEM AND METHOD FOR ACHIEVING NETWORK SEPARATION", U.S. Application No. 08/599,232, filed February 9, 1996 by Gooderum et al.

In the system shown in Figure 4, the in-bound and out-bound datagram processing of a security association continues to follow the conventions defined by the network separation model. Thus all datagrams received on or sent to a given burb remain in that burb once decrypted. In one such embodiment SADB socket 78 has been defined to have the type 'sadb'. Each proxy 50 that requires access to SADB socket 78 to execute its query as to whether the received message was encrypted must have create permission to the sadb type.

The following is list of specific requirements that a system such as is shown in Figure 4 must provide. Many of the requirements were discussed in the information provided earlier in this document.

1. Firewall applications may query the IPSEC subsystem to determine if traffic with a given address is guaranteed to be encrypted.
2. Receipt of an unencrypted datagram from an address that has a SA results in the datagram being dropped and an audit message being generated.
3. On receipt of encrypted protocol datagrams the SADB searches will be done using the SPI as the primary key. The source address will a secondary key. The SA returned by the search will be the SA which matches the SPI exactly and has the longest match with the address.

4. A search of the SADB for a SPI that finds an entry that is marked as SA for a dynamic IP will not consider the address in the search process.

5. A search of the SADB for a SPI that finds an entry that is marked as a SA for a tunnel mode connection will to consider the address if it is (0.0.0.0) i.e INADDR.

6. On receipt of a non-IPSEC datagram the SADB will be searched for an entry that matches the src address. If a SA is found the datagram will be dropped and an audit message sent.

7. SADB searches on output will be done using the DST address as key. If more than one SA entry in the SADB has that address the first one with the maximum address match will be returned.

8. The SADB must be structured so that searches are fast regardless if the search is done by SPI or by address.

9. The SADB must provide support for connections to a site with a fixed SPI but changing IP address. SA entries for such connections will be referred to as Dynamic Address Sites, or just Dynamic entries.

10. When a dynamic entry is found by a SPI search, the current datagram's SRC address, which is required to ensure that the return datagrams are properly encrypted, will be recorded in the SA only after the AH checking has passed successfully. (This is because if the address is recorded before AH passes then an attacker can cause return packets of an outgoing connection to be transmitted in the clear.)

11. A failure of an AH check on a dynamic entry results in an audit message.

12. In an embodiment where the firewall requires that all connections use both AH and ESP, on receipt the order should be AH first ESP second.

13. The processing structure on both input and output should try to minimize the number of SADB required lookups.

Returning to Figure 4, in one embodiment firewall 18 includes a crypto engine interface 80 used to encrypt an IPSEC payload. Crypto engine interface 80 may be connected to a software encryption engine 82 or to a hardware

encryption engine 84. Engines 82 and 84 perform the actual encryption function using, for example, DES-CBC. In addition, software encryption engine 82 may include the keyed MD5 algorithm used for AH.

In one embodiment, crypto engine interface 80 is a utility which provides a consistent interface between the software and hardware encryption engines. As shown in Figure 4, in one such embodiment interface 80 only supports the use of the use of hardware cryptographic engine 84 for IPSEC ESP processing. The significant design issue that interface 80 must deal with is that use of a hardware encryption engine requires that the processing be down in disjoint steps operating in different interrupt contexts as engine 84 completes the various processing steps.

The required information is stored in a request structure that is bound to the IP datagram being processed. The request is of type `crypto_request_t`. This structure is quite large and definitely does not contain a minimum state set.

In addition to the definition of the request data structure, this software implementing interface 80 provides two functions which isolate the decision of which cryptographic engine to use. The `crypt_des_encrypt` function is for use by the IP output processing to encrypt a datagram. The `crypt_des_decrypt` function is for use by the IP input processing to decrypt a datagram. If hardware encryption engine 84 is present and other hardware usage criteria are met the request is enqueued on a hardware processing queue and a return code indicating that the cryptographic processing is in progress is returned. If software engine 82 is used, the return code indicates that the cryptographic processing is complete. In the former case, the continuation of the IP processing is delayed until after hardware encryption is done. Otherwise it is completed as immediately in the same processing stream.

There are two software cryptographic engines 82 provided in the IPSEC software. One provides the MD5 algorithm used by the IPSEC AH processing, and the other provides the DES algorithm used by the IPSEC ESP processing. This software can be obtained from the US Government IPSEC implementation.

In one embodiment hardware cryptographic engine 84 is provided by a Cylink SafeNode processing board. The interface to this hardware card is provided by the Cylink device driver. A significant aspect of the Cylink card that plays a major part in the design of the IPSEC Cylink driver is that the card functions much like a low level subroutine interface and requires software support to initiate each processing step. Thus to encrypt or decrypt an individual datagram there are a minimum of two steps, one to set the DES initialization vector and one to do the encryption. Since the IP processing can not suspend itself and wait while the hardware completes and then be rescheduled by the hardware interrupt handler, in one embodiment a finite state machine is used to tie sequences of hardware processing elements together. In one such embodiment the interrupt handler looks at the current state, executes a defined after state function, transitions to the state and then executes that state's start function.

One function, `cyl_enqueue_request`, is used to initiate either an encrypt or a decrypt action. This function is designed to be called by cryptographic engine interface 80. All of the information required to initiate the processing as well as the function to be performed after the encryption operation is completed is provided in the request structure. This function will enqueue the request on the hardware request queue and start the hardware processing if necessary.

A system 30 which can be used for firewall-to-workstation encryption is shown in Figure 5. In Figure 5, system 30 includes a workstation 12 communicating through a firewall 14 to an unprotected network 16 such as the Internet. System 30 also includes a workstation 32 communicating directly with firewall 14 through unprotected network 16. Firewall 14 is an application level gateway incorporating IPSEC handling as described above. (It should be noted that IPSEC security cannot be used to authenticate the personal identity of the sender for a firewall to firewall transfer. When IPSEC is used, however, on a single user machine such as a portable personal computer, IPSEC usage should

be protected with a personal identification number (PIN). In these cases IPSEC can be used to help with user identification to the firewall.)

According to the IPSEC RFC's, you can use either tunnel or transport mode with this embodiment based on your security needs. In certain situations, the communications must be sent in tunnel mode to hide unregistered addresses.

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiment shown. This application is intended to cover any adaptations or variations of the present invention. Therefore, it is intended that this invention be limited only by the claims and the equivalents thereof.

What is claimed is:

1. A method of regulating the flow of messages through a firewall having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer, the method comprising the steps of:

determining, at the IP layer, if a message is encrypted;

if the message is not encrypted, passing the unencrypted message up the network protocol stack to an application level proxy; and

if the message is encrypted, decrypting the message and passing the decrypted message up the network protocol stack to the application level proxy, wherein the step of decrypting the message includes the step of executing a procedure at the IP layer to decrypt the message.

2. A method of authenticating the sender of a message within a computer system having a network protocol stack, wherein the network protocol stack includes an Internet Protocol (IP) layer, the method comprising the steps of:

determining, at the IP layer, if the message is encrypted;

if the message is encrypted, decrypting the message, wherein the step of decrypting the message includes the step of executing a process at the IP layer to decrypt the message;

passing the decrypted message up the network protocol stack to an application level proxy;

determining an authentication protocol appropriate for the message; and

executing the authentication protocol to authenticate the sender of the message.

3. The method according to claim 2 wherein the step of determining an authentication protocol appropriate for the message includes the steps of:

determining a source IP address associated with the message; and

determining the authentication protocol associated with the source IP address.

4. The method according to claim 2 wherein the message includes security parameters index and wherein the step of determining an authentication protocol appropriate for the message includes the steps of:

determining the authentication protocol associated with a dynamic IP address, wherein the step of determining the authentication protocol includes the step of looking up a security association based on the security parameters index;

determining a current address associated with the dynamic source IP address; and

binding the current address to the security parameters index.

5. A firewall, comprising:

a first communications interface;

a second communications interface;

a network protocol stack connected to the first and the second communications interfaces, wherein the network protocol stack includes an Internet Protocol (IP) layer and a transport layer;

a decryption procedure, operating at the IP layer, wherein the decryption procedure decrypts encrypted messages received at one of said first and second communications interfaces and outputs decrypted messages; and

a proxy, connected to the transport layer of said network protocol stack, wherein the proxy receives decrypted messages from the decryption procedure and executes an authentication protocol based on the content of the decrypted message.

6. A firewall, comprising:

a first communications interface;

a second communications interface;

a first network protocol stack connected to the first communications interface, wherein the first network protocol stack includes an Internet Protocol (IP) layer and a transport layer;

a second network protocol stack connected to the second communications interface, wherein the second network protocol stack includes an Internet Protocol (IP) layer and a transport layer;

a decryption procedure, operating at the IP layer of the first network protocol stack, the decryption procedure receiving encrypted messages received by said first communications interface and outputting decrypted messages; and

a proxy, connected to the transport layers of said first and second network protocol stacks, the proxy receiving decrypted messages from the decryption procedure and executing an authentication protocol based on the content of the decrypted message.

7. The firewall according to claim 6 wherein the firewall further includes:

a third communications interface; and

a third network protocol stack connected to the third communications interface and to the proxy, wherein the third network protocol stack includes an Internet Protocol (IP) layer and a transport layer and wherein the second and third network protocol stacks are restricted to first and second burbs, respectively.

8. A method of establishing a virtual private network between a first and a second network, wherein each network includes an application level gateway firewall which uses a proxy operating at the application layer to process traffic through the firewall, wherein each firewall includes a network protocol stack and wherein each network protocol stack includes an Internet Protocol (IP) layer, the method comprising the steps of:

transferring a connection request from the first network to the second network;

determining, at the IP layer of the network protocol stack of the second network's firewall, if the connection request is encrypted;

if the connection request is encrypted, decrypting the request, wherein the step of decrypting the request includes the step of executing a procedure at the IP layer of the second network's firewall to decrypt the message;

passing the connection request up the network protocol stack to an application level proxy;

determining an authentication protocol appropriate for the connection request;

executing the authentication protocol to authenticate the connection request; and

if the connection request is authentic, establishing an active connection between the first and second networks.

9. The method according to claim 8 wherein the step of executing the authentication protocol includes the step of executing program code within the firewall of the second network to mimic a challenge/response protocol executing on a server internal to the second network.

10. The method according to claim 8 wherein the step of executing the authentication protocol includes the step of executing program code to execute the authentication protocol in line to the session.

11. The method according to claim 8 wherein the step of determining an authentication protocol includes the step of determining if the connection request arrived encrypted and selecting the authentication protocol based on whether the connection request was encrypted or not encrypted.

The Patent Office

28

Application No: GB 9719816.2 **Examiner:** B.J.SPEAR
Claims searched: 1-11 **Date of search:** 21 January 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): H4P (PPEB,PDCSA,PDCSC)

Int Cl (Ed.6): H04L 9/00, 9/32, 29/06, 29/08

Other: Online:WPI, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
XP	WO97/26734A1	(Raptor Systems) Whole document, eg Figs 1,3 and pages 6-12	1,2.5,6,8 at least
XP	WO97/26731A1	(Raptor Systems) Whole document, eg Figs 1,3 and pages 7-12	1,2.5,6,8 at least
XP	WO97/26735A1	(Raptor Systems) Whole document, eg Figs 1,3 and pages 4-10	1,2.5,6,8 at least
XP	WO97/23972A1	(V-ONE Corp) Whole document, eg Figs 1,2 and claim 1.	1,2.5,6,8 at least
XP	WO97/13340A1	(Digital Secured Networks) Whole document, eg pages 7-13	1,2.5,6,8 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Petitioner Apple Inc. - Exhibit 1026, p. 911

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04Q 11/04, H04L 12/22

A1

(11) International Publication Number: **WO 98/27783**

(43) International Publication Date: 25 June 1998 (25.06.98)

(21) International Application Number: PCT/IB97/01563

(22) International Filing Date: 12 December 1997 (12.12.97)

(30) Priority Data:
08/769,649 19 December 1996 (19.12.96) US

(71) Applicant *(for all designated States except US)*: NORTHERN TELECOM LIMITED [CA/CA]; World Trade Center of Montreal, 8th floor, 380 St. Antoine Street West, Montreal, Quebec H2Y 3Y4 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: TELLO, Antonio, G. [US/US]; 114 Fountain Hills Drive, Garland, TX 75044 (US). HUI, Margaret [US/US]; 9920 Forest Lane #208, Dallas, TX 75243 (US). HOLMES, Kim [US/US]; 5409 Scenic Drive, Rowlett, TX 75088 (US).

(74) Agents: MCCOMBS, David et al.; Haynes and Boone, L.L.P., Suite 3100, 901 Main Street, Dallas, TX 75202–3789 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: VIRTUAL PRIVATE NETWORK SERVICE PROVIDER FOR ASYNCHRONOUS TRANSFER MODE NETWORK

(57) Abstract

A virtual private network service provider is used to transfer data over a data network to a final destination, with third–party billing. The method comprises the steps of: prompting the user at a data terminal to select a destination, password, and call type; sending a set–up message to the data network; selecting a virtual private network provider through the data network; the virtual private network provider giving an encryption key to the user, and then prompting the user for a password and a user identification; encrypting the password, and sending the user identification and the encrypted password to the virtual private network provider; the virtual private network provider decrypting the encrypted password, and verifying the password; the virtual private network provider providing an authorization code; and the data terminal transferring the data through the data network to the final destination, using the authorization code.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

VIRTUAL PRIVATE NETWORK SERVICE PROVIDER FOR ASYNCHRONOUS TRANSFER MODE NETWORK

Technical Field

The invention relates generally to asynchronous transfer mode ("ATM") networks and virtual private networks ("VPN"), such as those offered by MCI and Sprint, and, more particularly, to a method of using a VPN to transfer data over a data network, with third-party billing.

Background of the Invention

Telephone service providers offer third-party billing. For example, local and long distance telephone companies offer calling cards for third party billing.

VPNs exist to provide the sense of a private network among a company's locations. The lines/trunks of a VPN are actually shared among several companies, to reduce costs, yet to each company the VPN appears to be that company's own private network. However, a user at a remote data terminal, such as a portable computer in a hotel room, can not immediately charge his company for the access time to a data net, such as the Internet. Instead, his access time is charged to his hotel room, and so he must pay the inflated rates that hotels charge for phone service.

What is needed is a VPN service provider that offers remote access for users belonging to a VPN, user authorizations to prevent delinquent access into the VPN, and convenient third-party billing.

Summary of the Invention

The present invention, accordingly, provides a system and method for using a VPN service provider to transfer data over a data network to a final destination, with third-party billing. The method comprises the steps of: prompting the user at a data terminal to select a destination, password, and call type; selecting a VPN through the data network; giving an encryption key to the user, and then prompting the user for a password and a user identification; verifying the password, and providing an authorization code to

CONFIRMATION COPY

Petitioner Apple Inc. - Exhibit 1026, p. 914

the user; and allowing the user to transfer the data through the data network to the final destination, using the authorization code.

In another feature of the invention, the method further comprises negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

In another feature of the invention, the method further comprises encrypting the user's password, and sending the user identification and the encrypted password to the VPN service provider.

In another feature of the invention, the method further comprises a step of sending a set-up message to the data network.

In another feature of the invention, the method further comprises a step of the VPN service provider decrypting the encrypted password.

A technical advantage achieved with the invention is that it shifts or defers costs from an end user to a bulk purchaser of data network services. Another technical advantage achieved with the invention is that it permits end users mobility while attaining a virtual appearance on a corporate intranet.

Brief Description of the Drawings

Fig. 1 is a system block diagram of a VPN service provider of the present invention.

Fig. 2 is a flow chart depicting the method of the present invention, as implemented by application software on a user terminal.

Fig. 3 is the initial screen display of the user interface of the application software.

Figs. 4A and 4B are call flow diagrams, illustrating the preferred sequence of steps of the method of the present invention.

Figs. 5A, 5B, 5C, 5D, 5E, and 5F comprise a flow chart depicting the method of the present invention, as implemented by switching control point software.

Petitioner Apple Inc. - Exhibit 1026, p. 915

Description of the Preferred Embodiment

In Fig. 1, the VPN service provider system of the present invention is designated generally by a reference numeral 10. The VPN service provider system 10 includes a VPN 12. The VPN 12 may be a corporate, government, association, or other organization's telephone/data line `network. The VPN service provider system 10 also includes access lines 13 from the VPN 12 to a data network 14, such as the Internet, or an ATM network. The VPN service provider system 10 also includes access lines 16 from the data network 14 to a long distance phone company 18, such as AT&T, MCI, or Sprint. The VPN service provider system 10 also includes access lines 20 from the data network 14 to a called party 22, such as, for example, American Express reservations service. The VPN service provider system 10 also includes access lines 24 from the data network 14 to a remote user terminal 26, such as a portable computer in a hotel room. The user terminal 26 includes user application software 28, which provides the interface for the user to enter the number to be called, the user identification number, and the user's authorization code. The VPN service provider system 10 also includes VPN service provider software 30, located in a switching control point (SCP) device 32, which, in the preferred embodiment may be physically located anywhere. The SCP 32 connects to the data network 14 via access lines 36. One possible physical location for the SCP 32 is on the premises of a local phone company central switch building 34. However, even when located within the building 34, the SCP 32 connects to the local phone company switches via the data network 14. The local phone company switches connect to the data network 14 via access lines 38.

In an alternate embodiment, the VPN service provider software 30 and the SCP device 32 may be located on the premises of an independent provider of local phone service, or on the premises of an independent VPN service provider.

Petitioner Apple Inc. - Exhibit 1026, p. 916

Referring now to Fig. 2, the application software 28 begins the data transfer process in step 50. In step 52, the user is presented with a screen display.

Referring now to Fig. 3, a screen display 100 displays the following information requests: whether the call is a direct call 102 or a VPN call 104, the number the user desires to call 106, the VPN user ID 108, and the user password 110. The user is also presented with the option to make the call 112, or to quit 114.

Referring back to Fig. 2, in step 54 the user terminal sends to the SCP 32 the information captured through the graphical user interface ("GUI") in step 52 within a user network interface ("UNI") setup message. In step 56 the user terminal 26 waits for a connect message from the SCP 32. In step 58 the user terminal 26 determines if a connection was made. If no connection was made, then in step 60 the user application software 28 displays an error message to the user, and returns to step 50 to begin again the data transfer process.

If a connection was made, then in step 62 the user terminal 26 sends the VPN user ID to the SCP 32. In step 64 the user terminal 26 waits for an encryption key from the SCP 32. In step 66, having received the encryption key from the SCP 32, the user application software 28 encrypts the user's password, and sends it to the SCP 32. In step 68 the user terminal 26 waits for authentication of the user. In step 70 the user application software 28 determines if the SCP 32 authorizes the user to make the call.

If the user is not authorized, then in step 72 the user terminal 26 displays an error message, terminates the connection, blanks the screen display 100, and returns to step 50 to begin again the data transfer process. If the user is authorized, then in step 74 the VPN service provider software 30 sets up the billing, and authorizes it. In step 76 the user terminal 26 sends a "release", meaning to terminate or disconnect the connection, to the SCP 32. In step 78 the user terminal 26 sends a setup message to the number listed by

Petitioner Apple Inc. - Exhibit 1026, p. 917

the user as the "number to call", that is, to the final destination. In step 80 the user terminal 26 waits for a connection. In step 82 the user terminal 26 determines if a connection was made.

If a connection to the final destination was not made, then the user application software 28 returns to step 72, in which step the user terminal 26 displays an error message, terminates the connection, blanks the screen display 100, and returns to step 50 to begin again the data transfer process. If a connection to the final destination was made, then in step 84 the user terminal 26 exchanges user data, services, and/or value added or user specific applications with the computer at the address, that is, the telephone number, of the final destination. In step 86 the user selects the option presented to him to release, or terminate, the call. In step 88 the user terminal 26 sends a release message to the final destination. In step 90 the data network 14 sends billing information to the SCP 32. In step 92 the application software 28 ends the data transfer process.

Fig. 4A and Fig. 4B are call flow diagrams, showing the sequence of messages in the method of the preferred embodiment. These diagrams present the same method as the flow chart of Fig. 2. The horizontal arrows represent the messages sent and received. The vertical lines represent the various devices involved in sending and receiving the messages. For example, the top left arrow in Fig. 4A represents a message sent from the user terminal 26, labeled "Macintosh" in Fig.4A, to an interface with a public network. The user terminal 26 can be any brand of a work station computer, a desktop computer, a laptop computer, or even a notebook computer. The interface could be any interface, but in the example of Fig. 4A and Fig. 4B, the interface is imagined to be at a hotel, where a business traveler is using the method of the present invention. Thus, the interface is labeled "Hotel ATM Interface", which is not shown in Fig. 1. The vertical line labeled "Public ATM Network" is the same as the data network 14 in Fig. 1. The vertical line labeled "Moe's VPN Service" represents the VPN service provider software 30

Petitioner Apple Inc. - Exhibit 1026, p. 918

within the SCP 32. The vertical line labeled "Travel ATM Interface" is not shown in Fig. 1, but is located between the called party 22 and the data network 14. The vertical line labeled "Travel Service" is one example of the called party 22 shown in Fig. 1. In the example of Fig. 4A and Fig. 4B, the business traveler is imagined to be using the method of the present invention to contact a travel service to make reservations for his next airline flight. In Figs. 4A and 4B the designation "Ack" represents "acknowledge", and the designation "Cmp" represents "complete".

Referring now to Fig. 5, the VPN service provider software 30 begins the data transfer process in step 300 by waiting for an event. The event it waits for is a setup message on a signaling port of the SCP 32, to be received from the user terminal 26. In step 302, having monitored the signaling ports, and the SCP 32 having received a setup message, the VPN service provider software 30 assigns a call condense block ("CCB") to the setup message, based on a call reference number. The CCB is a software data structure for tracking resources associated with the call. The call reference number is a number, internal to the SCP, for tracking calls. In step 304 the VPN service provider software 30 compiles the connect message. In step 306 the VPN service provider software 30 sends a connect message to the calling address, that is, the hotel room from which the user is calling. In step 308 the VPN service provider software 30 condenses, that is, it remains in a wait state for that call.

Referring now to Fig. 5B, in step 310 the VPN service provider software 30 waits for an event by monitoring the signaling ports of the SCP 32. After the SCP 32 receives a connect acknowledge message from the user terminal 26, then in step 312 the VPN service provider software 30 accesses the CCB, based on the call reference number. In step 314 the VPN service provider software 30 condenses.

Referring now to Fig. 5C, in step 316 the VPN service provider software 30 waits for dialog on a data port of the SCP 32. After the SCP 32 receives a

Petitioner Apple Inc. - Exhibit 1026, p. 919

VPN ID on a data port, the VPN service provider software 30 verifies the VPN ID in step 318. In step 320 the VPN service provider software 30 determines if the VPN ID is valid. If the VPN ID is not valid, then in step 322 the SCP 32 sends a reject message over an assigned switch virtual circuit ("SVC"). The SVC is a channel over the data network 14. In step 324 the VPN service provider software 30 waits for dialog. In step 326, because the VPN ID is valid, the VPN service provider software 30 assigns an encryption key to the user terminal 26, in step 328 sends the encryption key over the assigned SVC to the user terminal 26, and in step 330 waits for dialog.

Referring now to Fig. 5D, in step 332 the VPN service provider software 30 waits for dialog. When the SCP 32 receives the encrypted password from the user terminal 26 at a data port, then in step 334 the VPN service provider software 30 verifies the password, and determines in step 336 if the password is valid. If the password is not valid, then in step 338 the SCP 32 sends a reject message over the assigned SVC to the user terminal, and in step 340 waits for dialog. If the password is valid, then in step 342 the VPN service provider software 30 assigns an authorization token to the user terminal 26, in step 344 sends the token over an assigned SVC to the user terminal 26, and in step 346 waits for dialog.

Referring now to Fig. 5E, in step 348 the VPN service provider software 30 waits for an event. When the VPN service provider software 30 senses that the SCP 32 has received on a signaling port a release message from the user terminal 26, then in step 350 the VPN service provider software 30 accesses the CCB, based on the call reference number of the user terminal 26, in step 352 compiles a release complete message, in step 354 sends a release complete message to the user terminal 26, and in step 356 condenses.

Referring now to Fig. 5F, in step 358 the VPN service provider software 30 waits for an event. When the VPN service provider software 30 senses that the SCP 32 has received on a signaling port a third-party billing setup message from the user terminal 26, then in step 360 the VPN service provider

Petitioner Apple Inc. - Exhibit 1026, p. 920

software 30 verifies the token just received from the user terminal 26, to determine, in step 362, if it is the same token that the VPN service provider software 30 sent to the user terminal 26 in step 344. If the token is not valid, then in step 364 the SCP 32 sends a release message to the terminal 26, and in step 366 condenses. If the token is valid, then in step 368 the SCP 32 sends a modified third-party billing setup message to the data network 14, and in step 370 condenses.

Although an illustrative embodiment of the invention has been shown and described, other modifications, changes, and substitutions are intended in the foregoing disclosure. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.

Petitioner Apple Inc. - Exhibit 1026, p. 921

WHAT IS CLAIMED IS:

1. A computerized method of a virtual private network service provider with third party billing, using a virtual private network to transfer data over a data network to a final destination, the method comprising the steps of:

a. prompting the user at a data terminal to select a destination, password, and call type;

b. selecting a virtual private network through the data network;

c. giving an encryption key to the user, and then prompting the user for a password and a user identification;

d. verifying the password, and providing an authorization code to the user; and

e. allowing the user to transfer the data through the data network to the final destination, using the authorization code.

2. The method of claim 1, wherein step (d) further comprises negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

3. The method of claim 2, wherein step (c) further comprises encrypting the user's password, and sending the user identification and the encrypted password to the virtual private network service provider.

4. The method of claim 3, further comprising, after step (a), the step of sending a set-up message to the data network.

5. The method of claim 4, further comprising, after step (c), the step of the virtual private network service provider decrypting the encrypted password.

6. An apparatus for providing a datalink connection from a user terminal to a data network and to a virtual private network, with third party billing, comprising:

a. an interface between the user terminal and the data network;

Petitioner Apple Inc. - Exhibit 1026, p. 922

b. a switching control point device connected to the data network, the switching control point device connected to a computer; and

c. a computer-readable medium encoded with a method of using the virtual private network and the data network, with third party billing, the computer-readable medium accessible by the computer.

7. The apparatus of claim 6, wherein the method comprises negotiating for more bandwidth for the user, and including within an authorization code a grant of additional bandwidth.

8. The apparatus of claim 7, wherein the method further comprises encrypting a user's password, and temporarily storing the user identification and the encrypted password.

9. The apparatus of claim 8, wherein the method further comprises sending a set-up message to the data network.

10. The apparatus of claim 9, wherein the method further comprises decrypting the encrypted password.

11. A computer-readable medium encoded with a method of using a virtual private network, with third party billing, the method comprising the steps of:

a. prompting the user at a data terminal to select a destination, password, and call type;

b. selecting a virtual private network through the data network;

c. giving an encryption key to the user, and then prompting the user for a password and a user identification;

d. verifying the password, and providing an authorization code to the user; and

e. allowing the user to transfer the data through the data network to the final destination, using the authorization code.

Petitioner Apple Inc. - Exhibit 1026, p. 923

12. The computer-readable medium of claim 11 wherein step (d) further comprises negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

13. The computer-readable medium of claim 12 wherein step (c) further comprises encrypting the user's password, and sending the user identification and the encrypted password to the virtual private network service provider.

14. The computer-readable medium of claim 13 further comprising, after step (a), the step of sending a set-up message to the data network.

15. The computer-readable medium of claim 14 further comprising, after step (c), the step of the virtual private network service provider decrypting the encrypted password.

16. An apparatus for providing a datalink connection from a user terminal to a data network and to a virtual private network, with third party billing, comprising:

a. means for prompting a user at the data terminal to select a destination, password, and call type;

b. means for selecting the virtual private network through the data network;

c. means for giving an encryption key to the user, and then prompting the user for a password and a user identification;

d. means for verifying the password, and providing an authorization code to the user; and

e. means for allowing the user to transfer data through the data network to a final destination, using the authorization code.

17. The apparatus of claim 16, further comprising means for negotiating for more bandwidth for the user, and including within the authorization code a grant of additional bandwidth.

Petitioner Apple Inc. - Exhibit 1026, p. 924

18. The apparatus of claim 17, further comprising means for encrypting the user's password, and sending the user identification and the encrypted password to the virtual private network service provider.

19. The apparatus of claim 18, further comprising means for sending a set-up message to the data network.

20. The apparatus of claim 19, further comprising means for decrypting the encrypted password.

Petitioner Apple Inc. - Exhibit 1026, p. 925

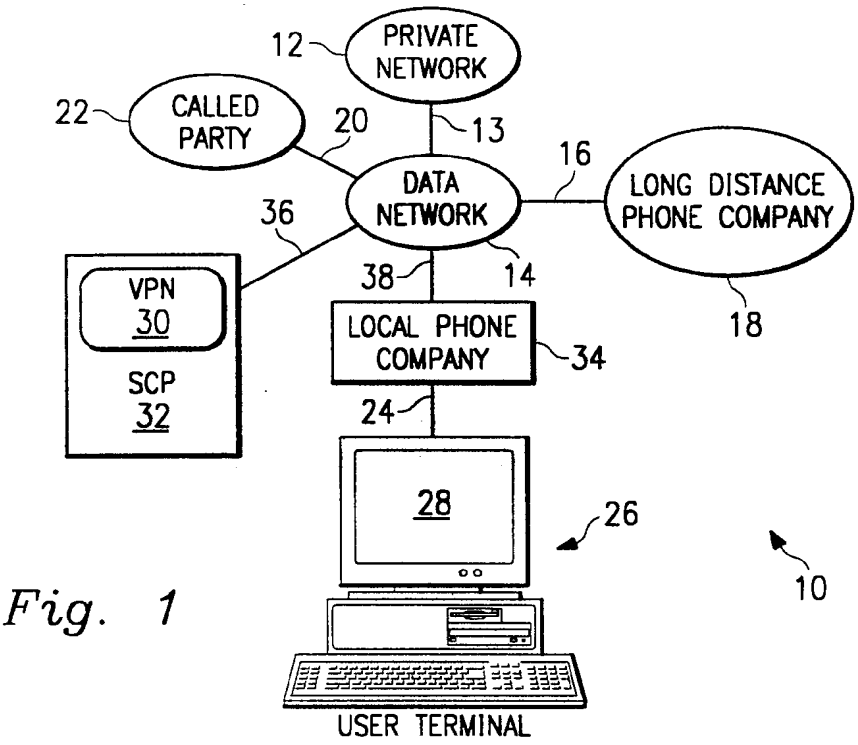

12
PRIVATE NETWORK
22
CALLED PARTY
20
13
16
DATA NETWORK
LONG DISTANCE PHONE COMPANY
36
38
14
18
VPN 30
SCP 32
LOCAL PHONE COMPANY
34
24
28
26
10
USER TERMINAL

Fig. 1

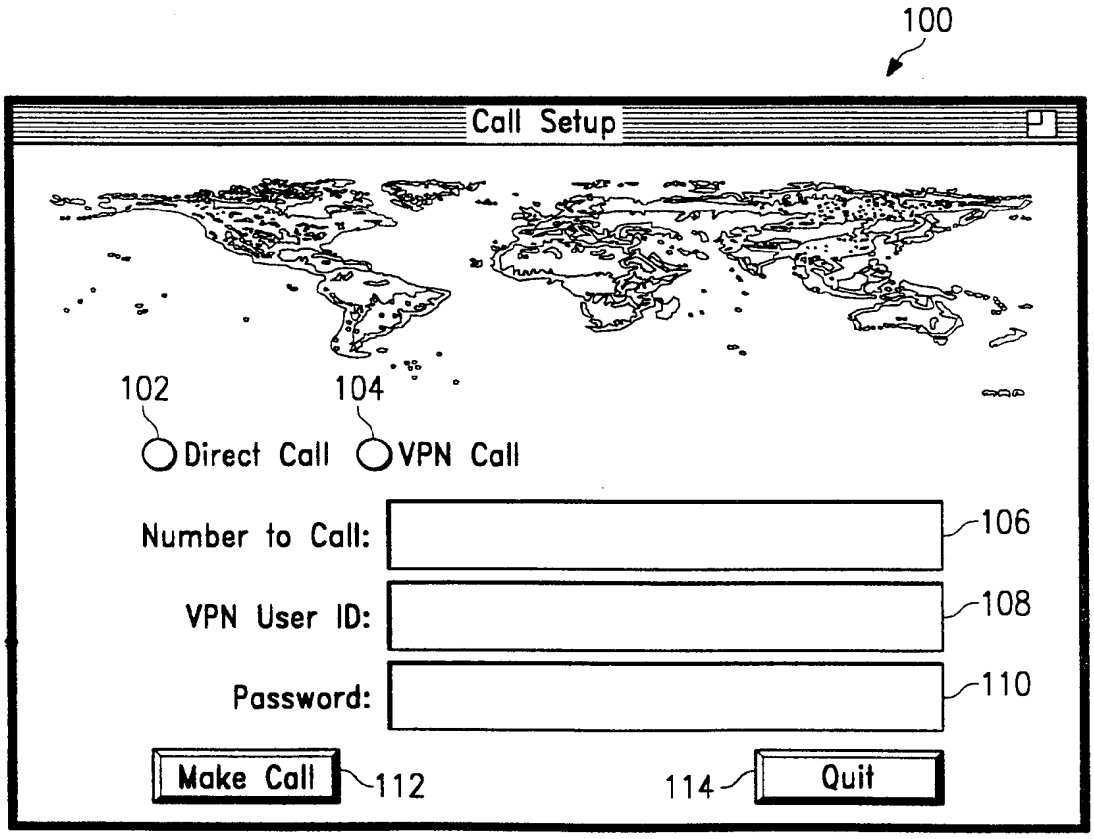

100
Call Setup
102
104
Direct Call
VPN Call
Number to Call:
106
VPN User ID:
108
Password:
110
Make Call
112
114
Quit

Fig. 3

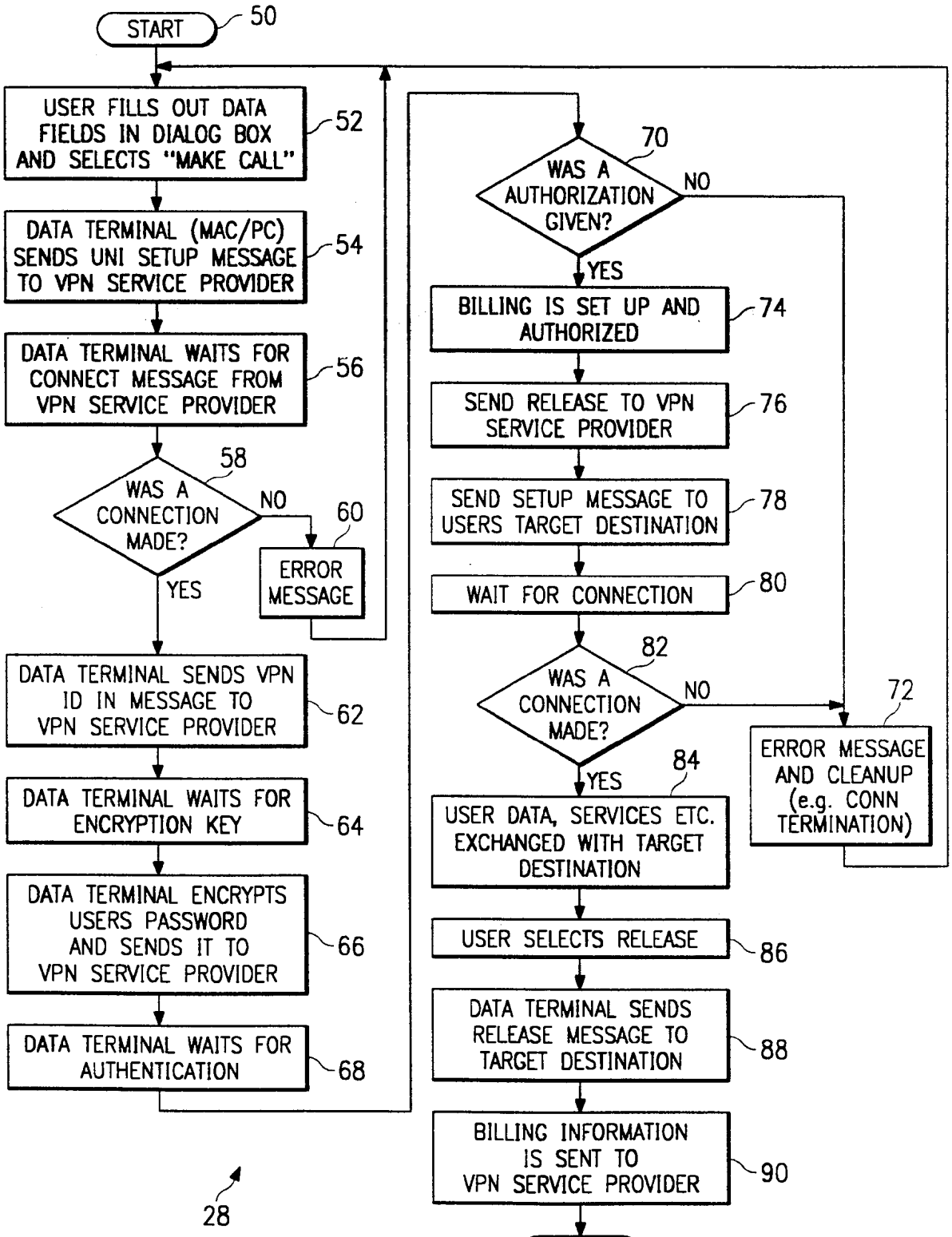

START
50
USER FILLS OUT DATA FIELDS IN DIALOG BOX AND SELECTS "MAKE CALL"
52
DATA TERMINAL (MAC/PC) SENDS UNI SETUP MESSAGE TO VPN SERVICE PROVIDER
54
DATA TERMINAL WAITS FOR CONNECT MESSAGE FROM VPN SERVICE PROVIDER
56
WAS A CONNECTION MADE?
58
NO
60
ERROR MESSAGE
YES
DATA TERMINAL SENDS VPN ID IN MESSAGE TO VPN SERVICE PROVIDER
62
DATA TERMINAL WAITS FOR ENCRYPTION KEY
64
DATA TERMINAL ENCRYPTS USERS PASSWORD AND SENDS IT TO VPN SERVICE PROVIDER
66
DATA TERMINAL WAITS FOR AUTHENTICATION
68
28
WAS A AUTHORIZATION GIVEN?
70
NO
YES
BILLING IS SET UP AND AUTHORIZED
74
SEND RELEASE TO VPN SERVICE PROVIDER
76
SEND SETUP MESSAGE TO USERS TARGET DESTINATION
78
WAIT FOR CONNECTION
80
WAS A CONNECTION MADE?
82
NO
72
ERROR MESSAGE AND CLEANUP (e.g. CONN TERMINATION)
YES
84
USER DATA, SERVICES ETC. EXCHANGED WITH TARGET DESTINATION
USER SELECTS RELEASE
86
DATA TERMINAL SENDS RELEASE MESSAGE TO TARGET DESTINATION
88
BILLING INFORMATION IS SENT TO VPN SERVICE PROVIDER
90
END
92

Fig. 2

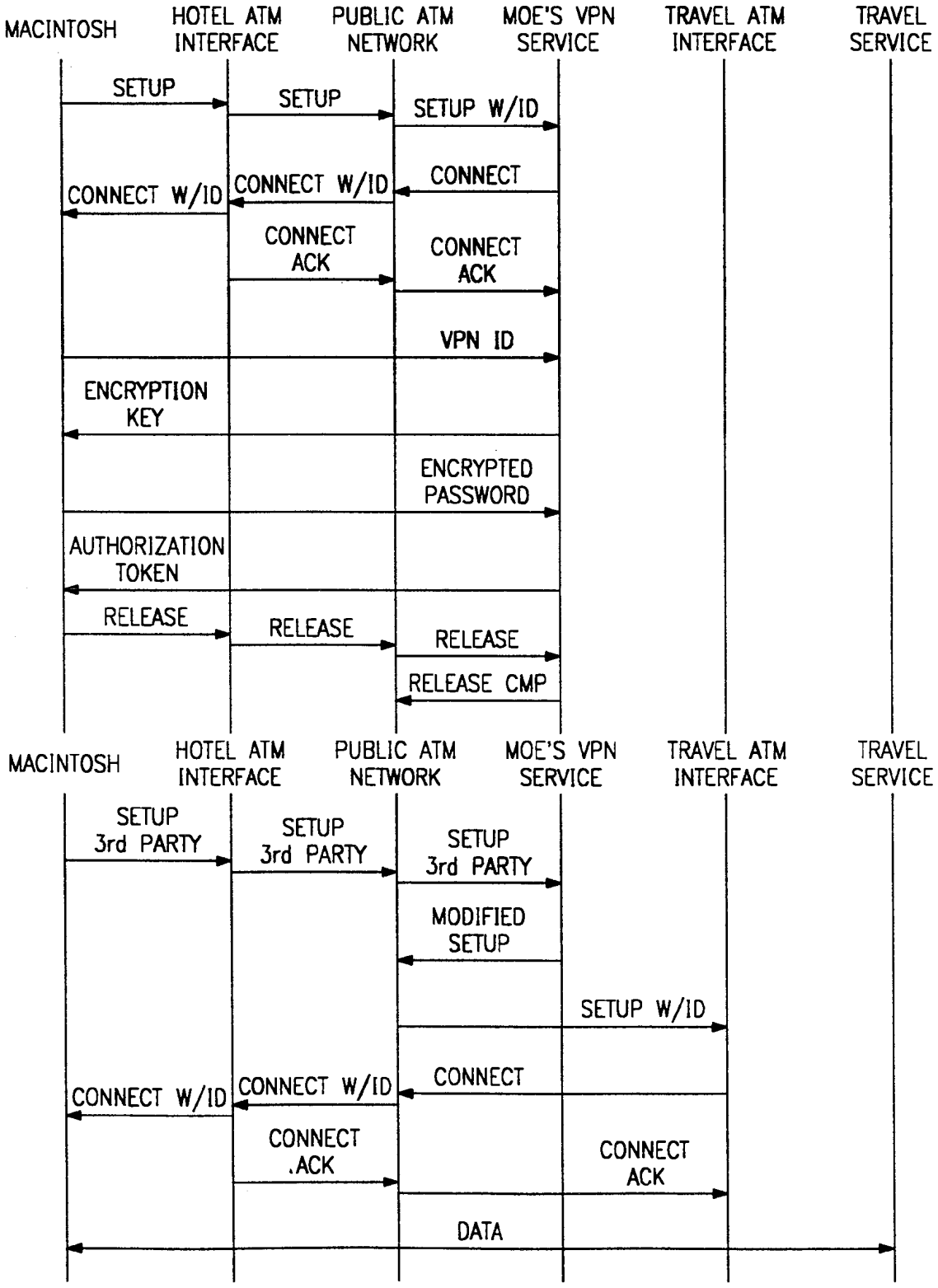

MACINTOSH
HOTEL ATM INTERFACE
PUBLIC ATM NETWORK
MOE'S VPN SERVICE
TRAVEL ATM INTERFACE
TRAVEL SERVICE
SETUP
SETUP
SETUP W/ID
CONNECT W/ID
CONNECT W/ID
CONNECT
CONNECT ACK
CONNECT ACK
VPN ID
ENCRYPTION KEY
ENCRYPTED PASSWORD
AUTHORIZATION TOKEN
RELEASE
RELEASE
RELEASE
RELEASE CMP
MACINTOSH
HOTEL ATM INTERFACE
PUBLIC ATM NETWORK
MOE'S VPN SERVICE
TRAVEL ATM INTERFACE
TRAVEL SERVICE
SETUP 3rd PARTY
SETUP 3rd PARTY
SETUP 3rd PARTY
MODIFIED SETUP
SETUP W/ID
CONNECT W/ID
CONNECT W/ID
CONNECT
CONNECT .ACK
CONNECT ACK
DATA

Fig. 4A

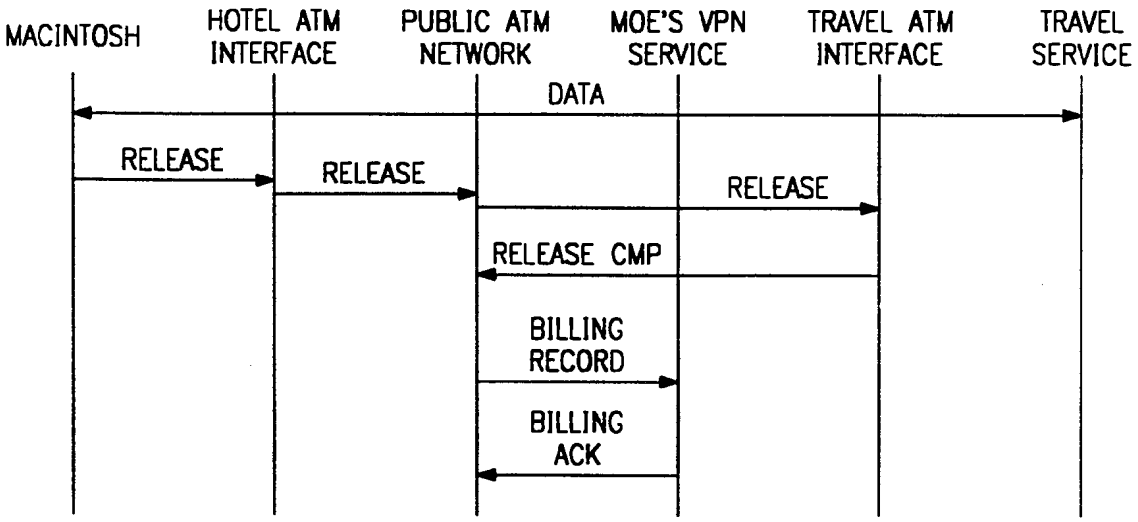


Fig. 4B

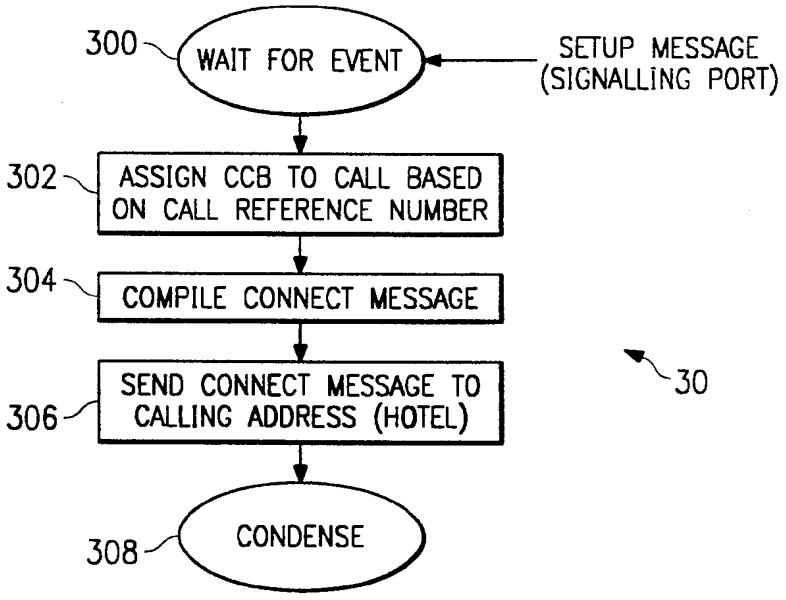


Fig. 5A

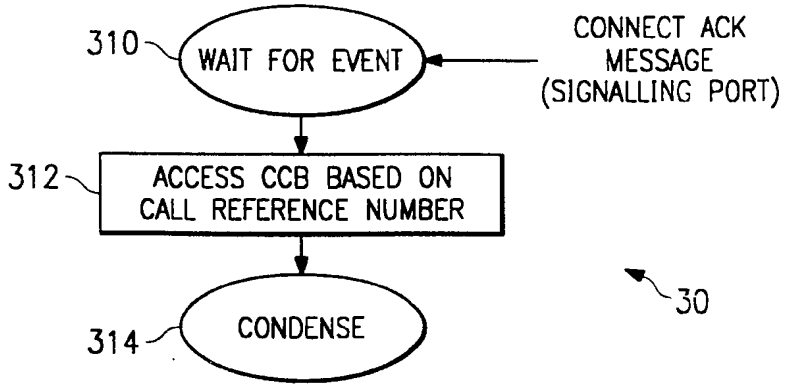


Fig. 5B

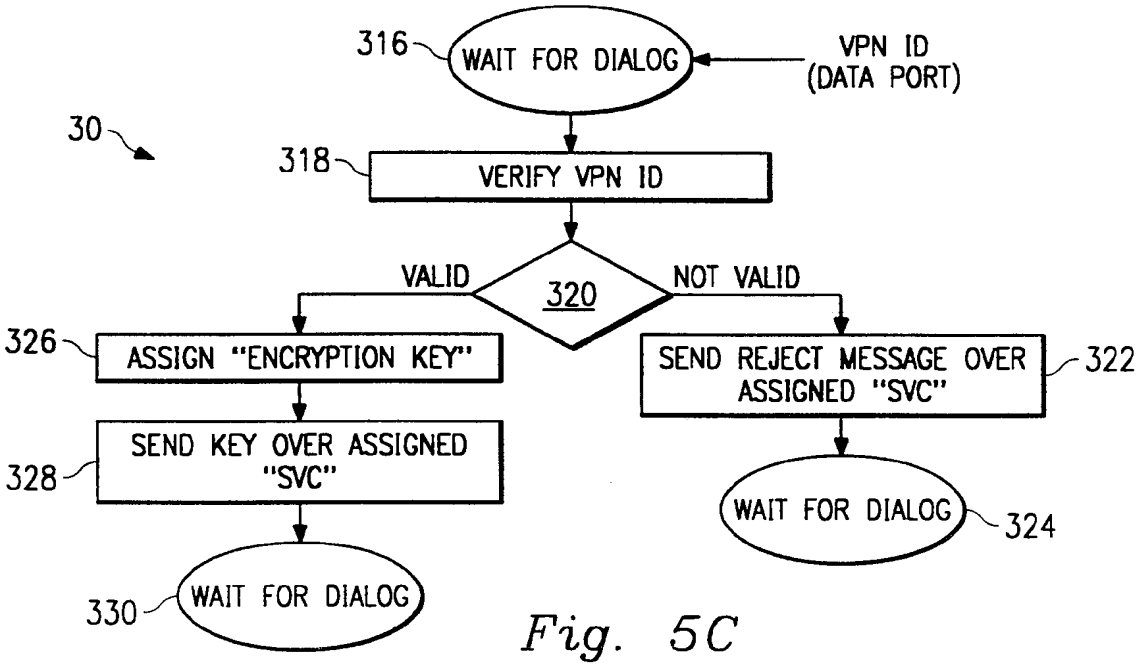

316
WAIT FOR DIALOG
VPN ID
(DATA PORT)
30
318
VERIFY VPN ID
VALID
320
NOT VALID
326
ASSIGN "ENCRYPTION KEY"
SEND REJECT MESSAGE OVER
ASSIGNED "SVC"
322
328
SEND KEY OVER ASSIGNED
"SVC"
WAIT FOR DIALOG
324
330
WAIT FOR DIALOG

Fig. 5C

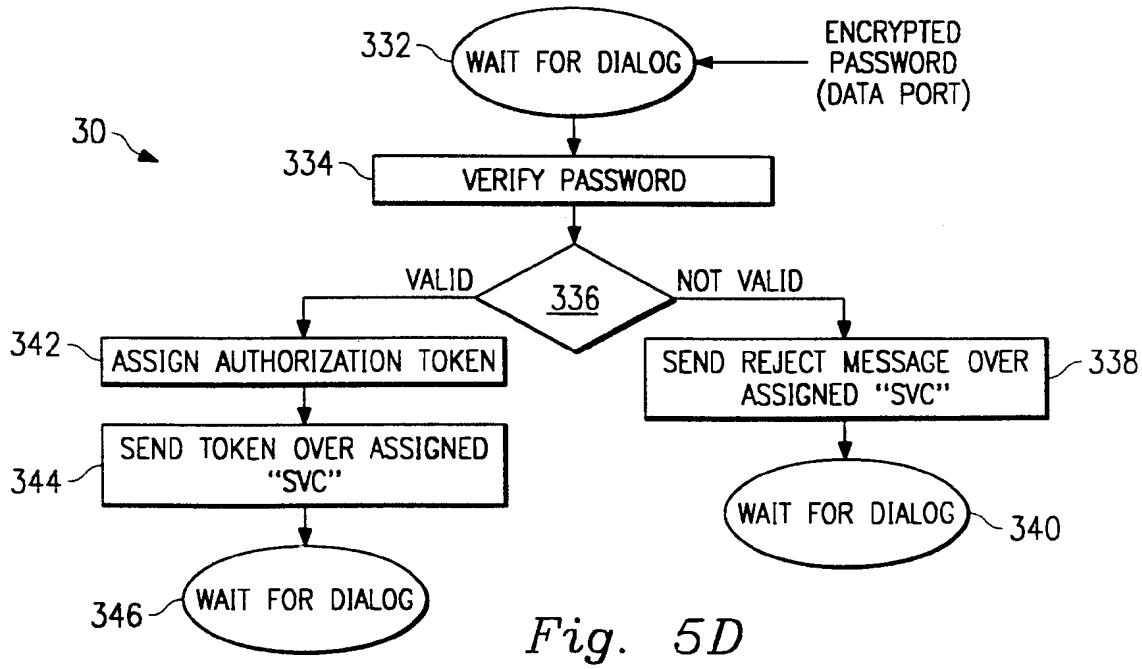

332
WAIT FOR DIALOG
ENCRYPTED
PASSWORD
(DATA PORT)
30
334
VERIFY PASSWORD
VALID
336
NOT VALID
342
ASSIGN AUTHORIZATION TOKEN
SEND REJECT MESSAGE OVER
ASSIGNED "SVC"
338
344
SEND TOKEN OVER ASSIGNED
"SVC"
WAIT FOR DIALOG
340
346
WAIT FOR DIALOG

Fig. 5D

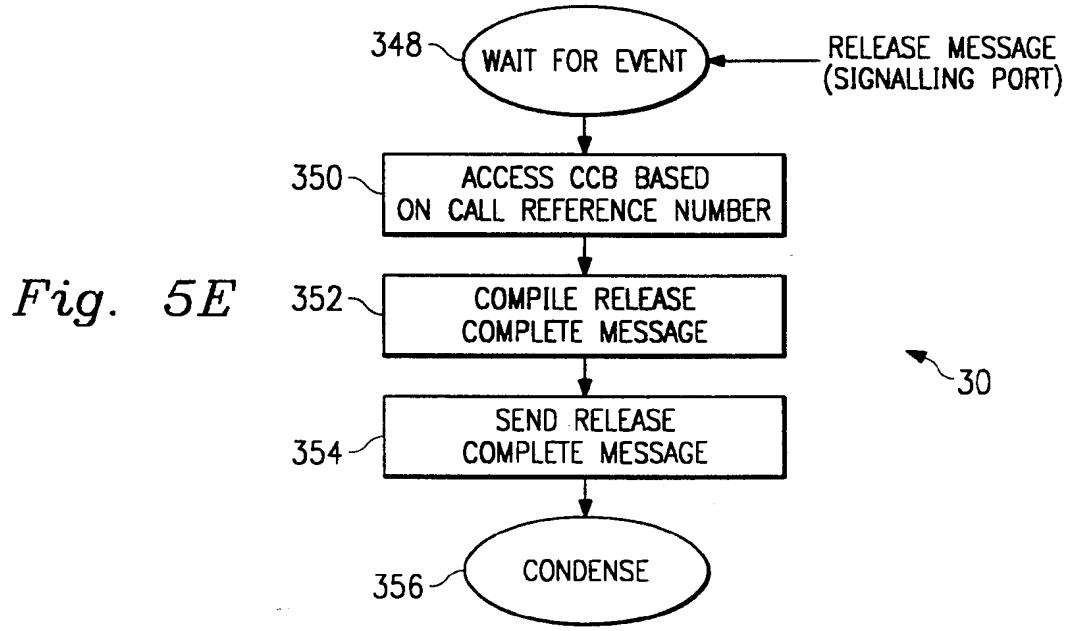

348
WAIT FOR EVENT
RELEASE MESSAGE (SIGNALLING PORT)
350
ACCESS CCB BASED ON CALL REFERENCE NUMBER
352
COMPILE RELEASE COMPLETE MESSAGE
30
354
SEND RELEASE COMPLETE MESSAGE
356
CONDENSE

Fig. 5E

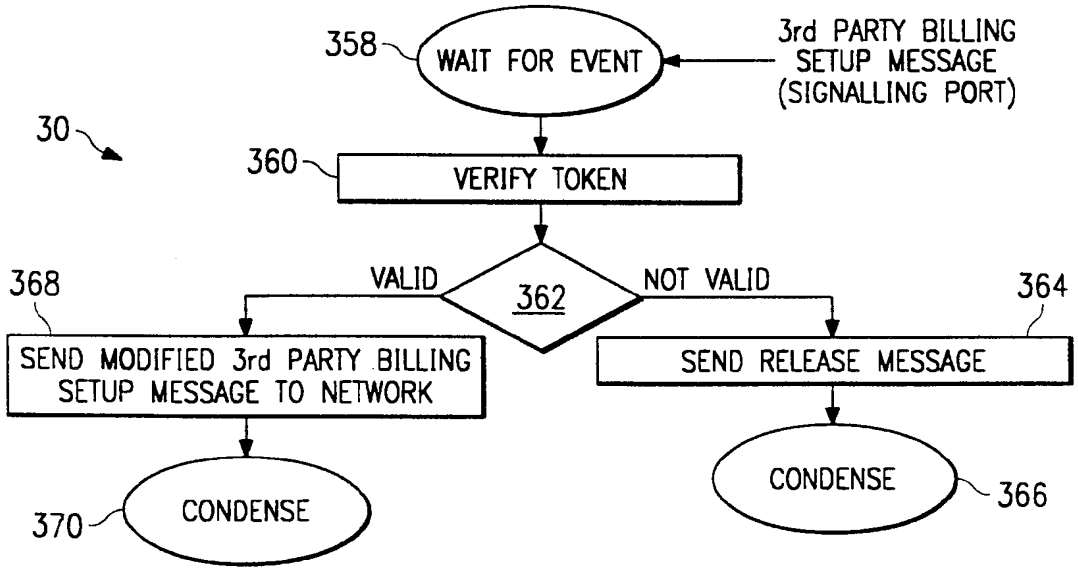

358
WAIT FOR EVENT
3rd PARTY BILLING SETUP MESSAGE (SIGNALLING PORT)
30
360
VERIFY TOKEN
368
VALID
362
NOT VALID
364
SEND MODIFIED 3rd PARTY BILLING SETUP MESSAGE TO NETWORK
SEND RELEASE MESSAGE
CONDENSE
370
CONDENSE
366

Fig. 5F

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/IB 97/01563

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q11/04 H04L12/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MUN CHOON CHAN ET AL: "AN ARCHITECTURE FOR BROADBAND VIRTUAL NETWORKS UNDER CUSTOMER CONTROL" NOMS '96 IEEE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM , vol. 1, 15 April 1996, KYOTO, JP, pages 135-144, XP000641086 see abstract ---	1-20
A	BIC V: "VOICE PERIPHERALS IN THE INTELLIGENT NETWORK" TELECOMMUNICATIONS, vol. 28, no. 6, June 1994, page 29/30, 32, 34 XP000600293 see the whole document ---	1-20
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
19 March 1998	02/04/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Staessen, B

Form PCT/ISA/210 (second sheet) (July 1992)

Petitioner Apple Inc. - Exhibit 1026, p. 932

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/IB 97/01563

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 729 256 A (NEDERLAND PTT) 28 August 1996 see abstract figures of pages 136 and 140	1-20
A	CROCETTI P ET AL: "ATM VIRTUAL PRIVATE NETWORKS: ALTERNATIVES AND PERFORMANCES COMPARISONS" SUPERCOMM/ICC '94, 1 May 1994, NEW ORLEANS, US, pages 608-612, XP000438985 see abstract	1-20

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

Petitioner Apple Inc. - Exhibit 1026, p. 933

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/IB 97/01563

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0729256 A	28-08-96	NL 9500339 A	01-10-96

Form PCT/ISA/210 (patent family annex) (July 1992)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00

A1

(11) International Publication Number: **WO 99/11019**

(43) International Publication Date: 4 March 1999 (04.03.99)

(21) International Application Number: PCT/US98/17198

(22) International Filing Date: 24 August 1998 (24.08.98)

(30) Priority Data:
08/917,341 26 August 1997 (26.08.97) US

(71) Applicant: V–ONE CORPORATION [US/US]; Suite 300, 20250 Century Boulevard, Germantown, MD 20874 (US).

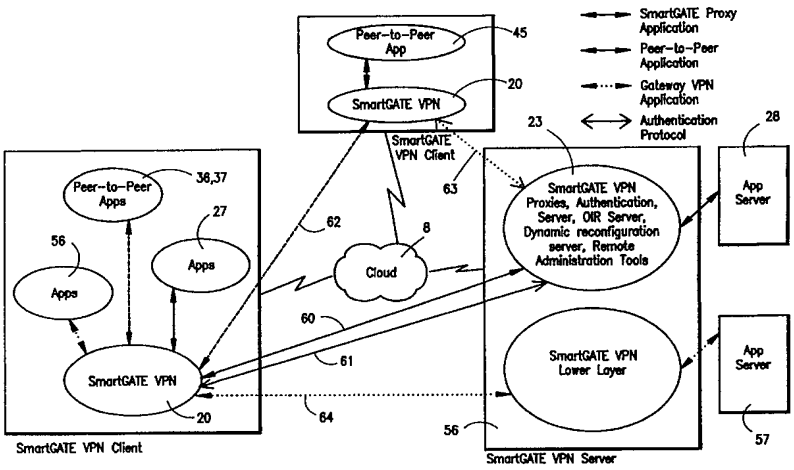
(72) Inventors: CHEN, James, F.; 12648 Tavilah Road, Potomac, MD 20854 (US). WANG, Jieh–Shan; 10903 Silent Wood Place, N. Potomac, MD 20878 (US). BROOK, Christopher, T.; 7308 Pomander Lane, Chevy Chase, MD 20815 (US). GARVEY, Francis; 2908 S. Buchanan Street, Arlington, VA 22206 (US).

(74) Agents: URCIA, Benjamin, E. et al.; Bacon & Thomas, PLLC, 4th floor, 625 Slaters Lane, Alexandria, VA 22314 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: MULTI–ACCESS VIRTUAL PRIVATE NETWORK



(57) Abstract

A virtual private network for communicating between a server and clients over an open network uses an applications level encryption and mutual authentication program (20) and at least one shim (50, 53) positioned above either the layers of a client computer to intercept function calls, communicate with the server and authenticate the parties to a communication and enable the parties to the communication to establish a common session key. Where the parties to the communication are peer–to–peer applications (36, 37, 45), the intercepted function calls, request for service, or data packets include the destination address of the peer application, which is supplied to the server so that the server can authenticate the peer and enable the peer to decrypt further direct peer–to–peer communications (62).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

MULTI-ACCESS VIRTUAL PRIVATE NETWORK

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates a system and method for allowing private communications over an open network, and in particular to a virtual private network which provides data encryption and mutual authentication services for both client/server and peer-to-peer applications at the applications, transport driver, and network driver levels.

2. Discussion of Related Art

A virtual private network (VPN) is a system for securing communications between computers over an open network such as the Internet. By securing communications between the computers, the computers are linked together as if they were on a private local area network (LAN), effectively extending the reach of the network to remote sites without the infrastructure costs of constructing a private network. As a result, physically separate LANs

can work together as if they were a single LAN, remote computers can be temporarily connected to the LAN for communications with mobile workers or telecommuting, and electronic commerce can be carried out without the risks inherent in using an open network.

In general, there are two approaches to virtual private networking, illustrated in Figs. 1A and 1B. The first is to use a dedicated server 1, which may also function as a gateway to a secured network 2, to provide encryption and authentication services for establishment of secured links 3 between the server 1 and multiple clients 4-6 over the open network 7, represented in Fig. 1A as a cloud, while the second is to permit private communications links 8 to be established between any two computers or computer systems 9-12 on network 7, as illustrated in Fig. 1B.

The advantages of a client/server arrangement such as the one shown in Fig. 1A are that the server can handle functions requiring the majority of the computing resources, increasing the number of potential clients, and that management of the network, including key management is centralized. The disadvantage of a client/server network of this type is that peer-to-peer communications links between applications on the client computers cannot utilize the security and management functions provided by the server, leaving such communications unprotected. On the

Petitioner Apple Inc. - Exhibit 1026, p. 938

other hand, the advantage of the direct peer-to-peer approach illustrated in Fig. 1B is that it permits secured links to be established between any computers capable of carrying out the required security functions, with the disadvantages being the cost of configuring each computer to carry-out encryption, authentication, and key management functions, and the lack of central control.

In both the client/server and peer-to-peer approaches, a virtual private network can in theory be based either on applications level technology or can operate at a lower level. Generally, however, peer-to-peer "tunneling" arrangements require modification of the lower layers of a computer's communications architecture, while client/server arrangements can use the applications level approach because less modification of the clients is required, and thus the two approaches are in practice mutually exclusive. The present invention, on the other hand, seeks to provide a virtual private network which utilizes a client/server approach, including centralized control of encryption, authentication, and key management functions, while at the same time enabling secured peer-to-peer communications between applications, by utilizing the server to provide authentication and session key generation functions for both client to server communications and peer-to-peer communications, providing a virtual private network capable of serving both as an extended intranet or wide area network (WAN), and as a commercial mass marketing network,

Petitioner Apple Inc. - Exhibit 1026, p. 939

with high level mutual authentication and encryption provided for all communications.

In order to completely integrate the two approaches and maximize the advantage of each approach, the invention maintains the applications level infrastructure of prior client server private networking arrangements, while adding shims to lower levels in order to accommodate a variety of peer-to-peer communications applications while utilizing the applications level infrastructure for authentication and session key generation purposes. This results in the synergistic effect that not only are existing peer-to-peer tunneling schemes and applications level client server security arrangements combined, but they are combined in a way which greatly reduces implementation costs

In order to understand the present invention, it is necessary to understand a few basic concepts about computer to computer communications, including the concepts of "layers" and communications protocols, and of mutual authentication and file encryption. Further information about layers and protocols can be found in numerous sources available on the Internet, a few of which are listed at the end of this section, while a detailed description of a mutual authentication and encryption system and method suitable for use in connection with the present invention can be found in U.S. Patent No. 5,602,918, which is incorporated herein by reference. In general, the basic

Petitioner Apple Inc. - Exhibit 1026, p. 940

communications protocols and architecture used by the present invention, as well as authentication, encryption, and key management schemes, are already well-known, and can be implemented as a matter of routine programming once the basic nature of the invention is understood. The changes made by the present invention to the conventional client server virtual private network may be thought of as, essentially, the addition of means, most conveniently implemented as shims, which add a secured mutual authentication and session key generation channel between the server and all parties to a communication, at all levels at which a communication can be carried out.

Having explained the key differences between the present invention and existing systems, the basic concepts of layers and so forth will now be briefly explained by way of background. First, the concept of "layers," "tiers," and "levels," which essential to an understanding of the invention, simply refers to libraries or sets of software routines for carrying out a group of related functions, and which can conveniently be shared or called on by different programs at a higher level to facilitate programming, avoiding duplication and maximizing computer resources. For example, the Windows NT device driver architecture is made up of three basic layers, the first of which is the Network Driver Interface Specification (NDIS 3.0) layer, the second of which is called the Transport Driver Interface (TDI) layer, and the third being the file

Petitioner Apple Inc. - Exhibit 1026, p. 941

systems. These layers are generically referred to as the network driver layer, the transport or transport driver layer, and the applications layer.

In the Windows NT architecture, the TDI layer formats data received from the various file systems or applications into packets or datagrams for transmission to a selected destination over the open network, while the NDIS layer controls the device drivers that send the data, packets, or IP datagrams, for example by converting the stream of data into a waveform suitable for transmission over a telephone line or a twisted pair cable of the type known as an Ethernet.

By providing layers in this manner, an applications software programmer can design an application program to supply data to the TDI layer without having to re-program any of the specific functions carried out by that layer, and all of the transmission, verification, and other functions required to send a message will be taken care of the TDI layer without further involvement by the applications software. In a sense, each "layer" simply accepts data from the higher layer and formats it by adding a header or converting the data in a manner which is content independent, with retrieval of the data simply involving reverse conversion or stripping of the headers, the receiving software receiving the data as if the intervening layers did not exist.

Petitioner Apple Inc. - Exhibit 1026, p. 942

In the case of Internet communications, the most commonly used set of software routines for the transport or TDI layer, which takes care of the data formatting and addressing, is the TCP/IP protocol, in which the transport control protocol (TCP) packages the data into datagrams and provides addressing, acknowledgements, and checksum functions, and the internet protocol (IP) further packages the TCP datagrams into packets by adding additional headers used in routing the packets to a destination address. Other transport protocols which can be included in the TDI layer include the user diagram protocol (UDP), the internet control message protocol (ICMP), and non-IP based protocols such as Netbeui or IPX.

Additional "protocols" are may be used at the applications level, although these protocols have nothing to do with the present invention except that they may be included in the applications programs served by the network. Common applications level protocols which utilize the TCP/IP protocol include hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), and file transfer protocol (FTP), all of which operate at the layer above the transport layer.

Some applications are written to directly call upon the TCP functions. However, for most applications utilizing a graphical user interface conveniently rely on a set of software routines which are considered to operate

Petitioner Apple Inc. - Exhibit 1026, p. 943

above the TDI layer, and are known as sockets. Sockets serve as an interface between the TCP set of functions, or stack, and various applications, by providing libraries of routines which facilitate TCP function calls, so that the application simply has to refer to the socket library in order to carry out the appropriate function calls. For Windows applications, a commonly used non-proprietary socket is the Windows socket, known as Winsock, although sockets exist for other operating systems or platforms, and alternative sockets are also available for Windows, including the Winsock 2 socket currently under development.

In order to implement a virtual private network, the encryption and authentication functions must be carried out at one of the above "levels," for example by modifying the network drivers to encrypt the IP datagrams, by inserting authentication headers into the TCP/IP stacks, or by writing applications to perform these functions using the existing drivers. If possible, it is generally desirable to minimize modification of the existing levels by adding a layer to perform the desired functions, calling upon the services of the layer below, while utilizing the same function calls so that the higher layer also does not need to be modified. Such a layer is commonly referred to as a "shim."

As indicated above, the preferred approach to implementing client/server virtual private networks is to

Petitioner Apple Inc. - Exhibit 1026, p. 944

use an applications level security system to encrypt files to be transmitted, and to then utilize existing communications layers such as Winsock, or TCP/IP directly. This is the approach taken by the commercially available access control system known as SmartGATE™, developed by V-One Corp. of Germantown, Md., which provides both encryption and mutual authentication at the applications level utilizing a dedicated server known as an authentication server and authentication client software installed at the applications level on the client computers. A description of the manner in which encryption and mutual authentication is carried out may be found in the above-cited U.S. Patent No. 5,602,918. While the principles of the invention are applicable to other client/server based virtual private networks, SmartGATE™ is used as an example because it provides the most complete range of mutual authentication and encryption services currently available.

The present invention can be implemented using the existing SmartGATE™ system, but adds mutual authentication and encryption services to lower layers by intercepting function calls or data packets and, during initialization of a communications link, establishing separate channels between the party initiating the communication and the authentication server, and between the authentication server and the party which is to share in the communication, so as to mutually authenticate the parties

Petitioner Apple Inc. - Exhibit 1026, p. 945

with respect to the server, and so as to establish a session key which can be used for further direct communications between the parties.

A number of protocols exist which can be used, in total or in part, to implement the mutual authentication and encryption services at the lower layers, using the same basic authentication and encryption scheme currently implemented by SmartGATE™ at the applications level. These include, by way of example, the SOCKS protocol, which places a shim between the TDI or transport layer and the applications, and the commercially available program, known as SnareNet, which operates at the network driver level and can be directly utilized in connection with the present invention.

On the other hand, a network level implementation such as the SKIP protocol, which operates below the TDI layer to encrypt the datagrams, and which in its description explicitly precludes the generation of session keys (see the above cited U.S. Patent No. 5,602,918), is fundamentally different in concept than the present invention. Similarly, alternative implementations such as Point-to-Point Tunneling Protocol (PPTP) which involve modifying the TCP/IP stack and/or hardware to provide encryption, as opposed to inserting shims, are not utilized by the preferred embodiment of the present invention, although individual aspects of the protocol could perhaps

Petitioner Apple Inc. - Exhibit 1026, p. 946

be used, and the present system could be added to computers also configured to accept PPTP communications.

The SmartGATE™ system uses public key and DES encryption to provide two-way authentication and 56-bit encrypted communications between a server equipped with the SmartGATE program and client computers equipped with a separate program. Currently, SmartGATE™ operates at the highest level, or applications level, by using shared secret keys to generate a session key for use in further communications between the authentication server or gateway and the client program. Since the session key depends on the secret keys at the gateway and client sides of the communication, mutual authentication is established during generation of the session key, which can then be used to encrypt further communications.

When installed on a client system, the SmartGATE™ client software reads a request for communications by an applications program, such as a browser program, and then proceeds to establish its own communications link with the destination server to determine if the server is an authentication server. If it is not, control of communications is relinquished, but if it is, then the security program and the server carry out a challenge/response routine in order to generate the session key, and all further communications are encrypted by the security program. Although this program is placed between

Petitioner Apple Inc. - Exhibit 1026, p. 947

the Winsock layer and the applications, it does not function as a shim, however, because it only affects communications directed to the authentication server.

Having briefly summarized the concepts used by the present invention, including the concepts of layers, protocols, and shims, and having described a specific applications level security program which is to be modified according to the present invention by adding shims in a way which enables secured authentication and session key generation channels to be set up from the lower layers, it should now be possible to understand the nature of the invention, and in particular how it integrates the two approaches to virtual private networking in a way which greatly expands the concept and yet can easily be implemented. More details will be given below, but as a final observation in this background portion of the patent specification, it should be noted that while the overall concept of the invention is in a sense very simple, it is fundamentally at odds with present approaches. For example, the literature is replete with references to conflicts between VPN standards and implementations, as exemplified by the title of an article from LAN Times On-Line, 9/96, (http://www.wcmh.com/), which reads *Clash Over VPN Supremacy*. Even a cursory search of the available literature indicates that the amount of information and choices available to those wishing to set up a virtual private network is overwhelming. One can choose between

Petitioner Apple Inc. - Exhibit 1026, p. 948

Netscape Communications Secure Socket Layer, Open Market Inc.'s Secure HTTP, Microsoft's PPTP, among others. However, all of these approaches operate at a single level, and force a choice between establishing a network of the type shown in Fig. 1A and a network of the type shown in Fig. 1B. Only the present invention offer the advantages of both approaches, without the inflexibility of client/server arrangements or the costs of more distributed architectures.

For further information on the various competing VPN protocols and systems, see also *The Development of Network Security Technologies*, Internet Smartsec, 2/97 (http://www.smartsec.se), which compares SmartGATE™ to other application level security systems, including PPTP, SSL, and S-HTTP; *Point-To-Point Tunneling Protocol (PPTP) Frequently Asked Questions*, Microsoft Corp., date unknown, (http://www.microsoft.com), *Simple Key-Management for Internet Protocols (SKIP)*, Aziz *et al.*, date unknown, (http://skip.incog.com), and *SOCKS Protocol Version 5, RFC 1928*, Leech *et al.*, 3/96 (http://andrew2.andrew.cmu.edu) (this document describes a protocol involving a TDI shim). For more general information on security problems, Internet protocols, and sockets, see *Introduction to the Internet Protocols*, Charles L. Hedrick, Rutgers University, 1987 (http://oac3.hsc.uth.tmc.edu); *Windows Sockets - Where Necessity is the Mother of Reinvention*, Stardust

Petitioner Apple Inc. - Exhibit 1026, p. 949

Technologies, Inc., 1996, (http//www.stardust.com), and *Secure Internet Connections*, LAN Times, 6/17/96 (Ibid).

SUMMARY OF THE INVENTION

It is accordingly a principal objective of the invention to provide a client/server virtual private network which is capable not only of carrying out authenticated secure communications over an open network between an authentication server and clients, but also authenticated secure peer-to-peer communications.

It is also an objective the invention to provide a virtual private network that provides data encryption and mutual authentication for both client/server and peer-to-peer communications for different-types of applications, using both the applications level and lower levels of a communications hierarchy.

It is a further objective of the invention to provide a client/server virtual private network which can provide both client/server and peer-to-peer encryption and authentication services for any application sharing a specified socket or sockets, whether or not the application is recognized by the encryption and authentication program.

It is a still further objective of the invention to provide a client/server virtual private network which can

Petitioner Apple Inc. - Exhibit 1026, p. 950

provide encryption and authentication services at the applications level, transport driver interface level, and network interface level, without the need for modifying either the communication driver or network driver, or any sockets utilizing the communications driver interface.

It is yet another objective of the invention to provide a virtual private network which provides encryption and authentication services for peer-to-peer communications while maintaining centralized control of key distribution and management functions.

Finally, it is also an objective of the invention to provide a virtual private network which provides encryption and authentication services for peer-to-peer communications and in which registration is carried out by a central gateway server.

These objectives of the invention are accomplished by providing a virtual private network for communicating between a server and clients over an open network and in which the clients are equipped with an applications level encryption and mutual authentication program which includes at least one shim positioned above either the socket, transport driver interface, or network interface layers of a client computers communications hierarchy, and which intercepts function calls or data packets in order to authenticate the parties to the communication by

Petitioner Apple Inc. - Exhibit 1026, p. 951

establishing secured channels between the server and the parties to the communication, prior to establishment of the secured communications link between the parties, in order to carry out mutual authentication and session key generation functions.

More particularly, according to the principles of a preferred embodiment of the invention, client communications software is provided which, at the socket or transport driver interface levels, intercepts function calls to the socket or transport driver and directs calls to the authentication server in order to perform encryption and authentication routines, and at the network driver interface, performs encryption and authentication functions by intercepting the datagrams or data portions of the packets transmitted by the transport driver interface based on communications between the authentication server and the client. According to this aspect of the invention, a system of providing authentication and encryption services for the purpose of establishing a virtual private network includes a plurality of shims arranged to operate at different protocol levels in order to establish a common secure communications link to an authentication server.

In one especially preferred embodiment of the invention, the client software includes a Winsock shim arranged to intercept function calls to the Winsock library on a client machine and redirect initial communications

Petitioner Apple Inc. - Exhibit 1026, p. 952

through the authentication client software to the authentication server, so that any function calls to the Winsock library of programs are intercepted by the shim and carried out by the applications level security program. In this embodiment, the client authentication software substitutes its own function calls for the original function calls in order to establish a secured communications link to the authentication server over which such functions as mutual authentication between the client and server, indirect authentication of peer applications by the now trusted server, session key generation, are carried out, as well as ancillary functions such as on-line registration (OLR), utilizing the unmodified original Winsock library and TCP/IP communications stacks.

By inserting a shim at the Winsock level, an applications level client/server based security program such as SmartGATE™ can be used to provide secure communications for any application which utilizes the Winsock library. In addition, by including analogous shims at other levels, the invention can be used to secure virtually any communications application, including those which by-pass the TDI layer and communicate directly with the network driver level.

Instead of the current array of mutually exclusive alternative methods and systems of establishing secured communications over an open network, the invention thus

Petitioner Apple Inc. - Exhibit 1026, p. 953

provides a single integrated method and system capable of carrying out both client/server communications and peer-to-peer communications between a wide variety of communications applications regardless of whether the applications use a socket or even commonly accepted internet protocols, with complete mutual authentication and encryption of data files at all levels and between all parties to the network.

It will be appreciated that the term "virtual private network" is not to be taken as limiting, and that the principles of the invention can be applied to any remote access schemes which utilize the Internet or other relatively insecure networks to provide access for remote users, corporate intranets, and electronic commerce.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1A is a schematic diagram of a client/server virtual private network.

Fig. 1B is a schematic diagram of an alternative virtual private network based on peer-to-peer communications.

Fig. 2 is a functional block diagram showing the operation of an applications level security program in a conventional communications network hierarchy.

Petitioner Apple Inc. - Exhibit 1026, p. 954

Fig. 3 is a functional block diagram showing the communications network hierarchy of Fig. 1, modified to provide a second layer of service in accordance with the principles of a preferred embodiment of the invention.

Fig. 4 is a functional block diagram showing the communications network hierarchy of Fig. 2, modified to provide a third layer of service in accordance with the principles of the preferred embodiment.

Fig. 5 is a functional block diagram showing the communication network hierarchy of Fig. 3, modified to provide a fourth layer of service in accordance with the principles of the preferred embodiment.

Fig. 6 is a schematic diagram of a virtual private network utilizing the principles of the preferred embodiment of the invention.

Fig. 7 is a flowchart illustrating a method of implementing the system of the preferred embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 2 illustrates the operation of a client authentication program which is utilized in the present invention. An example of such a program is the SmartGATE™ program discussed briefly above, although other

Petitioner Apple Inc. - Exhibit 1026, p. 955

applications level security programs, whether or not token based, could be modified in a manner similar to that discussed in the following description. The illustrated hierarchy is the Windows NT architecture, although versions of SmartGATE™ exist for other architectures, and the invention could easily be adapted for use with any version of SmartGATE™, including UNIX and MacIntosh versions, as well as for use with applications level security programs designed for communications architectures other than those supported by SmartGATE™. Conversely, it is intended that the present invention can be used with authentication and encryption schemes other than that used by SmartGATE™ and disclosed in U.S. Patent No. 5,602,918. For purposes of convenience, therefore, the software represented by SmartGATE™ is simply referred to as client authentication software.

In addition, it noted that the client computer architectures illustrated in Figs. 3-6, which are modified versions of the architecture of Fig. 2, is to be used with an overall network layout such as the one illustrated in Fig. 6, which includes an authentication server that may be a SmartGATE™ server, or another server depending on the client authentication software. The invention is not merely the addition of shims to the client software, but involves the manner in which the shims are used in the establishment of the authentications and key generation links to the server.

Petitioner Apple Inc. - Exhibit 1026, p. 956

Turning to Fig. 2, which provides background for the description of the invention illustrated in Figs. 3-6, the client authentication software 20 is situated above the boundary of the transport or TDI layer 21 and is designed to utilize a socket 22, such as Winsock, to carry out communications with the authentication server 23 shown in Fig. 6 by means of a transport protocol such as TCP/IP, UDP, or the like, which in turn supply datagrams or packets to a hardware driver layer 24, such as NDIS 3.0, of a network or modem connection 25.

In operation, the client authentication software 20 intercepts interconnect calls 26 form client authentication software supported applications 27 and, if the calls are directed to the authentication server 23, or to a server 28 situated on a secured network whose access is controlled by the authentication server, establishes a secured communications link to the server by executing appropriate function calls 29 to the socket library, which in turn transmits function calls 30 to the TDI layer, causing the TDI layer to form datagrams or packets 31. Datagrams or packets 31 are then formatted over packaged for transmission by the hardware drivers 24 and sent to the communications network in the form of Ethernet packets or analog signals 32 containing the original datagrams from the TDI layer. Once the secured communications link has been established, client authentication software 20 encrypts all further data communications 34 from

Petitioner Apple Inc. - Exhibit 1026, p. 957

applications 27, which are indicated by dashed lines, before handing them off to the next lower layer in the form of encrypted files 35. The dashed lines are shown in Fig. 2 as extending only to the TDI layer 21, because the datagrams formed by the TDI layer are indistinguishable as to content, but it is to be understood that datagrams or packets 31 carry both the communications used to establish the secure channel, and the encrypted files subsequently sent therethrough.

Finally, in the case of SmartGATE™, the authentication client software utilizes either a smart card or secured file to supply the secret keys used during authentication to generate a session key for encryption of further communications, and also to carry out certain other encryption and authentication functions, although it is of course within the scope of the invention to use key distribution and authentication methods which do not rely on smartcards or tokens, and the tokens are not involved in any of the basic communications functions of the client authentication software 20.

In addition to the applications 27 which communicate with the server via the authentication/encryption software 20, a typical system will have a number of additional software applications 36 and 37 capable of carrying out communications over the open network, but which the authentication client software is not configured to handle,

Petitioner Apple Inc. - Exhibit 1026, p. 958

and which are not specifically adapted or intended to carry out communications with the authentication server. These are referred to herein as peer-to-peer applications, and can include applications which use the same sockets as the authentication client software, applications which directly call upon a transport driver interface stack, whether using the same protocol as the authentication client software or another protocol, all of which are intended to be represented by the TDI layer, and applications which are written to call directly upon the hardware drivers. These peer-to-peer applications may have their own encryption and authentication capabilities, but cannot utilize the services of the authentication server or client software, and therefore the function calls made by the applications and the files transmitted are indicated by separate reference numerals 40-43.

It will be appreciated by those skilled in the art that lower layer application programs which generate packets in forms other than those represented by the TDI layer are also possible, and should be considered within the scope of the invention, but at present virtually all open network applications use at least one of the TDI protocols, and thus while these programs may interact directly with the network driver layer, and require a network driver layer shim, as will be discussed below, are illustrated for purposes of convenience as part of the TDI layer applications.

Petitioner Apple Inc. - Exhibit 1026, p. 959

Turning now to a preferred embodiment of the invention, the arrangement shown in Fig. 3 modifies the arrangement of Fig. 2 by adding a socket shim 50 between the socket 22 utilized by the authentication client software 20, the peer-to-peer applications 36 which also utilize the socket 20, and the authentication client software itself. The shim 50 operates by hooking or intercepting call initiation function calls 40 made to the socket and, in response thereto, having the authentication client software initiate communications with the authentication server 23, shown in Fig. 6, in order to carry out the authentication protocol, as will be discussed in more detail below. Shim 50 also causes files 41 intended for the TDI layer to be diverted to the authentication software for encryption based on the session keys generated during the initial communications with the authentication server, and transmission as encrypted files 51 addressed to the peer application, also shown in Fig. 6, which could also be an application on the application server 28.

Since the basic authentication client software is designed to send all communications directly to the authentication server, while the peer-to-peer applications are designed only to communicate with "peers" 45 and not with the authentication server, the principal function of shim 50 is to arrange for the destination of address of the communication to be supplied to both the authentication

Petitioner Apple Inc. - Exhibit 1026, p. 960

client software and to authentication server, even though the peer application assumes that it is communicating only with the peer application. This function permits session key encrypted communications to be forwarded directly to the peer application, as illustrated in Fig. 6, while the latter function provides the authentication server with the client address so that the authentication server can establish a secured and authenticated link with the peer application, via authentication client software on the peer computer, and transmit the session key to the peer application or at least enable the peer application to recreate the session so that it can decrypt the encrypted files received directly from the client application.

Thus, while it is appreciated that the use of socket shims is well-known, as mentioned above, the socket shim shown in Fig. 2 has the unique function of enabling direct peer-to-peer communications with mediation by the authentication server, permitting the highest level of authentication service and collateral functions. In addition, because of the mediation by the key server, the peer applications do not need to have a shared secret key, allowing centralized key management, with only the authentication server having access to all of the client's secret keys.

Figs. 4 shows the variation of the client authentication software 20 in which a TDI shim 52 similar

Petitioner Apple Inc. - Exhibit 1026, p. 961

in function to the socket shim 50 is provided above the TDI layer. Like the socket shim, implementation of the TDI shim essentially simply involves diverting certain information to the client software in order to establish a communications link with the authentication server, and subsequently perform encryption to obtain encrypted files 54 for transmission directly through the TDI layer in the usual manner. As with the socket shim, TDI shims are not new and can be implemented in known manner, by intercepting TDI service requests, but with the difference from prior TDI shims that the TDI shim works with the authentication software 20 and authentication server to authenticate communications and generate a session key.

Finally, as shown in Fig. 5, a further layer of authentication and encryption may be added by adding a network driver shim 55, either to the arrangement shown in Fig. 3 without the TDI shim, in combination with the TDI shim shown in Fig. 4, or in combination with the TDI shim of Fig. 4 but not the socket shim, to provide for authentication of communications at the network driver layer. At this layer, the shim 55 intercepts IP packets from applications 56, but instead of referring back to the applications level routine, checks the destination address (which can be in TCP format, UDP format, and so forth), establishes a session key by communications with the authentication server, converts the session key into a format which can be used to encrypt the IP packet, and

Petitioner Apple Inc. - Exhibit 1026, p. 962

sends the IP packet towards the destination, all by carrying out the necessary operations at the network driver level, in a manner similar to that utilized by the above-mentioned SnareNet software program, but with the difference that the authenticating communications link and key generation is carried out by packets addressed to a corresponding layer 56 of the authentication server, which may be further connected to an applications server 57.

It will be noted that since the IP packets are not distinguishable by content, the network driver layer shim could be used as an additional level of security, rather than as an alternative to applications level encryption, with the encrypted files generated by software 20 being further encrypted by shim 55 before transmission to the authentication server or associated gateway.

The overall system utilizing the authentication client software illustrated in Figs. 3-5 is schematically illustrated in Fig. 6. The principal components of the overall system are the client computers containing software of the type illustrated in Figs. 2-5, including client authentication software 20 and shims 50, 53, and/or 55, and applications with communications capabilities (represented by applications 27, 36, 37, and 56 on one client, and application 45 on the other). For purposes of illustration, the client of Figs. 6 is thus depicted as including applications for communicating at the highest

Petitioner Apple Inc. - Exhibit 1026, p. 963

levels, such as the SmartGATE™ proxy application, applications for communicating at the network driver level with corresponding applications connected to the lower layer of the authentication server, and peer-to-peer applications with no capability of communicating with SmartGATE™, but which use sockets or TDI protocols recognized by the shims.

In the case of the SmartGATE™ proxy application, communications are established in the same manner as in the currently available version of the SmartGATE™ authentication client software, and as described in U.S. Patent No. 5,602,918, the communications link being indicated by arrows 60 and 61, with arrow 60 representing the client/server response channel used to authenticate the parties and generate the session key.

In the case of a peer-to-peer application, in which the clients wish to communicate over a direct link 62, the invention provides for the function calls establishing the communications to be intercepted and the initialization procedure routed through channel 61 to the authentication server 23. Server 23 then opens a secured channel 63 to the authentication client software 20 associated with peer application 45 by performing the same mutual authentication procedure performed for the purpose of establishing channel 63, and once the channel is established with its own session key, transmits information using the channel 63

Petitioner Apple Inc. - Exhibit 1026, p. 964

session key which allows the client to recreate the channel 60 session key for use in decrypting communications sent over channel 62. Alternatively, after establishing channel 63, the channel 60 session key could be used to transmit back to the original sending party information necessary to recreate the channel 63 session key. In either case, the authentication server is thus used to establish a fully authenticated "tunnel" between the peer applications without the need to modify any of the sockets, TDI protocols, or hardware drivers on either of the client computers. While the transmitting peer application has no way of directly authenticating the receiving peer, only a receiving peer authenticated by the authentication server will be able to generate the necessary session keys, and thus each of the parties to the communication is effectively authenticated.

For the lower layer application 56, a similar protocol may be employed, in which the attempted communication between lower layer applications is intercepted, and the communications link to the authentication server is used to generate a session key, which is then used to encrypt the packets or datagrams being sent. In this case, the destination must be the lower layer of the authentication server, and thus the communications link is indicated by a separate channel 67.

Petitioner Apple Inc. - Exhibit 1026, p. 965

Finally, the procedures associated with the network illustrated in Fig. 6 are summarized in the flowchart of Fig. 7. For communications directly with the applications level portion of the server 23, steps 100-103 are used, while for peer-to-peer communications, steps 104-109 are used, and for network driver level communications, steps 110-114 are used.

In particular, step 100 by which the applications level authentication program 20 illustrated in Figs. 3-5 receives a call initiation request, either directly from a supported applications program 27 or from a programs 36 and 37 via one of the shims 50 and 53, step 101 is step by which the program 20 addresses the authentication server, step 102 is the step by which the client and server are mutually authenticated and the session keys generated using, for example, the procedure described in U.S. Patent No. 5,602,918, and step 103 is the step by which program 20 encrypts further communications received directly or via shims 50 and 53 from the applications programs 27, 36, and 37.

For peer-to-peer communications, step 105, which is part of step 100, is the step by which the peer address is supplied to program 20, steps 106 and 107 are identical to steps 101 and 102, step 108 is the step by which communications channel 63 shown in Figure 6 is established, step 109 is the step by which the destination computer

Petitioner Apple Inc. - Exhibit 1026, p. 966

authenticated by the server is enabled to decrypt communications received over channel 62, and step 110 is the step by which program 20 encrypts the communications. It will of course be appreciated that these steps represent only a summary of the steps involved in carrying out the present invention, and that further steps will be apparent to those skilled in the art based on the above description of the apparatus and software portions of the preferred embodiment of the invention.

Having thus described various preferred embodiments of the invention, those skilled in the art will appreciate that variations and modifications of the preferred embodiment may be made without departing from the scope of the invention. It is accordingly intended that the invention not be limited by the above description or accompanying drawings, but that it be defined solely in accordance with the appended claims.

Petitioner Apple Inc. - Exhibit 1026, p. 967

I claim:

1. Apparatus for carrying out communications over a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network, comprising:

means for intercepting function calls and requests for service sent by an applications program on one of said client computers to a lower level set of communications drivers; and

means for causing an applications level authentication and encryption program in said one of said client computers to communicate with the server, generate said session key, and encrypt files sent by the applications program before transmittal over said open network.

2. Apparatus as claimed in claim 1, further comprising means for intercepting files packaged by a transport driver interface layer to form packets and encrypting the packets using a session key generated during communications with a lower layer of the server.

3. A method as claimed in claim 1, further comprising

means for intercepting a destination address during initialization of communications between said one of said

Petitioner Apple Inc. - Exhibit 1026, p. 968

client computers and a second of said client computers on said virtual private network;

means for causing said applications level authentication and encryption program to communicate with the server to carry out functions a.) and b.);

means for transmitting said destination address to said server;

means for causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

means for enabling said second of said two client computers to recreate the session key;

means for causing said authentication software to encrypt files to be sent to the destination address using the session key; and

means for transmitting the encrypted files directly to the destination address.

4. Apparatus as claimed in claim 3, wherein said means for intercepting the destination address is carried out by a shim positioned between a peer-to-peer applications program and a layer of a communications driver architecture of said one of the two client computers.

5. A multi-tier virtual private network, comprising:

a server and a plurality of client computers, the server and client computers each including means for

Petitioner Apple Inc. - Exhibit 1026, p. 969

transmitting data to and receiving data from an open network,

wherein said means for transmitting data to and receiving data from the open network includes, in any client computer initiating communications with the server:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files;

at least one lower level set of communications drivers;

and a shim arranged to intercept function calls and requests for service sent by an applications program to the lower level set of communications drivers in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before transmittal over said open network.

6. A multi-tier virtual private network as claimed in claim 5, wherein said lower level set of communications drivers includes a network driver layer, a transport driver

Petitioner Apple Inc. - Exhibit 1026, p. 970

interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and an applications socket for facilitating service requests by said applications program to the transport driver interface layer, and wherein said shim is a socket shim positioned between the applications program and the socket to intercept function calls to the socket in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

7. A multi-tier virtual private network as claimed in claim 6, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said function calls to the socket, is diverted by the socket shim and wherein a destination address including said intercepted function calls is supplied to the server during communications with the server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

Petitioner Apple Inc. - Exhibit 1026, p. 971

8. A multi-tier virtual private network as claimed in claim 6, further including a transport driver interface shim positioned between the transport driver interface layer and a second applications program, for intercepting requests from the second applications program for service by the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

9. A multi-tier virtual private network as claimed in claim 8, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

10. A multi-tier virtual private network as claimed in claim 5, wherein said lower level set of communications drivers includes a network driver layer, and a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and wherein said shim is a transport driver interface layer shim positioned

Petitioner Apple Inc. - Exhibit 1026, p. 972

between the applications program and the transport driver interface layer to intercept service requests by the applications program to the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

11. A multi-tier virtual private network as claimed in claim 10, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said intercepted requests for service, is diverted by the transport driver interface layer shim and supplied to the server during communications with the server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

12. A multi-tier virtual private network as claimed in claim 10, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and

Petitioner Apple Inc. - Exhibit 1026, p. 973

encrypt the files using a session key generated during communications with a lower layer of the server.

13. A multi-tier virtual private network, comprising:

a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said means for transmitting data to and receiving data from the open network includes, in any client computer initiating communications with the server:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

at least one lower level set of communications drivers,

wherein said lower level set of communications drivers includes a network driver layer, a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and a

Petitioner Apple Inc. - Exhibit 1026, p. 974

network driver layer shim positioned between the transport driver interface layer and the network driver layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

14. A multi-tier virtual private network, comprising:

a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said means for transmitting data to and receiving data from the open network includes, in any client computer initiating communications with the server:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

further comprising means for securing peer-to-peer communications between applications on two of said client computers, said peer-to-peer communications securing means comprising:

Petitioner Apple Inc. - Exhibit 1026, p. 975

means for intercepting a destination address during initialization of communications by a first of said two client computers;

means for causing said authentication software to communicate with the server to carry out functions a.) and b.);

means for transmitting said destination address to said server;

means for causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

means for enabling said second of said two client computers to recreate the session key;

means for causing said authentication software to encrypt files to be sent to the destination address using the session key;

means for transmitting the encrypted files directly to the destination address.

15. A multi-tier virtual private network as claimed in claim 14, wherein said means for intercepting the destination address comprises a shim positioned between the peer-to-peer applications program and a layer of a communications driver architecture of said first of the two client computers.

16. A multi-tier virtual private network as claimed in claim 5, wherein said shim is positioned above a socket,

Petitioner Apple Inc. - Exhibit 1026, p. 976

the socket being positioned above a transport driver layer of said communications driver architecture.

17. A multi-tier virtual private network as claimed in claim 5, wherein said shim is positioned above a transport driver layer of said communications driver architecture.

18. Computer software for installation on a client computer of a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said computer software includes:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files;

and a shim arranged to intercept function calls and requests for service sent by an applications program to a lower level set of communications drivers in order to cause the applications level authentication and encryption program to communicate with the server, generate

Petitioner Apple Inc. - Exhibit 1026, p. 977

said session key, and encrypt files sent by the applications program before transmittal over said open network.

19. Computer software as claimed in claim 18, wherein said lower level set of communications drivers includes a network driver layer, a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and an applications socket for facilitating service requests by said applications program to the transport driver interface layer, and wherein said shim is a socket shim positioned between the applications program and the socket to intercept function calls to the socket in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

20. Computer software as claimed in claim 19, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said function calls to the socket, is diverted by the socket shim and wherein a destination address including said intercepted function calls is supplied to the server during communications with the

Petitioner Apple Inc. - Exhibit 1026, p. 978

server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

21. Computer software as claimed in claim 19, further including a transport driver interface shim positioned between the transport driver interface layer and a second applications program, for intercepting requests from the second applications program for service by the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

22. Computer software as claimed in claim 21, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

23. Computer software as claimed in claim 18, wherein said lower level set of communications drivers includes a

Petitioner Apple Inc. - Exhibit 1026, p. 979

network driver layer, and a transport driver interface layer arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and wherein said shim is a transport driver interface layer shim positioned between the applications program and the transport driver interface layer to intercept service requests by the applications program to the transport driver interface layer in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files sent by the applications program before the files are packaged by the transport driver interface layer.

24. Computer software as claimed in claim 23, wherein said applications program is a peer-to-peer communications program, and wherein a peer application destination address, included in said intercepted requests for service, is diverted by the transport driver interface layer shim and supplied to the server during communications with the server, causing the service to establish a communications link with a peer application, mutually authenticate the peer application, and enable the peer application to reconstruct the session key in order to receive encrypted files sent by the peer-to-peer communications program over the open network.

Petitioner Apple Inc. - Exhibit 1026, p. 980

25. Computer software as claimed in claim 23, further comprising a network driver layer shim positioned between the network driver layer and the transport driver interface layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

26. Computer software for installation on a client computer of a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said computer software includes:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

at least one lower level set of communications drivers,

wherein said lower level set of communications drivers includes a network driver layer, a transport driver interface layer

Petitioner Apple Inc. - Exhibit 1026, p. 981

arranged to package applications files as packets capable of being routed over the open network and supply the packets to the network driver layer for transmission to the open network, and a network driver layer shim positioned between the transport driver interface layer and the network driver layer and arranged to intercept files packaged by the transport driver interface layer and encrypt the files using a session key generated during communications with a lower layer of the server.

27. Computer software for installation on a client computer of a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network,

wherein said computer software includes:

applications level encryption and authentication software arranged to communicate with the server in order to: a.) mutually authenticate the server and the client computer initiating communications with the server and b.) generate a session key for use by the client computer initiating communications to encrypt files; and

further comprising means for securing peer-to-peer communications between applications on two of said client

Petitioner Apple Inc. - Exhibit 1026, p. 982

computers, said peer-to-peer communications securing means comprising:

means for intercepting a destination address during initialization of communications by a first of said two client computers;

means for causing said authentication software to communicate with the server to carry out functions a.) and b.);

means for transmitting said destination address to said server;

means for causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

means for enabling said second of said two client computers to recreate the session key;

means for causing said authentication software to encrypt files to be sent to the destination address using the session key;

means for transmitting the encrypted files directly to the destination address.

28. Computer software as claimed in claim 27, wherein said means for intercepting the destination address comprises a shim positioned between the peer-to-peer applications program and a layer of a communications driver architecture of said first of the two client computers.

Petitioner Apple Inc. - Exhibit 1026, p. 983

29. Computer software as claimed in claim 27, wherein said shim is positioned above a socket, the socket being positioned above a transport driver layer of said communications driver architecture.

30. Computer software as claimed in claim 27, wherein said shim is positioned above a transport driver layer of said communications driver architecture.

31. A method of carrying out communications over a multi-tier virtual private network, said network including a server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network, comprising the steps of:

intercepting function calls and requests for service sent by an applications program in one of said client computers to a lower level set of communications drivers;

causing an applications level authentication and encryption program said one of said client computers to communicate with the server, generate said session key, and encrypt files sent by the applications program before transmittal over said open network.

32. A method as claimed in claim 31, further comprising the step of intercepting files packaged by a transport driver interface layer to form packets and encrypting the

Petitioner Apple Inc. - Exhibit 1026, p. 984

packets using a session key generated during communications with a lower layer of the server.

33. A method as claimed in claim 31, further comprising the step of intercepting a destination address during initialization of communications between said one of said client computers and a second of said client computers on said virtual private network;

causing said applications level authentication and encryption program to communicate with the server to carry out functions a.) and b.);

transmitting said destination address to said server;

causing said server to carry-out functions a.) and b.) with respect to the second of said two client computers;

enabling said second of said two client computers to recreate the session key;

causing said authentication software to encrypt files to be sent to the destination address using the session key; and

transmitting the encrypted files directly to the destination address.

34. A method as claimed in claim 33, wherein said step of intercepting the destination address is carried out by a shim positioned between a peer-to-peer applications program

Petitioner Apple Inc. - Exhibit 1026, p. 985

and a layer of a communications driver architecture of said one of the two client computers.

Petitioner Apple Inc. - Exhibit 1026, p. 986

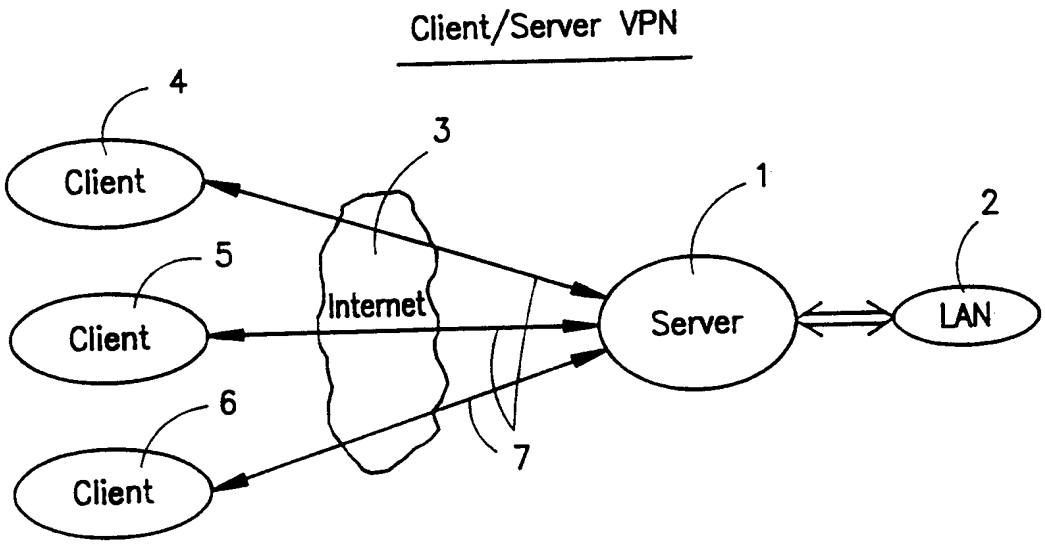


FIG. 1A
(PRIOR ART)

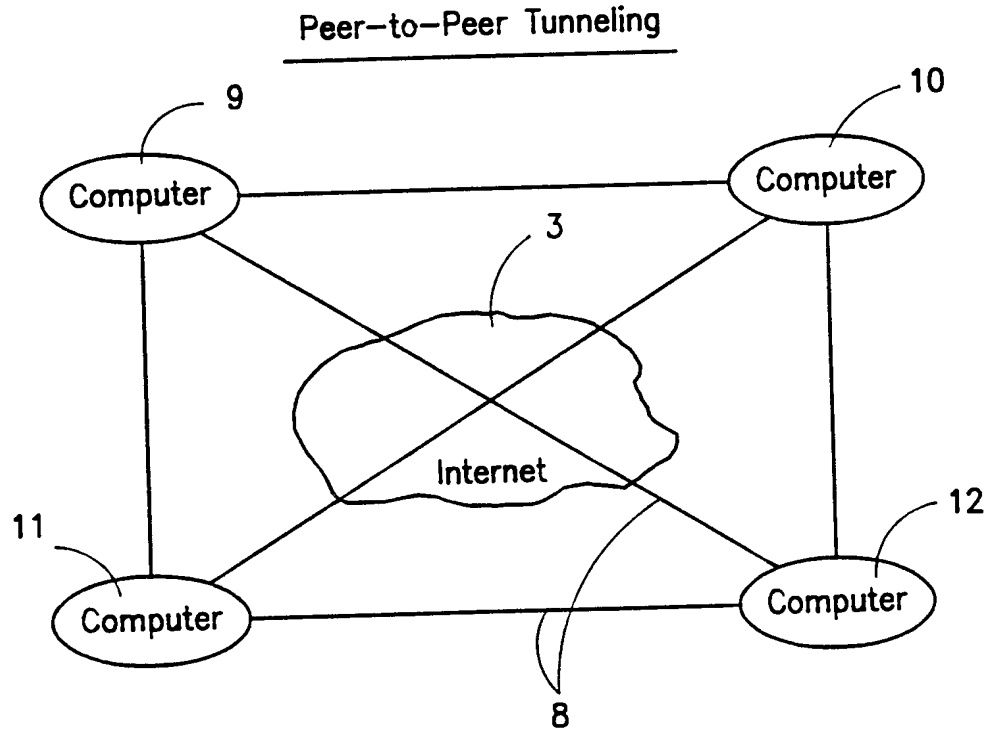


FIG. 1B
(PRIOR ART)

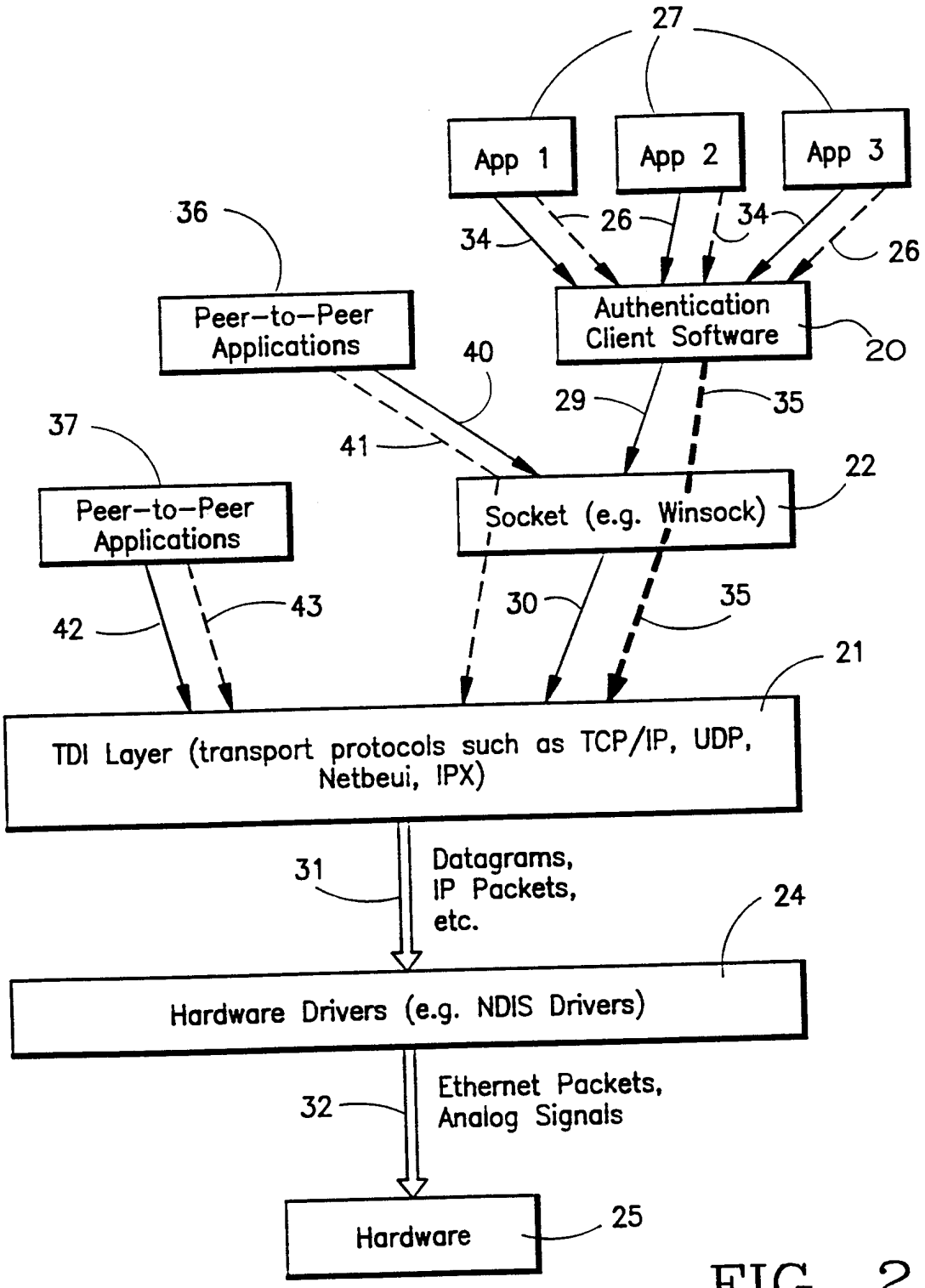


FIG. 2
(PRIOR ART)

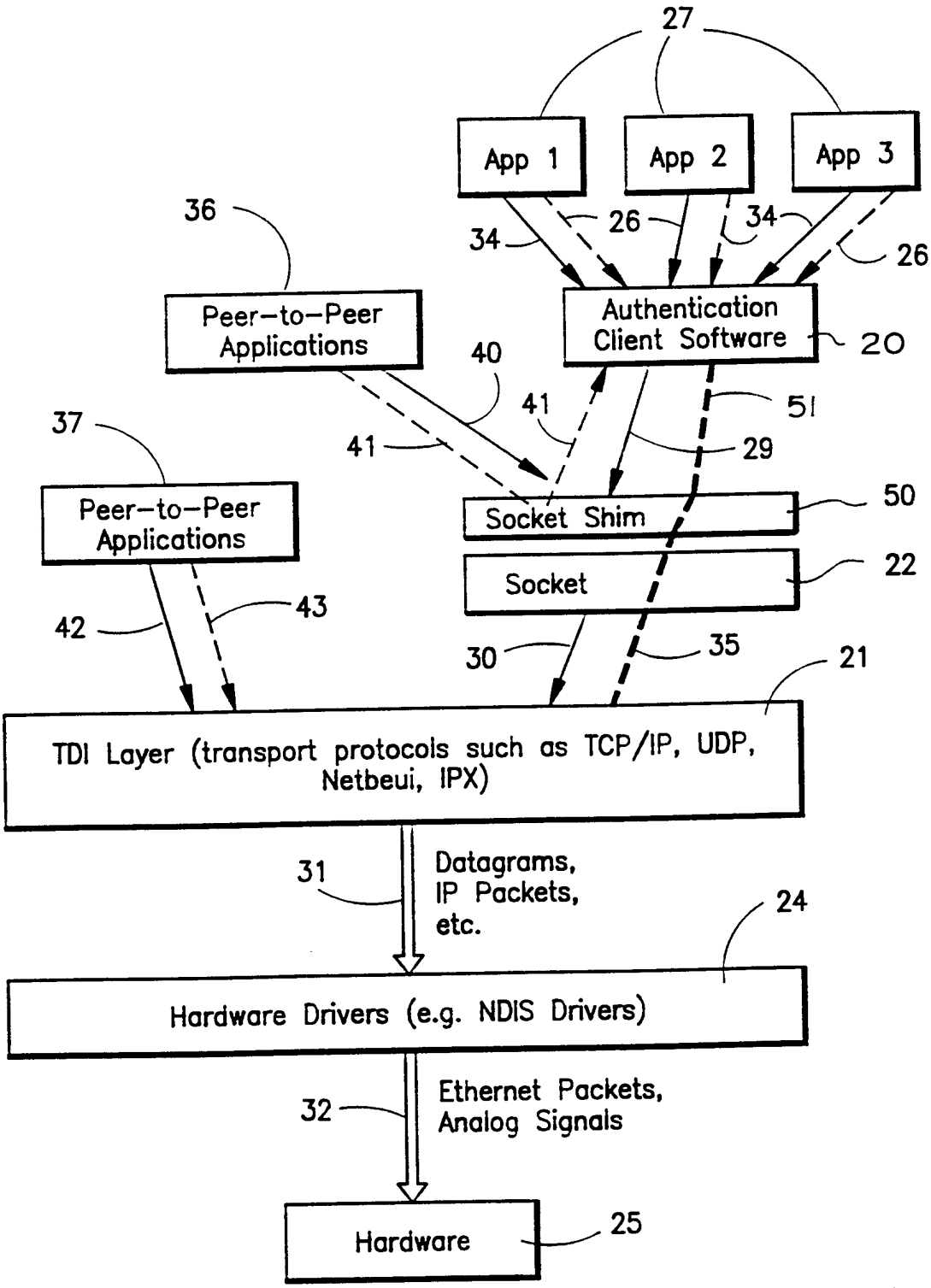

27
App 1
App 2
App 3
36
34
26
34
26
Peer–to–Peer Applications
Authentication Client Software
20
40
41
51
37
41
29
Peer–to–Peer Applications
Socket Shim
50
Socket
22
42
43
30
35
21
TDI Layer (transport protocols such as TCP/IP, UDP, Netbeui, IPX)
31
Datagrams, IP Packets, etc.
24
Hardware Drivers (e.g. NDIS Drivers)
32
Ethernet Packets, Analog Signals
Hardware
25

FIG. 3

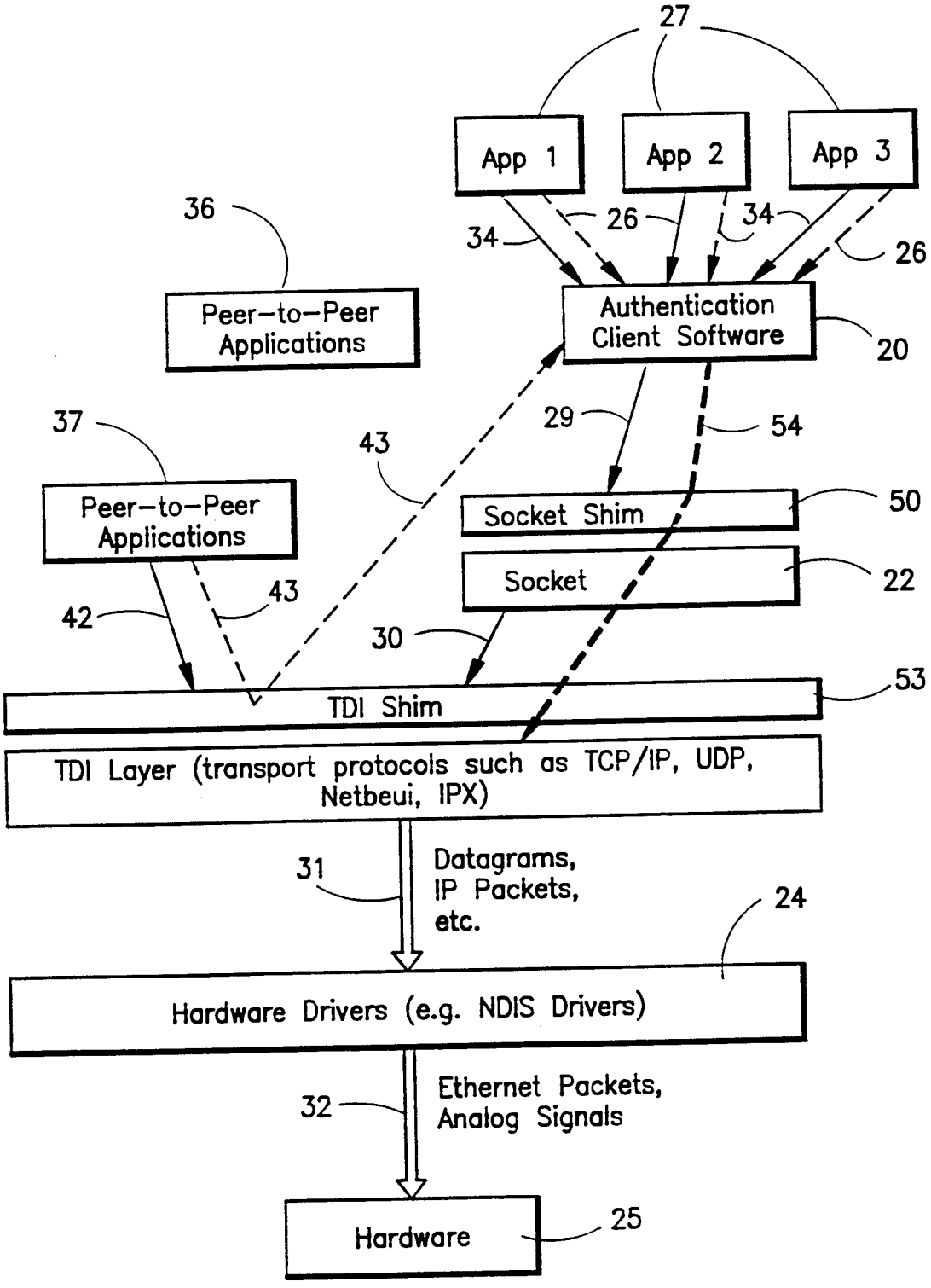

27
App 1
App 2
App 3
36
34
26
34
26
Peer-to-Peer Applications
Authentication Client Software
20
37
29
54
43
Peer-to-Peer Applications
Socket Shim
50
Socket
22
43
42
30
53
TDI Shim
TDI Layer (transport protocols such as TCP/IP, UDP, Netbeui, IPX)
31
Datagrams, IP Packets, etc.
24
Hardware Drivers (e.g. NDIS Drivers)
32
Ethernet Packets, Analog Signals
Hardware
25

FIG. 4

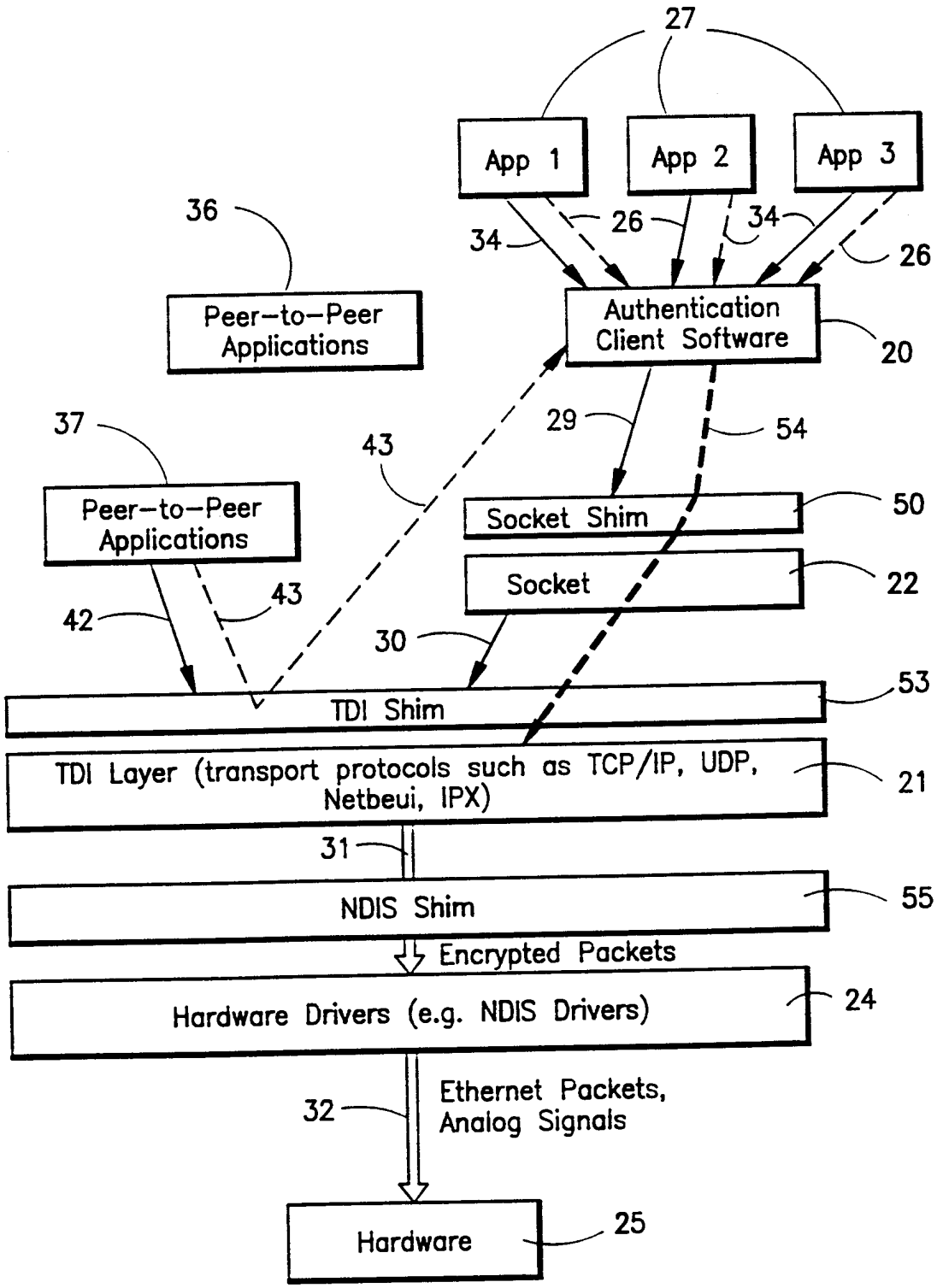

27
App 1
App 2
App 3
36
34
26
34
26
Peer–to–Peer Applications
Authentication Client Software
20
37
29
54
43
Peer–to–Peer Applications
Socket Shim
50
Socket
22
43
42
30
TDI Shim
53
TDI Layer (transport protocols such as TCP/IP, UDP, Netbeui, IPX)
21
31
NDIS Shim
55
Encrypted Packets
Hardware Drivers (e.g. NDIS Drivers)
24
32
Ethernet Packets, Analog Signals
Hardware
25

FIG. 5

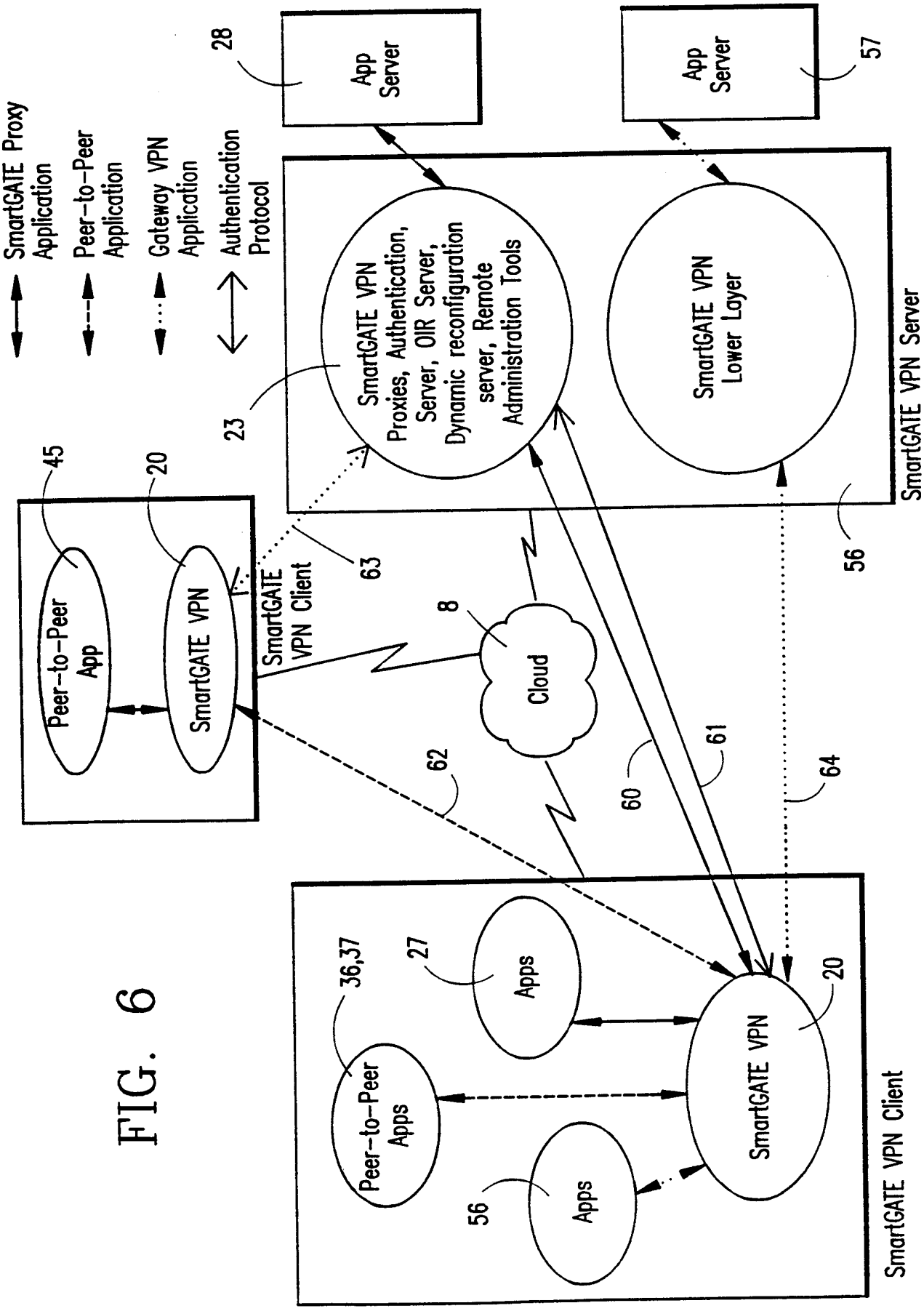

SmartGATE Proxy Application
Peer-to-Peer Application
Gateway VPN Application
Authentication Protocol
28
App Server
App Server
57
SmartGATE VPN Proxies, Authentication, Server, OIR Server, Dynamic reconfiguration server, Remote Administration Tools
SmartGATE VPN Lower Layer
SmartGATE VPN Server
23
56
45
20
Peer-to-Peer App
SmartGATE VPN
SmartGATE VPN Client
63
8
Cloud
62
60
61
64
36,37
27
Apps
Peer-to-Peer Apps
SmartGATE VPN
20
56
Apps
SmartGATE VPN Client

FIG. 6

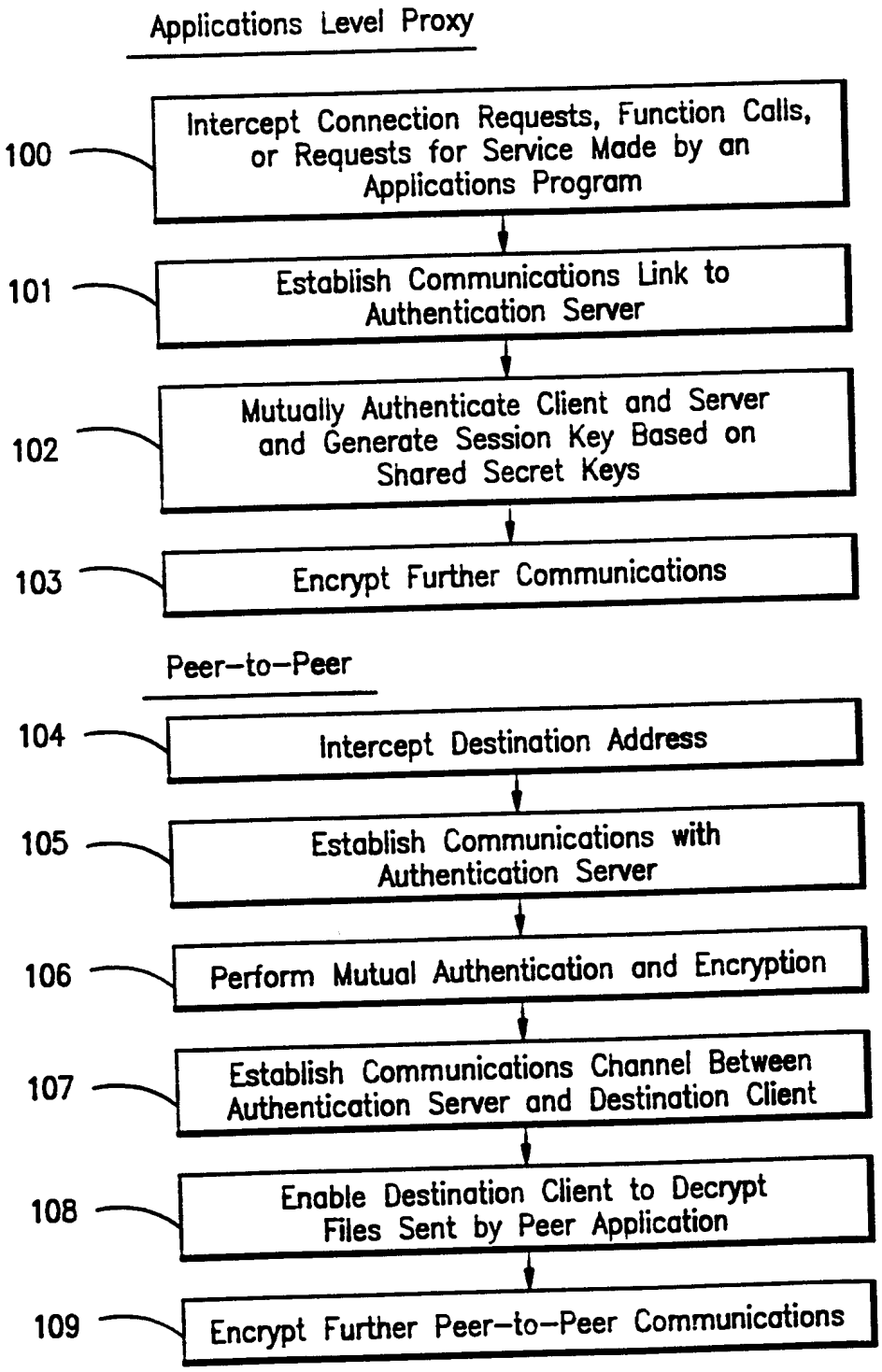

Applications Level Proxy
100
Intercept Connection Requests, Function Calls, or Requests for Service Made by an Applications Program
101
Establish Communications Link to Authentication Server
102
Mutually Authenticate Client and Server and Generate Session Key Based on Shared Secret Keys
103
Encrypt Further Communications
Peer-to-Peer
104
Intercept Destination Address
105
Establish Communications with Authentication Server
106
Perform Mutual Authentication and Encryption
107
Establish Communications Channel Between Authentication Server and Destination Client
108
Enable Destination Client to Decrypt Files Sent by Peer Application
109
Encrypt Further Peer-to-Peer Communications

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/17198

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :395/187.01

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/187.01, 186, 188.01, 200.17, 200.12; 380/49, 21, 25, 4

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, STN, IEEE ProQuest
search terms: virtual private network, shims, DLLs, protocol layers, Winsock, sockets, encryption, authentication.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,657,390 A (ELGAMAL ET AL) 12 AUGUST 1997, FIGURES 1-8, COL. 3, LINES 20-55, COL. 5, LINE 15 TO COL. 8, LINE 32, COL. 11, LINE 1 TO COL. 16, LINE 49.	1,5,6,16,17,18,19,23,31
A	US 5,602,918 A (CHEN ET AL) 11 FEBRUARY 1997, SEE ENTIRE PATENT.	1-34
A	US 5,550,984 A (GELB) 27 AUGUST 1996, ABSTRACT, COL. 3, LINE 52 TO COL. 4, LINE 45, COL.6, LINES 27-55.	1-34
Y	HURWICZ, A VIRTUAL PRIVATE AFFAIR, BYTE MAGAZINE, JULY 1997, PAGES 79-87.	1,5,6,16,17,18,19,23,31

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
22 OCTOBER 1998

Date of mailing of the international search report
12 NOV 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
JOSEPH PALYS
Telephone No. (703) 305-9600

Form PCT/ISA/210 (second sheet)(July 1992)*

(12) UK Patent Application (19) GB (11) 2 334 181 (13) A

(43) Date of A Publication 11.08.1999

(21) Application No 9802545.5

(22) Date of Filing 06.02.1998

(51) INT CL[6]
H04Q 7/32

(52) UK CL (Edition Q)
H4L LDSC

(56) Documents Cited
US 5613204 A US 5109403 A

(58) Field of Search
UK CL (Edition P) H4L LDSC LDSU LECC LECX
INT CL[6] H04Q 7/32 7/38
Online: WPI

(71) Applicant(s)
NEC Technologies (UK) Ltd
(Incorporated in the United Kingdom)
Castle Farm Campus, Priorslee, TELFORD, Shropshire,
TF2 9SA, United Kingdom

(72) Inventor(s)
Charles Marie Herve Noblet

(74) Agent and/or Address for Service
J W White
NEC Technologies (UK) Ltd, Level 3, The Imperium,
Imperial Way, READING, Berks, RG2 0TD,
United Kingdom

(54) Abstract Title
Over-the-air re-programming of radio transceivers

(57) A method of downloading reprogramming data from a network for installation in a mobile station makes use of a dedicated small bandwidth pilot channel. The mobile station obtains from the base station the radio access parameters of a second channel. The second channel is a large bandwidth (bootstrap) channel suitable for fast transfer of data. The bootstrap channel is logically mapped onto a local transmission mode such as DECT or GSM by the mobile station and re-programming data may be downloaded from the base station via the bootstrap channel.

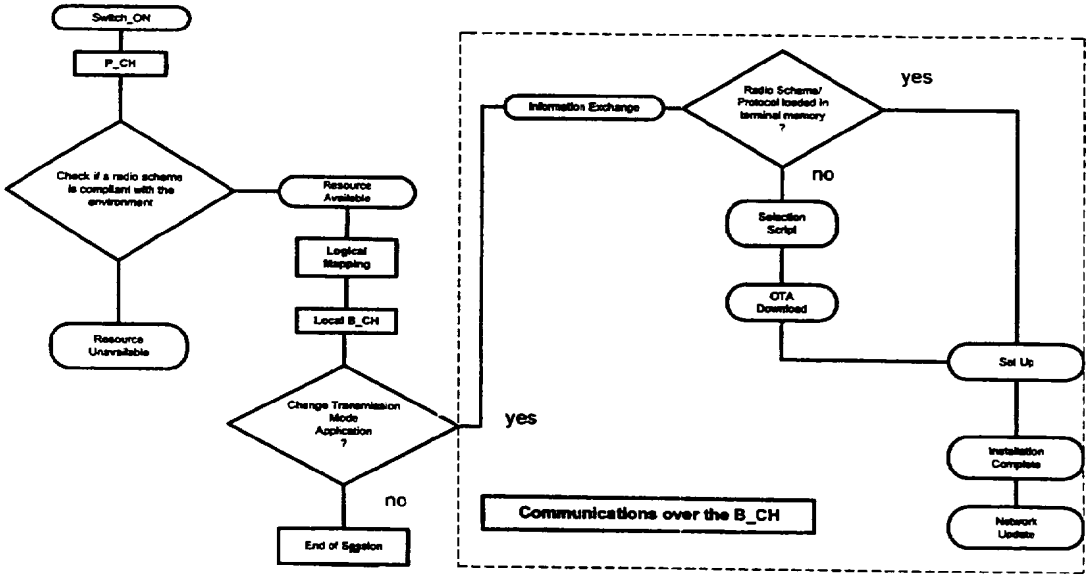


Figure 2

GB 2 334 181 A

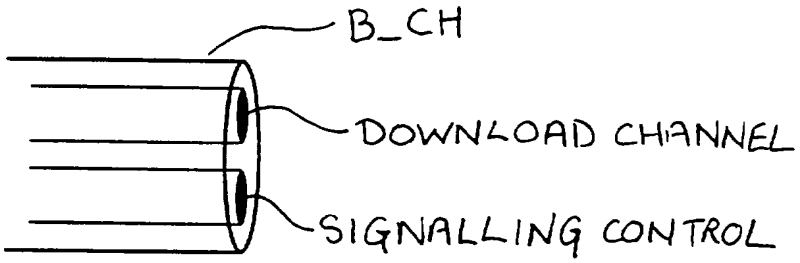


Figure: 1

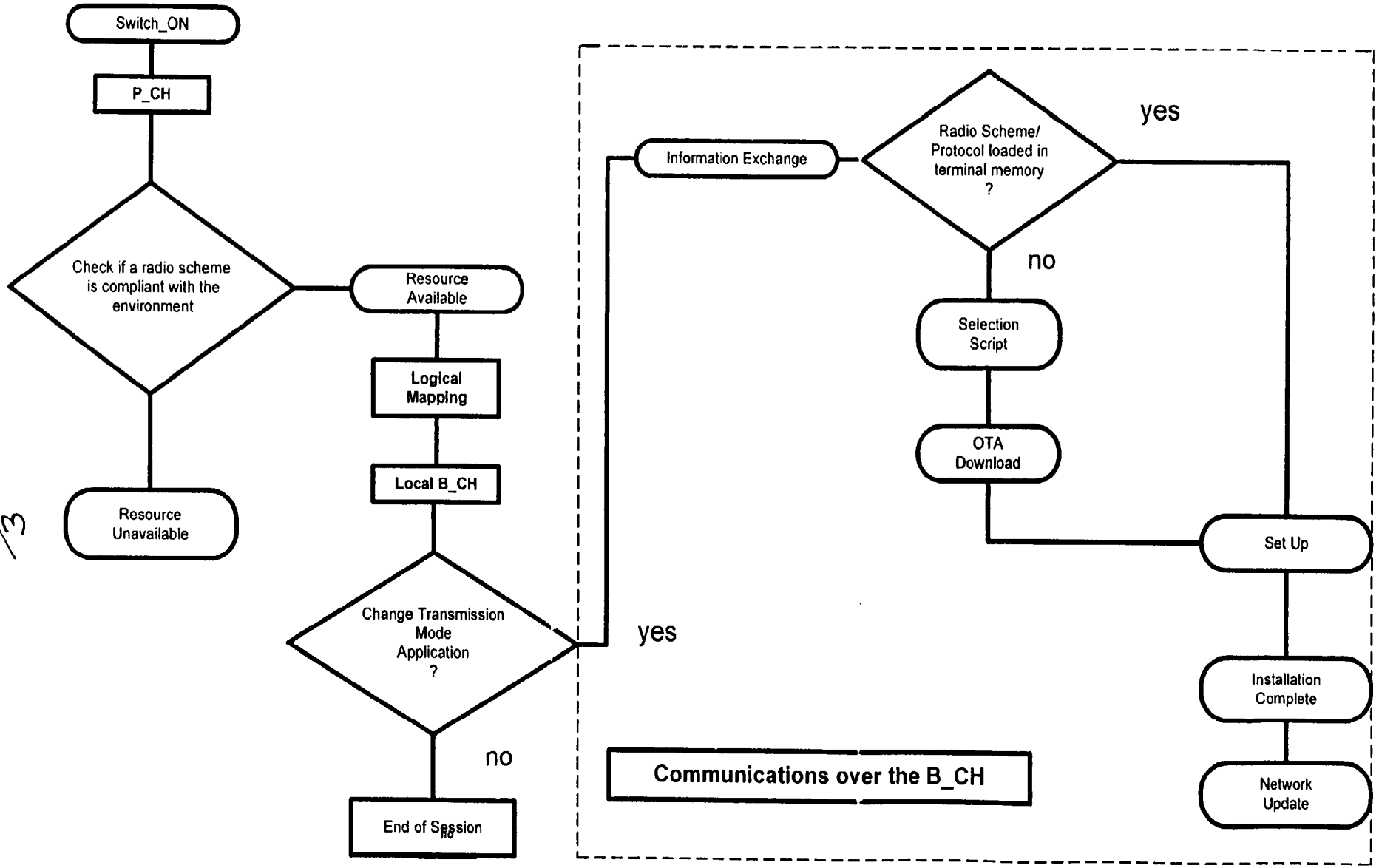


Figure 2

Petitioner Apple Inc. - Exhibit 1026, p. 997

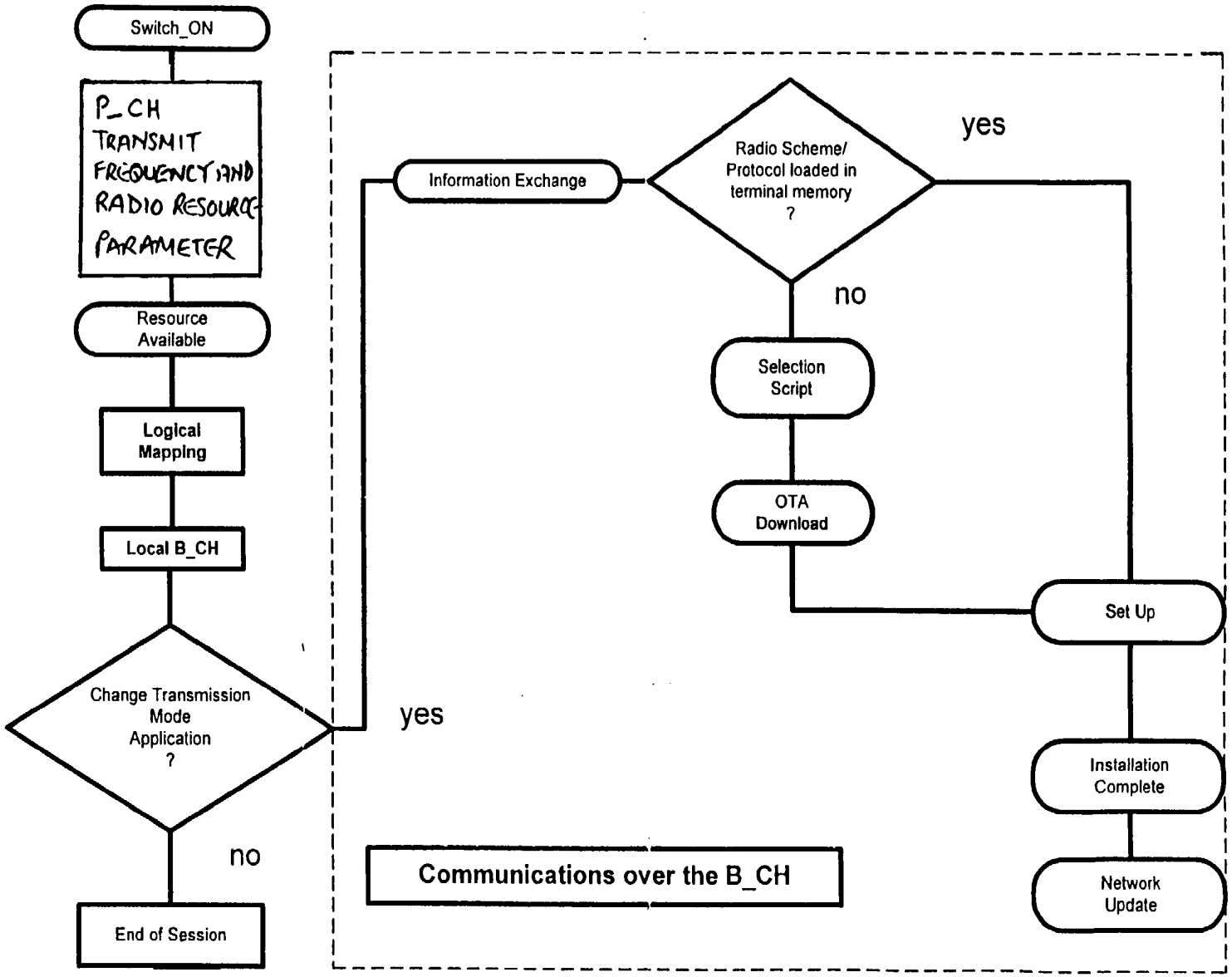


Figure 3

Petitioner Apple Inc. - Exhibit 1026, p. 998

Over-the-air re-programming of radio transceivers

This invention relates to radio transmitter/receivers and in particular it relates to a method of re-programming radio transmitter/receivers over-the-air.

A radio transmitter/receiver (transceiver) such as a radiotelephone is designed for operation with particular types of networks such as GSM 900 or DCS 1800. Intended use of the radiotelephone with a particular network(s) in a restricted geographical area, however, requires that the telephone be configured so as properly to communicate with the particular network (s). The user of a radiotelephone will usually have a telephone which has been configured for communication with a so called "home network". The home network is the local network usually most used by the subscriber.

The area within which a user of e.g. a GSM radiotelephone may operate, however, is considerable and is not limited to the home network but may be used on many other networks throughout the world. Use of a handset outside the home network is known as "roaming".

When the radiotelephone is to be used in roaming it is often necessary for it to have a configuration different to that for use with the home network. It is possible for re-configuration of radio transmitter/receivers to be effected by means of signals received across the air interface.

It is also convenient for the radio to be re-configurable over the air interface so as to support different types of communication and user applications e.g. addition of address book manager, whether or not it is located in the home network.

Over the air re-programming of radio receivers is well known in the art and reference may be made to US patent 5 381 138 for example. The capability to obtain programming data from a network is particularly useful for a roaming radio transmitter/receiver.

When beginning operation in an area for which the radiotelephone is not configured and it is required to download the data for reconfiguration from one of the available networks, a communication link must first be established with the network of interest. It has been proposed that a pilot channel be established in all areas from which the roaming radiotelephone may obtain the data necessary for reconfiguration.

A pilot channel of this type, however, will require a relatively large bandwidth to allow a sufficiently fast transfer of the data required.

According to the invention there is provided a method of downloading reprogramming data from a network for installation in a radio transmitter/receiver comprising initial communication from a first dedicated channel of relatively small bandwidth broadcasting at least the frequency and radio access parameters of a second channel of relatively large bandwidth from which reprogramming data may be downloaded.

Examples of the invention will now be described in more detail with reference to the accompanying figures in which

figure 1 Illustrates the logical structure of the bootstrap channel

Figure 2 Is a flow diagram of a reconfiguration process

figure 3 Is a flow diagram of an alternative reconfiguration process

A roaming radio transmitter/receiver (mobile) is located in a region served by one or more networks and the user wishes to communicate with a network from which he can obtain reprogramming data and subsequently begin communicating with the network in the communication mode selected.

A pilot channel broadcast is maintained in the region and contained in the pilot channel broadcast there is at least sufficient information for the mobile to connect to a second channel which we shall call the bootstrap channel. Conveniently the pilot channel will be broadcast in all regions over a standardised radio interface. Only a small bandwidth is required for the pilot channel because of the small amount of information contained in the broadcast.

The small bandwidth requirement makes the task of standardisation much easier with respect to the pilot channel. The wider bandwidth channels are more conveniently assigned locally for ease of implementation.

The Pilot Channel (P_CH) broadcasts a list of sets of parameters corresponding to networks available in the region. The mobile receives the network transmission through the P_CH. If the existing configuration of the mobile is matched to the available regional radio schemes, then a second channel the bootstrap channel (B_CH) is logically mapped onto the selected transmission mode. The base station and mobile exchange information over this dedicated logical channel.

The Bootstrap channel is logically mapped on top of one of the default modes of the terminal; a mapping of a logical B_CH onto the physical GSM channel for instance may be implemented. Once the mapping has been effected the terminal may download data from the base station. The bootstrap channels provided by each operator may accommodate differing services with regard to the applications available for downloading.

The flow diagram shown at fig 3 depicts a reconfiguration procedure.

When the mobile is switched on, it reads the Pilot Channel broadcast. The mobile must be configured to support the (standardised) radio interface of the Pilot Channel. The Pilot Channel carries local radio parameters (standards supported in the regional environment in which the mobile is located). After processing the received information, the mobile

communicates with the base station through the Bootstrap Channel, provided that the mobile has the minimum resources required by its local radio environment. Prior to the change of channel, P_CH to B_CH, a logical mapping of the Bootstrap Channel is performed within the mobile on the selected air interface.

When operation on a local B_CH transmission has been established, the user may wish to change some properties or the performance of his mobile and can request supply of the desired services from the network. If no changes are required then the mobile adopts the default transmission mode in stand-by and releases the allocated B_CH.

If the user requests a change then communication between the base station and mobile is maintained for the exchange, the nature of which will depend on the capabilities of both mobile and network. At least 3 conditions can affect the nature of this information exchange.

Firstly, the mobile may not be able to support the required software. Where the mobile is not able to support the required software, no communication channel is available to the mobile from the existing network resources and use of the mobile within the region will therefore not be possible.

Secondly, the required software may be stored already in the mobile's memory. In this situation there is no need to download a software module but the allocated B_CH connection is maintained for further operations as described.

Thirdly, the software module required to support a different type of communication or user application may need to be downloaded from the base station. Where the download of a software module is required, initially a selection script is downloaded to the mobile followed by downloading and installation of the required software.

When the installation of the required software into the mobile has been completed, the mobile signals to the network the achievement of correct reconfiguration. On receipt of the "correct reconfiguration" signal from the mobile details of the mobile identity and its present configuration are entered on the network database (to license the product for instance) .

With reference to figure 1, the logical structure of the bootstrap channel will include 2 logical sub-channels : a download channel and a signalling control channel (S_CH). The signalling control channel assists in the reduction of errors in transmission so as to allow correct software download.

In the above example, the first channel, the Pilot Channel, is standardised and the mobile must be configured to support the radio interface for the Pilot Channel. The second (bootstrap) channel may be subject to local definition through logical mapping on a local transmission mode e.g. GSM, DECT and the mobile is not initially configured to support the radio interface for the bootstrap channel..

An example of a method of reprogramming providing greater flexibility will now be given. In this example the mobile is configured to support the radio interfaces for both the first, dedicated relatively small bandwidth (Pilot) channel and the second relatively large bandwidth (bootstrap) channel. That is to say that when the mobile is switched on in most and preferably all regions, the network can communicate with the mobile via both pilot and bootstrap channels.

In order for the mobile always to have the appropriate radio interface for the bootstrap channel then this channel would need also to be standardised (in addition to the Pilot Channel). The parameters of the bootstrap channels provided in different regions may have local variations in terms of e.g. allocated frequency, data rate and available user applications.

With reference to figure 3 which is a flow diagram of the reconfiguration process for this example, the mobile when switched on reads the Pilot Channel broadcast. The allocated frequency and radio resource parameters for the bootstrap channel contained in the pilot channel broadcast are processed and any required logical mapping effected. After processing the received information, the mobile communicates with the base station through the Bootstrap Channel.

The condition likely to be experienced in the previous example whereby the mobile is not able to support the required software and no communication channel is available to the mobile from the existing network resources does not apply in this arrangement. The communication via the bootstrap

channel allows the request for and supply of the software module necessary to establish communication with the network. The transfer to the bootstrap channel does not depend on the existing configuration of the mobile since the bootstrap channel is standardised in this example and the mobile is equipped to interface, via the pilot channel, with the bootstrap channel.

The services and structure offered by the Bootstrap Channel are common for both of the above examples, however, the requirements on the terminals and networks differ.

The bootstrap channel will provide the following services by means of over -the-air (OTA) reconfiguration :
capability Exchange - the terminal provides some information to the network on its current configuration and capabilities.
module Selection : at this stage the user specifies the software that his terminal requires to download. This operation could be compared to an installation script.
data download : transfer of the data. In some cases software code will have to be downloaded whilst in other cases the software may already be implemented in the mobile. In the latter case, a set-up mechanism would be sufficient to initiate the reconfiguration.

Once the mobile and the base station are synchronised on the bootstrap channel, information exchange can begin.

Claims

1. A method of downloading reprogramming data from a network for installation in a radio transmitter/receiver comprising initial communication from a first dedicated channel of relatively small bandwidth broadcasting at least the frequency and radio access parameters of a second channel of relatively large bandwidth from which reprogramming data may be downloaded.

2. A method of downloading reprogramming data from a network as in claim 1 where first, dedicated relatively small bandwidth channel has a standard radio interface common to many network locations.

3. A method of downloading reprogramming data from a network as in claim 2 where second relatively large bandwidth channel has a standard radio interface common to many network locations.

4. A method of downloading reprogramming data from a network as in claims 1 to 3 where first, dedicated relatively small bandwidth channel broadcasts a list of sets of parameters corresponding to networks available in the region.

5. A method of downloading reprogramming data from a network as in claim 1 where the radio transmitter/receiver is configured to support the radio interfaces for both the first, dedicated relatively small bandwidth channel and the second relatively large bandwidth channel.

The Patent Office

10

Application No: GB 9802545.5 **Examiner:** Glyn Hughes
Claims searched: 1 to 5 **Date of search:** 17 August 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): H4L (LDSC, LDSU, LECC, LECX)

Int Cl (Ed.6): H04Q 7/32, 7/38

Other: Online: WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	US 5613204	(HABERMAN ET AL) see in particular column 15 lines 48 to 50	1
X	US 5109403	(SUTPHIN) see abstract	1

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Petitioner Apple Inc. - Exhibit 1026, p. 1008

(12) UK Patent Application (19) GB (11) 2 340 702 (13) A

(43) Date of A Publication 23.02.2000

(21) Application No 9912200.4

(22) Date of Filing 25.05.1999

(30) Priority Data
(31) 09087823 (32) 29.05.1998 (33) US

(51) INT CL[7]
H04L 29/06 // H04L 9/00 12/22 12/46

(52) UK CL (Edition R)
H4P PPEB

(56) Documents Cited
EP 0887979 A2 EP 0825748 A2 WO 98/31124 A1

(58) Field of Search
UK CL (Edition Q) H4P PPA PPEB PPEC PPG
INT CL[6] H04L 12/22 12/46 12/66 29/06
ONLINE DATABASES: WPI, EPODOC, JAPIO

(71) Applicant(s)
Sun Microsystems Inc
(Incorporated in USA - Delaware)
901 San Antonio Road, MS Palo Alto-521,
California 94303, United States of America

(72) Inventor(s)
Joseph E Provino

(74) Agent and/or Address for Service
D Young & Co
21 New Fetter Lane, LONDON, EC4A 1DA,
United Kingdom

(54) Abstract Title
Accessing a server in a virtual private network protected by a firewall

(57) A virtual private network 15 has a firewall 30, at least one server 31 and a nameserver 32 each having a network address (eg. an n-bit integer address). The server 31 also has a secondary address (eg. a human readable address) and the nameserver 32 provides an association between the secondary address and the network address. An authorised external device 12 establishes a secure tunnel between itself and the firewall for communication using encryption. When the external device requests connection to server 31 using the secondary address of server 31, the firewall provides external device 12 with the network address of the nameserver 32. The external device 12 transmits a request for resolution of the network address associated with the secondary address to the nameserver through the firewall. The nameserver then transmits the network address of the server 31 through the firewall to the external device using the secure tunnel. The external device can thereafter use the network address of server 31 in subsequent communications.

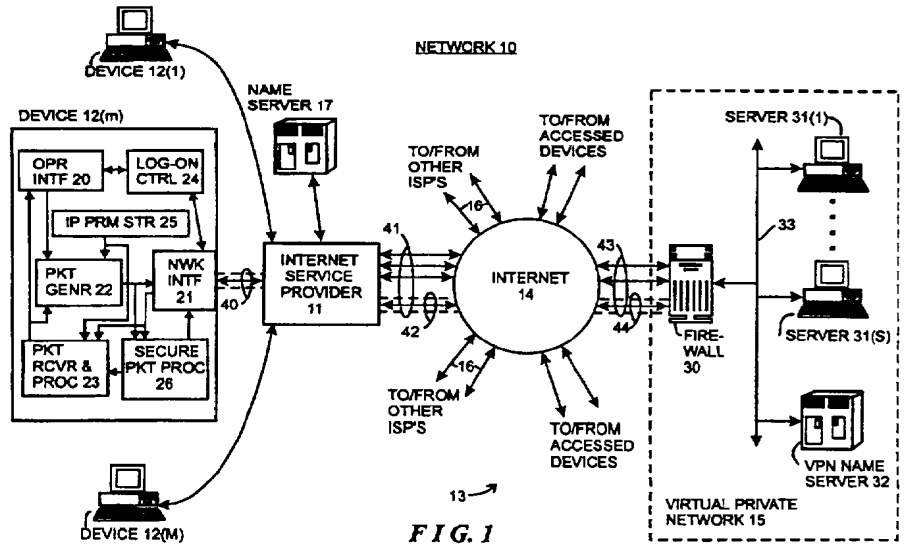


FIG. 1

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

GB 2 340 702 A

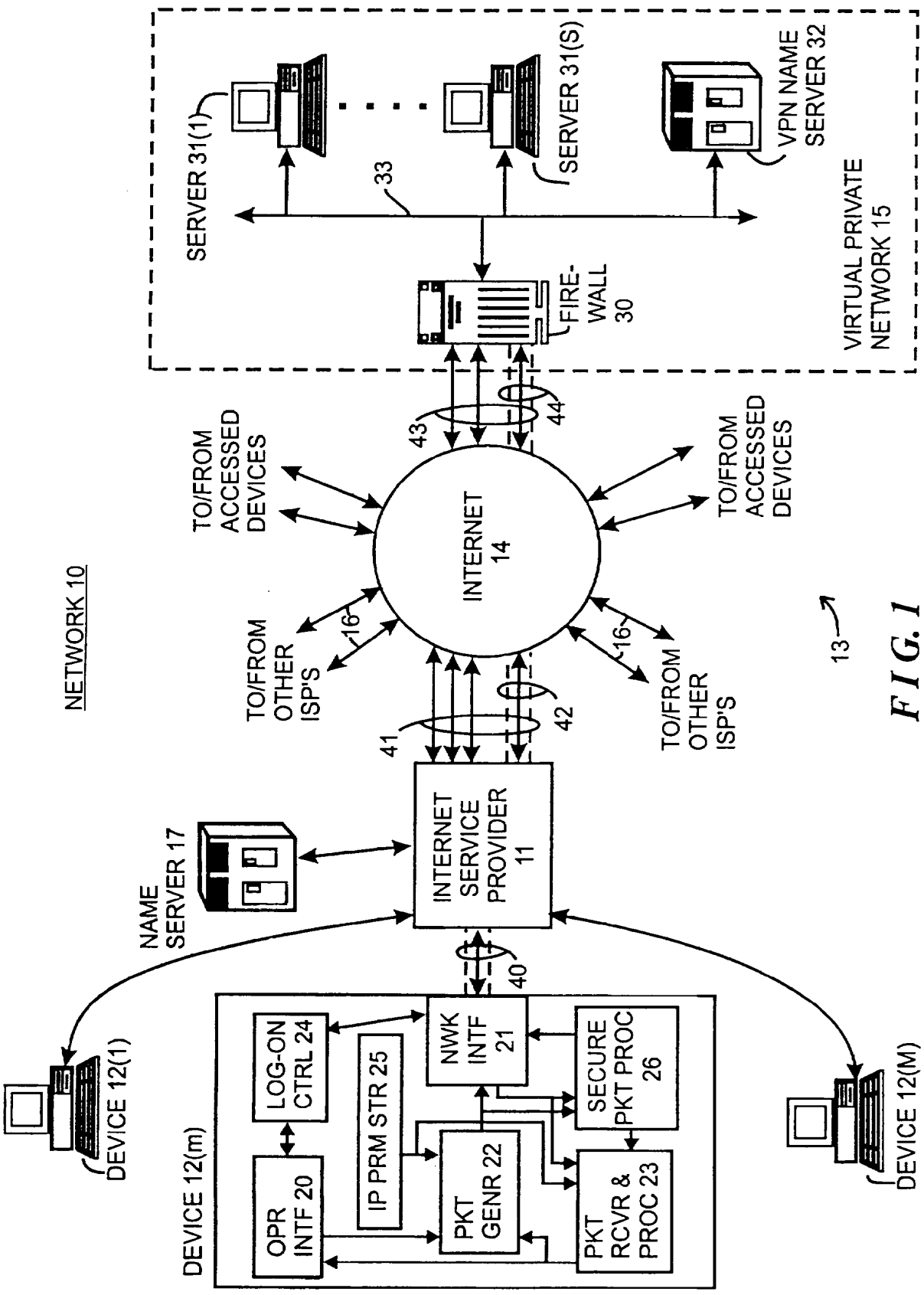

NETWORK 10
VIRTUAL PRIVATE NETWORK 15
SERVER 31(1)
SERVER 31(S)
VPN NAME SERVER 32
33
FIRE-WALL 30
43
44
TO/FROM ACCESSED DEVICES
TO/FROM ACCESSED DEVICES
INTERNET 14
TO/FROM OTHER ISP'S
16
16
TO/FROM OTHER ISP'S
41
42
13
NAME SERVER 17
INTERNET SERVICE PROVIDER 11
40
DEVICE 12(1)
DEVICE 12(m)
DEVICE 12(M)
LOG-ON CTRL 24
NWK INTF 21
SECURE PKT PROC 26
IP PRM STR 25
OPR INTF 20
PKT GENR 22
PKT RCVR & PROC 23

FIG. 1

FIELD OF THE INVENTION

The invention relates generally to the field of digital communications systems and methods, and more particularly to systems and methods for easing communications between devices connected to public networks such as the Internet and devices connected to private networks.

BACKGROUND OF THE INVENTION

Digital networks have been developed to facilitate the transfer of information, including data and programs, among digital computer systems and other digital devices. A variety of types of networks have been developed and implemented, including so-called "wide-area networks" (WAN's) and "local area networks" (LAN's), which transfer information using diverse information transfer methodologies. Generally, LAN's are implemented over relatively small geographical areas, such as within an individual office facility or the like, for transferring information within a particular office, company or similar type of organization. On the other hand, WAN's are generally implemented over relatively large geographical areas, and may be used to transfer information between LAN's as well as between devices that are not connected to LAN's. WAN's also include public networks, such as the Internet, which can carry information for a number of companies.

Several problems have arisen in connection with communication over a network, particularly a large public WAN such as the Internet. Generally, information is transferred over a network in message packets, which are transferred from one device, as a source device, to another device as a destination device, through one or more routers or switching nodes (generally, switching nodes) in the network. Each message packet includes a destination address which the switching nodes use to route the respective message packet to the appropriate destination device. Addresses over the Internet are in the form of an "n"-bit integer (where "n" may be thirty two or 128), which are difficult for a person to remember and enter when he or she wishes to enable a message packet to be transmitted. To relieve a user of the necessity of remembering and entering specific integer Internet

addresses, the Internet provides second addressing mechanism which is more easily utilized by human operators of the respective devices. In that addressing mechanism, Internet domains, such as LAN's, Internet service providers ("ISP's") and the like which are connected in the Internet, are identified by relatively human-readable names. To accommodate the use of human-readable names, nameservers, also referred to as DNS servers, are provided to resolve the human-readable names to the appropriate Internet addresses. When an operator at one device, wishing to transmit a message packet to another device, enters the other device's human-readable name, the device will initially contact a nameserver. Generally, the nameserver may be part of the ISP itself or it may be a particular device which is accessible through the ISP over the Internet; in any case, the ISP will identify the nameserver to be used to the device when the device logs in to the ISP. If, after being contacted by the device, the nameserver has or can obtain an integer Internet address for the human-readable domain name, it (that is, the nameserver) will provide the integer Internet address corresponding to the human-readable domain name to the operator's device. The device, in turn, can thereafter include the integer Internet address returned by the nameserver in the message packet and provide the message packet to the ISP for transmission over the Internet in a conventional manner. The Internet switching nodes use the integer Internet address to route the message packet to the intended destination device.

Other problems arise, in particular, in connection with the transfer of information over a public WAN such as the Internet. One problem is to ensure that information transferred over the WAN that the source device and the destination device wish to maintain confidential, in fact, remains confidential as against possible eavesdroppers which may intercept the information. To maintain confidentiality, various forms of encryption have been developed and are used to encrypt the information prior to transfer by the source device, and to decrypt the information after it has been received by the destination device. If it is desired that, for example, all information transferred between a particular source device and a particular destination device is maintained confidential, the devices can establish a "secure tunnel" therebetween, which essentially ensures that all information to be transferred by the source device to the destination device is encrypted (except for certain

protocol information, such as address information, which controls the flow of network packets through the network between the source and destination devices) prior to transfer, and that the encrypted information will be decrypted prior to utilization by the destination device. The source and destination devices may themselves perform the encryption and decryption, respectively, or the encryption and decryption may be performed by other devices prior to the message packets being transferred over the Internet.

A further problem that arises in particular in connection with companies, government agencies, and private organizations whose private networks, which may be LAN's, WAN's or any combination thereof, are connected to public WAN's such as the Internet, is to ensure that their private networks are secure against others whom the companies do not wish to have access thereto, or to regulate and control access by others whom the respective organizations may wish to have limited access. To accommodate that, the organizations typically connect their private networks to the public WAN's through a limited number of gateways sometimes referred to as "firewalls," through which all network traffic between the internal and public networks pass. Typically, network addresses of domains and devices in the private network "behind" the firewall are known to nameservers which are provided in the private network, but are not available to nameservers or other devices outside of the private network, making communication between a device outside of the private network and a device inside of the private network difficult.

SUMMARY OF THE INVENTION

Particular and preferred aspects of the invention are set out in the accompanying independent and dependent claims. Features of the dependent claims may be combined with those of the independent claims as appropriate and in combinations other than those explicitly set out in the claims.

The invention provides a new and improved system and method for easing communications between devices connected to public networks such as the Internet and devices connected to private networks by facilitating resolution of secondary addresses, such as the Internet's human-readable addresses, to network addresses by nameservers or the like connected to the private networks.

In brief summary, an embodiment of the invention provides a system comprising a virtual private network and an external device interconnected by a digital network. The virtual private network has a firewall, at least one internal device and a nameserver each having a network address. The internal device also has a secondary address, and the nameserver is configured to provide an association between the secondary address and the network address. The firewall, in response to a request from the external device to establish a connection therebetween, provides the external device with the network address of the nameserver. The external device, in response to a request from an operator or the like, including the internal device's secondary address, requesting access to the internal device, generates a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address. The firewall provides the address resolution request to the nameserver, and the nameserver provides the network address associated with the secondary address to the firewall. The firewall, in turn, provides the network address in a network address response message for transmission over the connection to the external device. The external device can thereafter use the network address so provided in subsequent communications with the firewall intended for the internal device.

BRIEF DESCRIPTION OF THE DRAWINGS

Exemplary embodiments of the invention are described hereinafter, by way of example only, with reference to the accompanying drawings, in which:

FIG. 1 is a functional block diagram of a network constructed in accordance with the invention.

DETAILED DESCRIPTION OF AN ILLUSTRATIVE EMBODIMENT

FIG. 1 is a functional block diagram of a network 10 constructed in accordance with the invention. The network 10 as depicted in FIG. 1 includes an Internet service provider ("ISP") 11 which facilitates the transfer of message packets among one or more devices 12(1) through 12(M) (generally identified by reference numeral 12(m)) connected to ISP 11, and other devices, generally identified by reference numeral 13, over the Internet 14, thereby to facilitate the transfer of information in message packets among the devices 12(m) and 13. The ISP 11 connects to the Internet 14 over one or more logical connections or gateways or the like (generally referred to herein as "connections") generally identified by reference numeral 41. The ISP 11 may be a public ISP, in which case it connects to devices 12(m) which may be controlled by operators who are members of the general public to provide access by those operators to the Internet. Alternatively, ISP 11 may be a private ISP, in which case the devices 12(m) connected thereto are generally operated by, for example, employees of a particular company or governmental agency, members of a private organization or the like, to provide access by those employees or members to the Internet.

As is conventional, the Internet comprises a mesh of switching nodes (not separately shown) which interconnect ISP's 11 and devices 13 to facilitate the transfer of message packets thereamong. The message packets transferred over the Internet 14 conform to that defined by the so-called Internet protocol "IP" and include a header portion, a data portion, and may include a error detection and/or correction portion. The header portion includes information used to transfer the message packet through the Internet 14, including, for example, a destination address that identifies the device that is to receive the message packet as the destination device and a source address that identifies the device which generated the message packet. For each message packet, the destination and source addresses are each in the form of an integer that uniquely identifies the respective destination and source devices. The switching nodes comprising the Internet 14 use at least the destination address of each respective message packet to route it (that is, the respective message packet) to the destination device, if the destination device is connected to the Internet, or to an ISP 11 or other device connected to the Internet 14, which, in turn, will forward the message packet to the appropriate destination. The data portion of each message packet includes the data to be transferred

in the message packet, and the error detection and/or correction portion contains error detection and/or correction information which may be used to verify that the message packet was correctly transferred from the source to the destination device (in the case of error detection information), and correct selected types of errors if the message packet was not correctly transferred (in the case of error correction information).

The devices 12(m) connected to ISP 11 may comprise any of a number of types of devices which communicate over the Internet 14, including, for example, personal computers, computer workstations, and the like, with other devices 13. Each device 12(m) communicates with the ISP 11 to transfer message packets thereto for transfer over the Internet 14, or to receive message packets therefrom received by the ISP 11 over the Internet 14, using any convenient protocol such as the well-known point-to-point protocol ("PPP") if the device 12(m) is connected to the ISP 11 using a point-to-point link, any conventional multi-drop network protocol if the device 12(m) is connected to the ISP 11 over a multi-drop network such as the Ethernet, or the like. The devices 12(m) are generally constructed according to the conventional stored-program computer architecture, including, for example, a system unit, a video display unit and operator input devices such as a keyboard and mouse. A system unit generally includes processing, memory, mass storage devices such as disk and/or tape storage elements and other elements (not separately shown), including network and/or telephony interface devices for interfacing the respective device to the ISP 11. The processing devices process programs, including application programs, under control of an operating system, to generate processed data. The video display unit permits the device to display processed data and processing status to the user, and the operator input device enables the user to input data and control processing.

These elements of device 12(m), along with suitable programming, cooperate to provide device 12(m) with a number of functional elements including, for example, an operator interface 20, a network interface 21, a message packet generator 22, a message packet receiver and processor 23, an ISP log-on control 24, an Internet parameter store 25 and, in connection with the invention, a secure message packet processor 26. The operator interface 20 facilitates reception by the device

12(m) of input information from the operator input device(s) of device 12(m) and the display of output information to the operator on the video display device(s) of the device 12(m). The network interface 21 facilitates connection of the device 12(m) to the ISP 11 using the appropriate PPP or network protocol, to transmit message packets to the ISP 11 and receive message packets therefrom. The network interface 21 may facilitate connection to the ISP 11 over the public telephone network to allow for dial-up networking of the device 12(m) over the public telephone system. Alternatively or in addition, the network interface 21 may facilitate connection through the ISP 11 over, for example, a conventional LAN such as the Ethernet. The ISP log on control 24, in response to input provided by the operator interface 20 and/or in response to requests from programs (not shown) being processed by the device 12(m), communicates through the network interface 21 to facilitate the initialization ("log-on") of a communications session between the device 12(m) and the ISP 11, during which communications session the device 12(m) will be able to transfer information, in the form of, message packets with other devices over the Internet 14, as well as other devices 12(m') ($m' \neq m$) connected to the ISP 11 or to other ISP's. During a log-on operation, the ISP log-on control 24 receives the Internet protocol ("IP") parameters which will be used in connection with message packet generation during the communications session.

During a communications session, the message packet generator 22, in response to input provided by the operator through the operator interface 20, and/or in response to requests from programs (not separately shown) being processed by the device 12(m), generates message packets for transmission through the network interface 21. The network interface 21 also receives message packets from the ISP 11 and provides them to message packet receiver and processor 23 for processing and provision to the operator interface 20 and/or other programs (not shown) being processed by the device 12(m). If the received message packets contain information, such as Web pages or the like, which is to be displayed to the operator, the information can be provided to the operator interface 20 to enable the information to be displayed on the device's video display unit. In addition or alternatively, the information may be provided to other programs (not shown) being processed by the device 12(m) for processing.

Generally, elements such as the operator interface 20, message packet generator 22, message packet receiver and processor 23, ISP log-on control 24 and Internet parameter store 25 may comprise elements of a conventional Internet browser, such as Mosaic, Netscape Navigator and Microsoft Internet Explorer.

In connection with the invention, as noted above the device 12(m) also includes a secure message packet processor 26. The secure message packet processor 26 facilitates the establishment and use of a "secure tunnel," which will be described below, between the device 12(m) and another device 12 (m') (m'≠m) or 13. Generally, in a secure tunnel, information in at least the data portion of message packets transferred between device 12(m) and a specific other device 12(m') (m'≠m) or 13 is maintained in secret by, for example, encrypting the data portion prior to transmission by the source device. Information in other portions of such message packets may also be maintained in secret, except for the information that is required to facilitate the transfer of the respective message packet between the devices, including, for example, at least the destination information, so as to allow the Internet's switching nodes and ISP's to identify the device that is to receive the message packet.

In addition to ISP 11, a number of other ISP's may connect to the Internet, as represented by arrows 16, facilitating communications between devices which are connected to those other ISP's with other devices over the Internet, which may include the devices 12(n) connected to ISP 11.

The devices 13 which devices 12(m) access and communicate with may also be any of a number of types of devices, including personal computers, computer workstations, and the like, and also including mini-and mainframe computers, mass storage systems, compute servers, local area networks ("LAN's") and wide area networks ("WAN's") including such devices and numerous other types of devices which may be connected directly or indirectly to the networks. In connection with the invention, at least one of the devices will include at least one private network, identified as virtual private network 15, which may be in the form of a LAN or WAN. The virtual private network 15 may comprise any of the devices 12(m') (m'≠m) (thereby connecting to the Internet 14

through an ISP) or 13 (thereby connecting directly to the Internet 14); in the illustrative embodiment described herein, the virtual private network 15 will be assumed to comprise a device 13. The virtual private network 15 itself includes a plurality of devices, identified herein as a firewall 30, a plurality of servers 31(1) through 31(S) (generally identified by reference numeral 31(s)) and a nameserver 32, all interconnected by a communication link 33. The firewall 30 and servers 31(s) may be similar to any of the various types of devices 12(m) and 13 described herein, and thus may include, for example, personal computers, computer workstations, and the like, and also including mini-and mainframe computers, mass storage systems, compute servers, local area networks ("LAN's") and wide area networks ("WAN's") including such devices and numerous other types of devices which may be connected directly or indirectly to the networks.

As noted above, the devices, including devices 12(m) and devices 13, communicate by transferring message packets over the Internet. The devices 12(m) and 13 can transfer information in a "peer-to-peer" manner, in a "client-server" manner, or both. Generally, in a "peer-to-peer" message packet transfer, a device merely transfers information in one or more message packets to another device. On the other hand, in a "client-server" manner, a device, operating as a client, can transfer a message packet to another device, operating as a server to for example, initiate service by the other device. A number of types of such services will be appreciated by those skilled in the art, including, for example, the retrieval of information from the other device, to enable the other device to perform processing operations, and the like. If the server is to provide information to the client, it (that is, the server) may generally be referred to as a storage server. On the other hand, if the server is to perform processing operations at the request of the client, it (that is, the server) may generally be referred to as a compute server. Other types of servers, for performing other types of services and operations at the request of clients, will be appreciated by those skilled in the art.

In a client/server arrangement, device 12(m) requiring service by, for example, a device 13, generates one or more request message packets requesting the required service, for transfer to the device 13. The request message packet includes the Internet address of the device 13 that is, as the destination device, to receive the message packet and perform the service. The device 12(m)

transfers the request message packet(s) to the ISP 11. The ISP 11, in turn, will transfer the message packet over the Internet to the device 13. If the device 13 is in the form of a WAN or LAN, the WAN or LAN will receive the message packet(s) and direct it (them) to a specific device connected therein which is to provide the requested service.

In any case, after the device 13 which is to provide the requested service receives the request message packet (s), it will process the request. If the device 12(m) which generated the request message packet(s), or its operator, has the required permissions to request the service from the device 13 which generated the request message packet, if the requested service is to initiate the transfer of information from the device 13 as a storage server to the device 12(m) as client, the device 13 will generate one or more response message packets including the requested information, and transmit the packet(s) over the Internet 14 to the ISP 11. The ISP 11, in turn, will transfer the message packet(s) to the device 12(m). On the other hand, if the requested service is to initiate processing by the device 13 as a compute server, the device 13 will perform the requested computation service(s). In addition, if the device 13 is to return processed data generated during the computations to the device 12(m) as client, the device 13 will generate one or more response message packet(s) including the processed data and transmit the packet(s) over the Internet 14 to the ISP 11. The ISP 11, in turn, will transfer the message packet(s) to the device 12(m). Corresponding operations may be performed by the devices 12(m) and 13, ISP 11 and Internet 14 in connection with other types of services which may be provided by the server devices 13.

As noted above, each message packet that is generated by devices 12(m) and 13 for transmission over the Internet 14 includes a destination address, which the switching nodes use to route the respective message packet to the appropriate destination device. Addresses over the Internet are in the form of an "n"-bit integer (where "n" currently may be thirty two or 128). To relieve, in particular, an operator of a device 12(m) of the necessity of remembering specific integer Internet addresses and providing them to the device 12(m) to initiate generation of a message packet for transmission over the Internet, the Internet provides a second addressing mechanism which is more easily utilized by human operators of the respective devices. In that addressing mechanism,

Internet domains, such as LAN's, Internet service providers ("ISP's") and the like which are connected in the Internet, are identified by relatively human-readable names. To accommodate human-readable domain names, ISP 11 is associated with a nameserver 17 (which may also be referred to as a DNS servers), which can resolve the human-readable domain names to provide the appropriate Internet address for the destination referred to in the respective human-readable name. Generally, the nameserver may be part of or connected directly to the ISP 11, as shown in FIG. 1, or it may be a particular device which is accessible through the ISP over the Internet. In any case, as noted above, when the device 12(m) logs on to the ISP 11 during a communications session, the ISP 11 will assign various Internet protocol ("IP") parameters which the device 12(m) is to use during the communications session, which will be stored in the Internet parameter store 25. These IP parameters include such information as

(a) an Internet address for the device 12(m) which will identify the device 12(m) during the communications session, and

(b) the identification of a nameserver 17 that the device 12(m) is to use during the communications session.

The device 12(m), when it generates message packets for transfer, will include its Internet address (item (a) above) as the source address. The device(s)13 which receives the respective message packets can use the source address from message packets received from the device 12(m) in message packets which they (that is, device(s) 13) generate for transmission to the device 12(m), thereby to enable the Internet to route the message packets generated by the respective device 13 to the device 12(m). If the device 12(m) is to access the nameserver 17 over the Internet 14, the nameserver identification provided by the ISP 11 (item (b) above) will be in the form of an integer Internet address which will allow the device 12(m) to generate messages to the nameserver 17 requesting resolution of human-readable Internet addresses into integer Internet addresses. The ISP 11 may also assign other IP parameters to the device 12(m) when it logs on to the ISP 11, including, for example, the identification of a connection to the Internet 14 that is to be used for messages transmitted by the

device 12(m), particularly if the ISP 11 has multiple gateways. Generally, the device 12(m) will store the Internet parameters in the Internet parameter store 25 for use during the communications session.

When an operator operating device 12(m) wishes to enable the device 12(m) to transmit a message packet to a device 13, he or she provides the Internet address for the device 13 to the device 12(m), through the operator interface 20, and information, or the identification of information maintained by the device 12(m) that is to be transmitted in the message. The operator interface 20, in turn, will enable the packet generator 22 to the required packets for transmission through the ISP 11 over the Internet 11. If

(i) the operator has provided the integer Internet address, or

(ii) the operator has provided the human-readable Internet address, but the packet generator 22 already has the integer Internet address which corresponds to the human-readable Internet address provided by the operator,

the packet generator 22 may generate the packets directly upon being enabled by the operator interface 20, and provide them to the network interface 21 for transmission to the ISP 11.

However, if the operator has provided the human-readable Internet address for the device 13 to which the packets are to be transferred, and if the packet generator 22 does not already have the corresponding integer Internet address therefor, the packet generator 22 will enable the network address to be obtained from the nameserver 17 identified in the IP parameter store 25. In that operation, the packet generator 22 will initially contact nameserver 17 to attempt to obtain the appropriate integer Internet address from the nameserver 17. In these operations, the device 12(m) will generate appropriate message packets for transmission to the nameserver 17, using the nameserver's integer Internet address as provided by the ISP 11 when it (that is, the device 12(m)) logs on at the beginning of the communications session. In any case, if the nameserver 17 has or can obtain the integer Internet address for the human-readable name, it (that is, the nameserver 17) will

provide the integer Internet address to the device 12(m). The integer Internet address will be received by the packet generator 22 through the network interface 21 and packet receiver and processor 23. After the packet generator 22 receives the integer Internet address, it can generate the necessary message packets for transmission to the device 13 through the network interface 21 and ISP 11.

As noted above, one of the devices 13 connected to the Internet 14 is virtual private network 15, the virtual private network 15 including a firewall 30, a plurality of devices identified as servers 31(s), and a nameserver 32 interconnected by a communication link 33. The servers 31(s), firewall 30 and nameserver 32 can, as devices connected in a LAN or WAN, transfer information in the form of message packets thereamong. Since the firewall 30 is connected to the Internet 14 and can receive message packets thereover it has an Internet address. In addition, at least the servers 31(s) which can be accessed over the Internet also have respective Internet addresses, and in that connection the nameserver 32 serves to resolve human-readable Internet addresses for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses.

Generally, the virtual private network 15 is maintained by a company, governmental agency, organization or the like, which desires to allow the servers 31(s) to access other devices outside of the virtual private network 15 and transfer information thereto over the Internet 14, but which also desires to limit access to the servers 31(s) by devices 12(m) and other devices over the Internet 14 in a controlled manner. The firewall 30 serves to control access by devices external to the virtual private network 15 to servers 31(s) within the virtual private network 15. In that operation, the firewall 30 also connects to the Internet 14, receives message packets therefrom for transfer to a server 31(s). If the message packet indicates that the source of the message packet is requesting access to the particular server 31(s), and if the source is authorized to access the server 31(s), the firewall 30 will forward the message packet over the communication link 33 to the server 31(s). On the other hand if the source is not authorized to access the server 31(s), the firewall 30 will not forward the message packet to the server 31(s), and may, instead, transmit a response message packet to the source device indicating that the source was not authorized to access the server 31(s). The

firewall may be similar to other devices 31(s) in the virtual private network 15, with the addition of one or more connections to the Internet, which are generally identified by reference numeral 43.

Communications between devices external to the virtual private network 15, such as device 12(m), and a device, such as a server 31(s), inside the virtual private network 15, may be maintained over a secure tunnel between the firewall 30 and the external device as described above to maintain the information transferred therebetween secret while being transferred over the Internet 14 and through the ISP 11. A secure tunnel between device 12(m) and virtual private network 15 is represented in FIG. 1 by logical connections identified by reference numerals 40, 42, and 44; it will be appreciated that the logical connection 42 comprises one of the logical connections 41 between ISP 11 and Internet 14, and logical connection 44 comprises one of the logical connections 43 between the Internet 14 and the firewall 30.

Establishment of a secure tunnel can be initiated by device 12(m) external to the virtual private network 15. In that operation, the device 12(m), in response to a request from its operator, generates a message packet for transfer through the ISP 11 and Internet 14 to the firewall 30 requesting establishment of a secure tunnel between the device 12(m) and firewall 30. The message packet may be directed to a predetermined integer Internet address associated with the firewall 30 which is reserved for secure tunnel establishment requests, and which is known to and provided to the device 12(m) by the nameserver 17. If the device 12(m) is authorized to access a server 31(s) in the virtual private network 15, the client 12(m) and firewall 30 engage in a dialog, comprising one or more message packets transferred therebetween over the Internet 14. During the dialog, the firewall 30 may provide the device 12(m) with the identification of a decryption algorithm and associated decryption key which the device 12(m) is to use in decrypting the encrypted portions of message packets which the virtual private network transmits to the device 12(m). In addition, the firewall 30 may also provide the device 12(m) with the identification of an encryption algorithm and associated encryption key which the device 12(m) is to use in encrypting the portions of message packets which the device 12(m) transmits to the virtual private network 15 which are to be encrypted; alternatively, the device 12(m) can provide the identification of the encryption algorithm

and key that it (that is device 12(m)) will use to the firewall 30 during the dialog. The device 12(m) can store in its IP parameter store 25 information concerning the secure tunnel, including information associating the identification of the firewall 30 and the identifications of the encryption and decryption algorithms and associated keys for message packets to be transferred over the secure tunnel.

Thereafter, the device 12(m) and firewall 30 can transfer message packets over the secure tunnel. The device 12(m), in generating message packets for transfer over the secure tunnel, makes use of the secure packet processor 26 to encrypt the portions of the message packets which are to be encrypted prior to transmission by the network interface 21 to the ISP 11 for transfer over the Internet 14 to the firewall 30, and to decrypt the encrypted portions of the message packets received by the device 12(m) which are encrypted. In particular, after the packet generator 22 generates a message packet for transmission to the firewall 30 over the secure tunnel, it will provide the message packet to the secure packet processor 26. The secure packet processor 26, in turn, encrypts the portions of the message packet that are to be encrypted, using the encryption algorithm and key. After the firewall 30 receives a message packet from the device 12(m) over the secure tunnel, it will decrypt it and, if the intended recipient of the message packet is another device, such as a server 31(s), in the virtual private network 14, it (that is, the firewall 30) will transfer the message packet to that other device over the communication link 33.

For a message packet that is to be transferred by a device, such as a server 31(s), in the virtual private network 15 to the device 12(m) over the secure tunnel, the firewall 30 will receive such to the message packet over the communication link 33 and encrypt the message packet for transfer over the Internet 14 to the ISP 11. The ISP 11, in turn, forwards the message packet to the device 12(m), in particular to its network interface 21. The network interface 21 provides the message packet to the secure packet processor 26, which decrypts the encrypted portions of the message packet, using the decryption algorithm and key.

A problem arises in connection with accesses by a device, such as device 12(m), which is external to the virtual private network 15, and a device, such as a server 31(s), which is external to the firewall, namely, that nameserver 17 is not provided with integer Internet addresses for servers 31(s) and other devices which are in the virtual private network 15, except for integer Internet addresses associated with the firewall 30. Thus, the device 12(m), after the operator has entered the human-readable Internet address, will not be able to obtain the integer Internet address of the server 31(s) which is to be accessed from that nameserver 17.

To accommodate this problem, when the device 12(m) and firewall 30 cooperate to establish a secure tunnel therebetween, in addition to possibly providing the device 12(m) with the identifications of the encryption and decryption algorithms and keys which are to be used in connection with the message packets transferred over the secure tunnel, the firewall 30 also provides the device 12(m) with the identification of a nameserver, such as nameserver 32, in the virtual private network 15 which the device 12(m) can access to obtain the appropriate integer Internet addresses for the human-readable Internet addresses which may be provided by the operator of device 12(m). The identification of nameserver 32 is also stored in the IP parameter store 25, along with the identification of nameserver 17 which was provided by the ISP 11 when the device 12(m) logged on to the ISP 11 at the beginning of a communications session. Thus, when the device 12(m) is to transmit a message packet to a device, such as a server 31(s) in the virtual private network 14 using a human-readable Internet address provided by, for example, an operator, the device 12(m) will initially access the nameserver 17, as described above, to attempt to obtain the integer Internet address associated with the human-readable Internet address. Since nameserver 17 is outside of the virtual private network 15 and will not have the information requested by the device 12(m), it will send a response message packet so indicating. The device 12(m) will thereafter generate a request message packet for transmission to the nameserver 32 through the firewall 30 and over the secure tunnel. If the nameserver 32 has an integer Internet address associated with the human-readable Internet address in the request message packet provided by the device 12(m), it will provide the integer Internet address in a manner that is generally similar to that described above in connection

with nameserver 18, except that the integer Internet address will be provided by the nameserver 32 in a message packet directed to the firewall 30, and the firewall 30 will thereafter transmit the message packet over the secure tunnel to the device 12(m). In the message packet transmitted by the firewall 30, it will be appreciated that the integer Internet address in the message packet will be in the data portion of the message packet transferred over the secure tunnel and, accordingly, will be in encrypted form. The message packet will be processed by the device 12(m) in a manner similar to that described above in connection with other message packets received by it over the secure tunnel, that is, the message packet will be decrypted by the secure packet processor 26 prior to being provided to the packet receiver and processor 23 for processing. The integer Internet address for the server 31(s) can be cached in an access control list ("ACL") in the IP parameter store 25, along with the association of the human-readable Internet address thereto, an indication that the server 31(s) associated with that human-readable Internet address is to be accessed through the firewall 30 of the virtual private network 15, and the identifications of the encryption and decryption algorithms and keys to be used for encrypting and decrypting the appropriate portions of the message packets transmitted to server 31(s) and received from server 31(s).

It will be appreciated that, if the nameserver 32, in response to a message packet from the device 12(m) requesting the nameserver 32 to provide an integer Internet address for a human-readable Internet address provided by the device 12(m), if the nameserver 32 does not have an association between the human-readable Internet address and an integer Internet address, the nameserver 32 can provide a response message packet so indicating. If the device 12(m) has identification of other nameservers, such as may be associated with other virtual private networks (not shown), to which it (that is, device 12(m)) may have access, then the device 12(m) can attempt to access the other nameservers in a similar manner as described above. If the device 12(m) is unable to obtain an integer Internet address associated with the human-readable Internet address from any of the nameservers to which it has access, and which generally will be identified in its IP parameter store 25, it will generally be unable to access a device having the human-readable Internet address, and may so notify its operator or program which requested the access.

With this background, operations performed by the device 12(m) and virtual private network 15 in connection with the invention will be described in detail. Generally, operations proceed in two phases. In the first phase, the device 12(m) and virtual private network 15 cooperate to establish a secure tunnel through the Internet 14. In that first phase, the virtual private network 15, in particular the firewall 30 provide the identification of a nameserver 32, and may also provide the encryption and decryption algorithm and key information, as described above. In the second phase, after the secure tunnel has been established, the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more servers 31(s) in the virtual private network 15, in the process obtaining resolution human-readable Internet addresses to integer Internet addresses as necessary from the nameserver 32 that was identified by the firewall 30 during the first phase.

Thus, in the first (secure tunnel establishment) phase, the device 12(m) initially generates a message packet requesting establishment of a secure tunnel for transfer to the firewall 30. The message packet will include an integer Internet address for the firewall (which may have been provided by the device's operator or a program being processed by the device 12(m) or have been provided by a the nameserver 17 after a human-readable Internet address was provided by the operator or a program), and which, in particular, is to enable the firewall 30 to establish secure tunnels therewith. If the firewall 30 accepts the secure tunnel establishment request, and if the firewall 30 provides the encryption and decryption algorithms and keys as noted above, it (that is, the firewall) will generate a response message packet for transmission to the device 12(m) that identifies the encryption and decryption algorithms and keys; as noted above, this response message packet will not be encrypted. When the device 12(m) receives the response message, the identifications of the encryption and decryption algorithms and keys will be stored in the IP parameter store 25.

At some point later in the first phase, the firewall 30 will also generate a message packet for transmission to the device 12(m) that includes the integer Internet address of the nameserver 32. For this message packet, the portion of the message packet that contains the integer Internet address of

the nameserver 32 will be encrypted, using encryption algorithm and key that can be decrypted using the decryption algorithm and key provided in the response message packet described above. This message will generally have a structure

"<IIA(FW),IIA(DEV12(m))><SEC_TUN>

<ENCR<<IIA(FW),IIA(DEV_12(m))><DNS_ADRS:IIA(NS_32)>>>"

where

(i) "IIA(FW)" represents the source address, that is, integer Internet address of the firewall 30,

(ii) "IIA(DEV_12(m))" represents the destination address, that is, the integer Internet address of the device 12(m),

(iii) "DNS_ADRS:IIA(NS) indicates that "IIA(NS_32)" represents the integer Internet address of the nameserver 32, the nameserver which the device 12(m) is authorized to use, and

(iv) "ENCR<....>" indicates that the information between brackets "<" and >" is encrypted.

The initial portion of the message "<IIA(FW),IIA(DEV_12(m))>" forms at least part of the header portion of the message, and "<ENCR<<IIA(FW),IIA(DEV_12(m))><IIA(NS)>>>" represents at least part of the data portion of the message. The "<SEC_TUN>" represents an indicator in the header indicating that the message is being transferred over the secure tunnel, thereby indicating that the data portion of the message contains encrypted information.

After the device 12(m) receives the message from the firewall 30 as described above, since the message packet contains the <SEC_TUN> indicator, its network interface 21 will transfer the encrypted portion "<ENCR<<IIA(FW),IIA(DEV_12(m))><DNS_ADRS:IIA(NS_32)>>>" to the secure packet processor 26 for processing. The secure packet processor will decrypt the encrypted portion, determine that the portion "IIA(NS_32)" is the integer Internet address of a nameserver, in

particular nameserver 32, that the device 12(m) is authorized to use, and store that address in the IP parameter store 25, along with an indication that message packets thereto are to be transferred to the firewall 30 and that data in the message packets is to be encrypted using the encryption algorithm and key previously provided by the firewall 30. It will be appreciated that, since the integer Internet address of nameserver 32 is transferred from the firewall to the device 12(m) in encrypted form, it will be maintained in confidence even if the packet is intercepted by a third party.

Depending on the particular protocol used to establish the secure tunnel, the firewall 30 and device 12(m) may also exchange message packets containing other information than that described above.

As noted above, in the second phase, after the secure tunnel has been established, the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more of the servers 31(s) in the virtual private network 15. In those operations, if the operator of device 12(m), or a program being processed by device 12(m), wishes to have device 12(m) transmit a message packet to a server 31(s) in the virtual private network 15, if the operator, through the operator interface 20, or the program provides a human-readable Internet address, the device 12(m), in particular the packet generator 22, will initially determine whether the IP parameter store 25 has cached therein an integer Internet address that is associated with the human-readable Internet address. If not, the packet generator 22 will generate a request message packet for transfer to the nameserver 17 requesting it to provide the integer Internet address associated with the human-readable Internet address. If the nameserver 17 has an integer Internet address associated with the human-readable Internet address, it will provide the integer Internet address to the device 12(m). It will be appreciated that this may occur if the human-readable Internet address in the request message packet has been associated with a device 13 external to the virtual private network 15, as well as with a server 32(s) in the virtual private network 15. Thereafter, the device 12(m) can use the integer Internet address to generate message packets for transfer over the Internet as described above.

Assuming, on the other hand, that the nameserver 17 does not have a integer Internet address associated with the human-readable Internet address, it (that is, the nameserver 17) will provide a response message packet so indicating to the device 12(m). Thereafter, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. If that next nameserver is nameserver 32, the packet generator 22 will provide the message packet to the secure packet processor 26 for processing. The secure packet processor 26, in turn, will generate a request message packet for transfer over the secure tunnel to the firewall 30. This message will generally have a structure

"<IIA(DEV_12(m)),IIA(FW)><SEC_TUN>

<ENCR<<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>>"

where

(i) "IIA(DEV_12(m))" represents the source address, that is, integer Internet address of the device 12(m)

(ii) "IIA(FW)" represents the destination address, that is, the integer Internet address of the firewall 30

(iii) "IIA(NS_32)" represents the address of the nameserver 32

(iii) "<<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>" represents the request message packet generated by the packet generator 22, where "<IIA(DEV_12(m)),IIA(NS_32)> represents the header portion of the request message packet, and "<IIA_REQ>" represents the data portion of the request message packet,

(iv) "ENCR<....>" indicates that the information between brackets "<" and >" is encrypted, and

(v) "<SEC_TUN>" represents an indicator in the header portion of the message packet generated by the secure packet generator 26 indicating that the message is being transferred over the secure tunnel, thereby indicating that the data portion of the message contains encrypted information.

When the firewall 30 receives the request message packet generated by the secure packet processor 26, it will decrypt the encrypted portion of the message packet to obtain <<IIA(DEV_12(m)),IIA(NS_32))><IIA_REQ>>" represents the request message packet as generated by the packet generator 22. After obtaining the request message packet, the firewall 30 will transmit it over the communication link 33 to the nameserver 32. In that process, depending on the protocol for transmission of message packets over the communication link 33, the firewall 30 may need to modify the request message packet to conform to the protocol of communication link 33.

After the nameserver 32 receives the request message packet, it will process it to determine whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet. If the nameserver determines that it has such an integer Internet address, it will generate a response message packet including the integer Internet address for transmission to the firewall. Generally, the response message packet will have a structure:

<<IIA(NS_32),IIA(DEV_12(m))><IIA_RESP>>

where

(i) "IIA(NS_32)" represents the source address, that is, integer Internet address of the nameserver 32,

(ii) "IIA(DEV_12(m))" represents the destination address, that is, integer Internet address of the device 12(m), and

(iii) "IIA_RESP" represents the integer Internet address associated with the human-readable Internet address.

After the firewall 30 receives the response message packet, since communications with device 12(m) are over the secure tunnel therebetween, it (that is, the firewall 30) will encrypt the response message packet received from the nameserver 32 and generate a message packet for transmission to the device 12(m) including the encrypted response message packet. Generally, the message packet generated by the firewall 30 has the structure:

"<IIA(FW),IIA(DEV12(m))><SEC_TUN>

<ENCR<<IIA(NS_32),IIA(DEV_12(m))><IIA_RESP>>>"

where

(i) "IIA(FW)" represents the source address, that is, integer Internet address of the firewall 30,

(ii) "IIA(DEV_12(m))" represents the destination address, that is, the integer Internet address of the device 12(m),

(iii) "SEC_TUN" represents an indicator in the header portion of the message packet generated by the secure packet generator 26 indicating that the message is being transferred over the secure tunnel, thereby indicating that the data portion of the message contains encrypted information, and

(iv) "ENCR<....>" indicates that the information between brackets "<" and >" (which constitutes the response message packet received from the nameserver 32) is encrypted.

In addition, depending on the protocol for transmission of message packets over the communication link 33, the firewall 30 may need to process and/or modify the message packet to conform to the protocol of Internet 14.

When the device 12(m) receives the message packet from the firewall 30, it (that is, the message packet) will be provided to the secure packet processor 26. The secure packet processor 26, in turn, will decrypt the encrypted portion of the message packet to obtain the integer Internet address associated with the human-readable Internet address, and load that information in the IP parameter store 25. Thereafter, the device can use that integer Internet address in generating message packets for transmission to the server 31(s) which is associated with the human-readable Internet address.

It will be appreciated that, if the nameserver 32 does not have an integer Internet address associated with the human-readable Internet address provided by the device 12(m) in the request message packet, it (that is, nameserver 32) can so indicate in the response message packet generated thereby. The firewall 30 will, in response to the response message packet provided by the nameserver 32, also generate a message packet for transmission to the device 12(m), the message packet including an encrypted portion comprising the response message packet generated by the nameserver 32. After the device 12(m) receives the message packet, the encrypted portion will be decrypted by the secure packet processor 26, which, in turn, will notify the packet generator 22 that the nameserver 32 does not have an integer Internet address associated with the human-readable Internet address. Thereafter, if the IP parameter store 25 contains the identification of another nameserver, the packet generator 22 of device 12(m) will generate a request message packet for transmission to the next nameserver identified in its IP parameter store 25 requesting that nameserver to provide the integer Internet address associated with the human-readable Internet address. On the other hand, if the IP parameter store 25 does not contain the identification of another nameserver, the packet generator 22 can notify the operator interface 20 or program that it is will be unable to generate a message packet for transmission to a device associated with the human-readable Internet address provided thereby.

An embodiment of the invention can provide a number of advantages. For example, it can provide a system for easing communications between devices connected to a public network such as the Internet 14, and devices connected to private networks such as virtual private network 15, by facilitating resolution

of human-readable addresses to network addresses by a nameservers connected to the private networks over a secure tunnel.

It will be appreciated that numerous modifications may be made to the arrangement described above in connection with FIG. 1. For example, although the network 10 has been described such that the identification of the encryption and decryption algorithms and keys are exchanged by the device 12(m) and firewall 30 during the dialog during which the secure tunnel is established, it will be appreciated that that information may be provided by the device 12(m) and firewall 30 separately from the establishment of a secure tunnel therebetween.

In addition, although an embodiment of the invention has been described in connection with the Internet, it will be appreciated that an embodiment of the invention can be used in connection with any network. Further, although an embodiment has been described in connection with a network which provides for human-readable network addresses, it will be appreciated that an embodiment can be used in connection with any network which provides for any form of secondary or informal network address arrangements.

It will be appreciated that a system in accordance with the invention can be constructed in whole or in part from special purpose hardware or a general purpose computer system, or any combination thereof, any portion of which may be controlled by a suitable program. Any program may in whole or in part comprise part of or be stored on the system in a conventional manner, or it may in whole or in part be provided in to the system over a network or other mechanism for transferring information in a conventional manner. Thus, such a computer program can form a product operable, when run on a computer, to provide the required functionality of an embodiment of the invention. The computer program product can be provided on a carrier medium, for example, a computer readable medium such as, for example, a memory, disc or other storage medium, or a transmission medium such as a telecommunications channel providing, for example, electrical, optical, wireless or other transmission. In addition, it will be appreciated that the system may be operated and/or otherwise controlled by means of information provided by an operator using operator input elements (not shown) which may be connected directly to the system or which may transfer the information to the system over a network or other mechanism for transferring information in a conventional manner.

The foregoing description has been limited to a specific embodiment of this invention. It will be apparent, however, that various variations and modifications may be made to the invention, with the attainment of some or all of the advantages of the invention.

CLAIMS

1. A system comprising a virtual private network and an external device which communicate over a digital network,

the virtual private network having a firewall, at least one internal device and a nameserver each having a network address, the internal device also having a secondary address, the nameserver being configured to provide an association between the secondary address and the network address,

the firewall, in response to a request from the external device to establish a connection therebetween, being configured to provide the external device with the network address of the nameserver, and

the external device, in response to a request requesting access to the internal device including the internal device's secondary address, being configured to generate a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address, the firewall being configured to provide the address resolution request to the nameserver, the nameserver being configured to provide the network address associated with the secondary address, the firewall in turn being further configured to provide the network address in a network address response message for transmission over the connection to the external device.

2. A system according to claim 1, wherein the external device is further configured to use the network address provided in the network address response message in generating at least one message for transmission to the internal device.

3. A system according to claim 1 or claim 2, wherein the external device is configured to connect to the network through a network service provider.

4. A system according to claim 3, wherein the external device is configured to establish a communications session with the network service provider, the network service provider providing the external device with the identification of a further nameserver, the further nameserver being configured to provide an association between a secondary address and a network address for at least one device.

5. A system according to any preceding claim, wherein the external device is configured to maintain a list of nameservers which have been identified to said external device, the external device being configured to interrogate successive ones of the nameservers in the list in response to a request requesting access to another device, said request including a secondary address for said other device, until said external device receives a network address, in each interrogation the external device being configured to generate a said network address request message for transmission over the network for response by one of said nameservers in said list and to receive a network address response message therefrom.

6. A system according to any preceding claim, wherein the connection between the external device and the firewall is a secure tunnel, in which at least some portion of messages transferred between the external device and the firewall is encrypted.

7. A method of operating a system comprising a virtual private network and an external device interconnected by a digital network, the virtual private network having a firewall, at least one internal device and a nameserver each having a network address, the internal device also having a

secondary address, the nameserver being configured to provide an association between the secondary address and the network address, the method comprising the steps of:

A. enabling the firewall, in response to a request from the external device to establish a connection therebetween, provide the external device with the network address of the nameserver; and

B. enabling

(i) the external device, in response to a request requesting access to the internal device including the internal device's secondary address, to generate a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address,

(ii) the firewall to provide the address resolution request to the nameserver,

(iii) the nameserver to provide the network address associated with the secondary address, and

(iv) the firewall to provide the network address in a network address response message for transmission over the connection to the external device.

8. A method according to claim 7, wherein the external device is further enabled to use the network address provided in the network address response message in generating at least one message for transmission to the internal device.

9. A method according to claim 7 or claim 8, wherein the external device is enabled to connect to the network through a network service provider.

10. A method according to claim 9, wherein the external device is enabled to establish a communications session with the network service provider, the network service provider being enabled to provide the external device with the identification of a further nameserver, the further nameserver being enabled to provide an association between a secondary address and a network address for at least one device.

11. A method according to any one of claims 7 to 10, wherein the external device is enabled to maintain a list of nameservers which have been identified to said external device, the external device being enabled to interrogate successive ones of the nameservers in the list in response to a request requesting access to another device, said request including a secondary address for said other device, until said external device receives a network address, in each interrogation the external device being enabled to generate a said network address request message for transmission over the network for response by one of said nameservers in said list and to receive a network address response message therefrom.

12. A method according to any one of claims 7 to 10, wherein the connection between the external device and the firewall is a secure tunnel, in which at least some portion of messages transferred between the external device and the firewall is encrypted.

13. A computer program product for use in connection with a virtual private network and an external device interconnected by a digital network, the virtual private network having a firewall, at least one internal device and a nameserver each having a network address, the internal device also having a secondary address, the nameserver being configured to provide an association between the secondary

address and the network address, the computer program product comprising :

A. a nameserver identification code module configured to enable the firewall, in response to a request from the external device to establish a connection therebetween, to provide the external device with the network address of the nameserver,

B. a network address request message generating code module for enabling the external device, in response to a request requesting access to the internal device including the internal device's secondary address, to generate a network address request message for transmission over the connection to the firewall requesting resolution of the network address associated with the secondary address,

C an address resolution request forwarding module for enabling the firewall to provide the address resolution request to the nameserver,

D. a nameserver control module for enabling the nameserver to provide the network address associated with the secondary address, and

E. a network address response message forwarding module for enabling the firewall to provide the network address in a network address response message for transmission over the connection to the external device.

14. A computer program product according to claim 13, further comprising a network address utilization module configured to enable the external device to use the network address provided in the network address response message in generating at least one message for transmission to the internal device.

15. A computer program product according to claim 13 or claim 14, further comprising a network service provider control module for enabling the external device to connect to the network through a network service provider.

16. A computer program product according to claim 15, wherein the network service provider control module includes a communications session establishment module for enabling the external device to a communications session with the network service provider and receive therefrom identification of a further nameserver.

17. A computer program product according to any one of claims 13 to 16, further including nameserver interrogation control module for enabling the external device to maintain a list of nameservers which have been identified to said external device, and to interrogate successive ones of the nameservers in the list in response to a request requesting access to another device, said request including a secondary address for said other device, until said external device receives a network address, in each interrogation the external device being enabled to generate a said network address request message for transmission over the network for response by one of said nameservers in said list and to receive a network address response message therefrom.

18. A computer program product according to any one of claims 13 to 16, wherein the connection between the external device and the firewall is a secure tunnel, in which at least some portion of messages transferred between the external device and the firewall is encrypted.

19. A computer program product according to any one of claims 13 to 18 on a carrier medium.

20. A computer program product according to claim 19, wherein the carrier medium is a computer readable medium.

21. A computer program product according to claim 19, wherein the carrier medium is a transmissions medium.

22. A system substantially as hereinbefore described with reference to the accompanying drawings.

23. A method substantially as hereinbefore described with reference to the accompanying drawings.

24. A computer program product substantially as hereinbefore described with reference to the accompanying drawings.

The Patent Office

34

INVESTOR IN PEOPLE

Application No: GB 9912200.4 **Examiner:** Gareth Griffiths
Claims searched: All **Date of search:** 7 December 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): H4P (PPA, PPEB, PPEC, PPG)

Int Cl (Ed.6): H04L 12/22, 12/46, 12/66, 29/06

Other: Online Databases: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X, P	EP0887979 A2	(SUN MICROSYSTEMS) col.15 line 35 - col.17 line 24	1, 2, 5-8, 11-14, 17-21
A	EP0825748 A2	(AT&T) col.6 line 46 - col.11 line 40	
A, P	WO98/31124 A1	(HANSON) p.5 line 2 - p.6 line 25	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Petitioner Apple Inc. - Exhibit 1026, p. 1044

Application Number	Application/Control No.	Applicant(s)/Patent under Reexamination	
	11/679,416	LARSON ET AL.	

Document Code - DISQ	Internal Document – DO NOT MAIL

TERMINAL DISCLAIMER	☒ APPROVED	☐ DISAPPROVED
Date Filed : 10/08/10	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:
2 td's Jean Proctor

U.S. Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/679,416	02/27/2007	Victor Larson	77580-015 (VRNK-1CP2DVCN)	3528

23630 7590 12/07/2010

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
LIM, KRISNA	

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
12/07/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mweipdocket@mwe.com

Office Action Summary	Application No.	Applicant(s)	
	11/679,416	LARSON ET AL.	
	Examiner	Art Unit	
	Krisna Lim	2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 October 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/08/2010 has been entered.

Claims 2-30 are presented for examination.

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 2-30 are rejected under 35 U.S.C. 102(b) as being anticipated by Aventail connect v3.1/v2.6 administrator's Guide References (hereafter Aventail). Applicants submitted this paper.

Aventail anticipated the invention substantially as claimed. Taking claim 2 as exemplary claims, the reference discloses a method of using a first device to communicate with a second device having a secure name (e.g., see pages 6, 12, 46, 62 and 66 for the teaching of "security firewall", "enabling remote users to gain secure access to internal network resources", etc.), the method comprising:

from the first device, sending a query message a secure domain service, the message requesting a network address associated with the secure name of the

second device (e.g., see page 8, 12, 45 and 48 for the teaching of Domain Name System lookup to convert the hostname to an IP address);

at the first network device, receiving a message containing the network address associated with the secure domain of the second device (e.g. see page 8 for the teaching of DNS lookup to convert the hostname into an IP address and vice versa, and see page 12 for the teaching of SOCKS negotiation when the connection is completed); and

from the first device, sending a message to the network of the second device using a secure communication link (e.g. see page 6 for the teaching of safeguard corporate networks and the exchanged information, and on pages 8 and 12 for the teaching of the application requests a connection to the specified remote host.., the handshake between two computers).

As to claim 3, Aventail further disclosed the secure name of the second device is a secure domain name (e.g. see page 6 for the teaching of security firewalls, and page 46 for the teaching of SOCKS v5 servers that often require user authentication before allowing access, the teaching of authentication module).

As to claim 4, Aventail further disclosed the secure name indicates security (e.g. see page 6 for the teaching of security firewalls, and page 46 for the teaching of SOCKS v5 servers that often require user authentication before allowing access, the teaching of authentication module).

As to claim 5, Aventail further disclosed receiving the message containing the network address associated with the secure name of the second device includes receiving the message in encrypted form (e.g., see pages 7, 10, 29, 46, 55, 68 and 77).

As to claim 6, Aventail further disclosed decrypting the message (e.g., see pages 7, 10, 29, 46, 55, 68 and 77).

As to claim 7, Aventail further disclosed the second device is capable of supporting a secure communication link as well as a non-secure communication link, the method further including establishing a non-secure communication link with the second device when needed (e.g. see page 29 for the teaching of Aventail allows user to select any, all or none of authentication modules and in versions of Aventail Connect that do not include encryption, the secure Sockets Layer).

As to claim 8, Aventail further disclosed receiving a message containing the network address associated with the secure name of the device includes receiving the network address as an IP address associated with the secure name of the device (e.g., see page 8, 12, 45 and 48 for the teaching of Domain Name System lookup to convert the hostname to an IP address).

As to claim 9, Aventail further disclosed automatically initiating the secure communication link after it is enabled (e.g., see page 116 for VPN: a secure channel used to transmit data over a public network, page 7 for VPN communication link).

As to claim 10, Aventail further disclosed receiving a message containing the network address associated with the secure name of the device includes receiving the message at the first device through tunneling within the secure communication link (e.g., see page 8, 12, 45 and 48 for the teaching of Domain Name System lookup to convert the hostname to an IP address).

As to claim 11, Aventail further disclosed receiving a message containing the network address associated with the secure name of the device includes receiving the message in the form of at least one tunneled packet (e.g. see page 7 for the teaching of establishing an encrypted tunnel automatically).

As to claim 12, Aventail further disclosed the receiving and sending of messages includes receiving and sending the messages in accordance with any one of a plurality of communication protocols (e.g., at page 68, Aventail Connect can open connections through SOCKS servers, through HTTP proxies, or through proxy chaining, and the teaching of TCP/IP in page 11-12).

As to claim 13, Aventail further disclosed the receiving and sending of messages through the secure communication link includes multiple sessions (e.g., at page 68, Aventail Connect can open connections through SOCKS servers, through HTTP proxies, or through proxy chaining, and the teaching of TCP/IP in page 11-12).

As to claim 14, Aventail further disclosed supporting a plurality of services over the secure communication link (e.g. see Aventail connect client connected to Internet on pages 77 and 79).

As to claim 15, Aventail further disclosed the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or a combination thereof (e.g., at page 68, Aventail Connect can open connections through SOCKS servers, through HTTP proxies, or through proxy chaining, and the teaching of TCP/IP in page 11-12).

As to claim 16, the feature of the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or a combination thereof is well known in the art at the time the invention was made.

As to claim 17, the feature of the plurality of services comprises audio, video or a combination thereof is well known in the art at the time the invention was made.

As to claim 18, Aventail further disclosed the secure communication link is an authenticated link (e.g. see authentication module on pages 6, 12, 29, 34 and 46).

As to claim 19, Aventail further disclosed the first device is a computer, and the steps are performed on the computer (e.g. see Aventail connect client connected to Internet on pages 77 and 79).

As to claim 20, Aventail further disclosed the first device is a client computer connected to a communication network, and the method is performed by the client computer on the communication network (e.g. see Aventail connect client connected to Internet on pages 77 and 79).

As to claim 21, Aventail further disclosed providing an unsecured name associated with the device (e.g. see page 29 for the teaching of Aventail allows user to select any, all or none of authentication modules and in versions of Aventail Connect that do not include encryption, the secure Sockets Layer).

As to claim 22, Aventail further disclosed the secure name is registered prior to the step of sending a message to a secure name service (see the teaching of define destination with IP address, subset and address ranges on pages 40-41).

As to claim 23, Aventail further disclosed the secure name of the second device is a secure, non-standard domain name (e.g. see page 29 for the teaching of Aventail allows user to select any, all or none of authentication modules and in versions of Aventail Connect that do not include encryption, the secure Sockets Layer, and on page 48 for the teaching of Disable/Enable authentication modules).

Claims 24-30 are rejected for the same rationale as claims 2-23, since they recite substantially identical subject matter. Any differences between the claims do not result in patentably distinct claims and all of the limitations are taught by the above cited references.

A shortened statutory period for response to this action is set to expire 3 (three) months and 0 (zero) days from the mail date of this letter.

Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.

If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.

Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Krisna Lim whose telephone number is 571-272-3956 The examiner can normally be reached on Tuesday to Friday from 7:10 AM to 5:40 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Krista Zele, can be reached on 571-272-7288. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kl

November 21, 2010

/Krisna Lim/

Primary Examiner, Art Unit 2453

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11679416	LARSON ET AL.
	Examiner	Art Unit
	Krisna Lim	2453

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	06/05/2009	03/27/2010	11/21/2010						
	1	✓	-	-						
	2		✓	✓						
	3		✓	✓						
	4		✓	✓						
	5		✓	✓						
	6		✓	✓						
	7		✓	✓						
	8		✓	✓						
	9		✓	✓						
	10		✓	✓						
	11		✓	✓						
	12		✓	✓						
	13		✓	✓						
	14		✓	✓						
	15		✓	✓						
	16		✓	✓						
	17		✓	✓						
	18		✓	✓						
	19		✓	✓						
	20		✓	✓						
	21		✓	✓						
	22		✓	✓						
	23		✓	✓						
	24		✓	✓						
	25		✓	✓						
	26		✓	✓						
	27		✓	✓						
	28		✓	✓						
	29		✓	✓						
	30		✓	✓						

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11679416	LARSON ET AL.
	Examiner	Art Unit
	Krisna Lim	2453

SEARCHED			
Class	Subclass	Date	Examiner
709	225-229, 245	6/6/09	kl

SEARCH NOTES		
Search Notes	Date	Examiner
Inventors, EAST	6/6/09	kl

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	11/679,416
Filing Date	02-27-2007
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	077580-0015

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	5,764,906	06/1998	Edelstein et al.	
	A2	5,864,666	01/1999	Shrader, Theodore Jack London	
	A3	5,898,830	04/1999	Wesinger et al.	
	A4	6,052,788	04/2000	Wesinger et al.	
	A5	6,061,346	05/2000	Nordman, Mikael	
	A6	6,081,900	06/2000	Subramaniam et al.	
	A7	6,101,182	08/2000	Sistanizadeh et al.	
	A8	6,199,112	03/2001	Wilson, Stephen K.	
	A9	6,202,081	03/2001	Naudus, Stanley **T**.	
	A10	6,298,341	10/2001	Mann et al.	
	A11	6,262,987	07/2001	Mogul, Jeffrey C.	
	A12	6,314,463	11/2001	Abbott et al.	
	A13	6,338,082	01/2002	Schneider, Eric	
	A14	6,502,135	12/2002	Munger et al.	
	A15	6,557,037	04/2003	Provino, Joseph E.	
	A16	6,687,746	02/2004	Shuster et al.	
	A17	6,757,740	06/2004	Parkh et al.	
	A18	7,039,713	05/2006	Van Gunter et al.	
	A19	7,167,904	01/2007	Devarajan et al.	
	A20	7,188,175	03/2007	McKeeth, James A.	
	A21	7,461,334	12/2008	Lu et al.	
	A22	7,490,151	02/2009	Munger et al.	
	A23	7,493,403	02/2009	Shull et al.	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B1	US2001/0049741	12/2001	Skene et al.	
	B2	US2004/0199493	10/2004	Ruiz et al.	
	B3	US2004/0199520	10/2004	Ruiz et al.	
	B4	US2004/0199608	10/2004	Rechterman et al.	
	B5	US2004/0199620	10/2004	Ruiz et al.	
	B6	US2007/0208869	09/2007	Adelman et al.	
	B7	US2007/0214284	09/2007	King et al.	
	B8	US2007/0266141	11/2007	Norton, Michael Anthony	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	11/679,416
Filing Date	02-27-2007
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	077580-0015

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B9	US2008/0235507	09/2008	Ishikawa et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
	C1	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp		English Abstract	
	C2	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp		English Abstract	
	C3	JP10-070531	03/10/1998	Brother Ind Ltd.		English Abstract	
	C4	JP62-214744	9/21/1987	Hitachi Ltd.		English Abstract	

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1	Yuan Dong Feng, "A novel scheme combining interleaving technique with cipher in Rayleigh fading channels," Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998)	
	D2	D.W. Davies and W.L. Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	

EXAMINER	DATE CONSIDERED
/Krisna Lim/	11/21/2010

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /K.L./

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	11/679,416
Filing Date	02-27-2007
First Named Inventor	Victor Larson
Art Unit	2453
Examiner Name	Krisna Lim
Docket Number	077580-0015

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 – Number 4 – Kind Code5 (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C1	EP0838930	4/29/1988	Digital Equipment Corporation			
	C2	EP0814589	12/29/1997	AT&T Corp.			
	C3	GB2317792	04/01/1998	Secure Computing Corporation			
	C4	WO98/27783	06/25/1998	Northern Telecom Limited			
	C5	WO99/11019	03/04/1999	V One Corp			
	C6	GB2334181	08/11/1999	NEC Technologies			
	C7	GB2340702	02/23/2000	Sun Microsystems Inc.			

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D1	Baumgartner et al, "Differentiated Services: A New Approach for Quality of Service in the Internet," International Conference on High Performance Networking, 255-273 (1998)	
	D2	Chapman et al., "Domain Name System (DNS)," 278-296 (1995)	
	D4	Davila et al., "Implementation of Virtual Private Networks at the Transport Layer," M. Mambo, Y. Zheng (Eds), Information Security (Second International) Workshop, ISW' 99. Lecture Notes in Computer Science (LNCS), Vol. 1729; 85-102 (1999)	
	D5	De Raadt et al., "Cryptography in OpenBSD," 10 pages (1999)	
	D6	Eastlake, "Domain Name System Security Extensions," Internet Citation, Retrieved from the Internet: URL:ftp://ftp.inet.no/pub/ietf/internet-drafts/draft-ietf-dnssec-secext2-05.txt (1998)	

/Krisna Lim/ 11/21/2010

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** ***(Use as many sheets as necessary)***				**Complete if Known**	
				Application Number	11/679,416
				Filing Date	02-27-2007
				First Named Inventor	Victor Larson
				Art Unit	2453
				Examiner Name	Krisna Lim
				Docket Number	077580-0015

	D8	Gunter et al., "An Architecture for Managing QoS-Enabled VRNs Over the Internet," Proceedings 24th Conference on Local Computer Networks. LCN' 99 IEEE Comput. Soc Los Alamitos, CA, pages 122-131 (1999)	
	D9	Shimizu, "Special Feature: Mastering the Internet with Windows 2000", Internet Magazine, 63:296-307 (2000)	
	D10	Stallings, "Cryptography and Network Security," Principals and Practice, 2nd Edition, pages 399-440 (1999)	
	D11	Takata, "U.S. Vendors Take Serious Action to Act Against Crackers – A Tracking Tool and a Highly Safe DNS Software are Released", Nikkei Communications, 257:87 (1997)	
	D12	Wells, Email (Lancasterb1be@mail.msn.com), Subject: "Security Icon," (1998)	

/Krisna Lim/ 11/21/2010

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

Courtesy Reminder for
Application Serial No: 11/679,416

Attorney Docket No: 77580-015
(VRNK-1CP2DVCN)
Customer Number: 23630
Date of Electronic Notification: 12/07/2010

This is a courtesy reminder that new correspondence is available for this application. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

mweipdocket@mwe.com

Please verify that these email addresses are correct.

To view your correspondence online or update your email addresses, please visit us anytime at **https://sportal.uspto.gov/secure/myportal/privatepair.** If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 836 306 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
15.04.1998 Bulletin 1998/16

(51) Int. Cl.[6]: **H04L 29/06**, H04Q 11/04

(21) Application number: **96410106.7**

(22) Date of filing: **10.10.1996**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV SI

(71) Applicant:
Hewlett-Packard Company
Palo Alto, California 94304 (US)

(72) Inventors:
- **Sasyan, Serge**
  38170 Seyssinet (FR)
- **Roger, Denis**
  38760 Varces (FR)
- **Terrasse, Denis**
  38320 Eybens (FR)

(74) Representative:
Squibbs, Robert Francis
Intellectual Property Section,
Legal Department,
Hewlett-Packard France,
Etablissements de Grenoble
F-38053 Grenoble Cédex 9 (FR)

Remarks:
The application is published incomplete as filed (Article 93 (2) EPC). A claim No.7 is missing.

(54) System providing for multiple virtual circuits between two network entities

(57) Computers sending IP datagrams over an ATM network are generally capable of operating multiple simultaneous virtual circuits over the network. However, in doing so, they normally only set up one virtual circuit to each destination IP address so that in order to test the simultaneous operation of N virtual circuits by a computer under test, N target computers are needed. To enable a single computer (T) to provide the destination endpoints for multiple virtual circuits (SVC) from a computer (M) under test, both computers (M,T) are allocated a plurality of virtual IP addresses ($I_{M(j)}$,$I_{T(i)}$) and the target computer (T) is additionally provided with a module running address-changing processes (70,71) that avoids the IP layers (20) of both computers from rejecting IP datagrams (25A,25B) addressed with the virtual IP addresses. As a result, each computer (M,T) can be addressed with any of a plurality of IP addresses and each will result in the creation of a respective virtual circuit (SVC) between the computers (M,T).

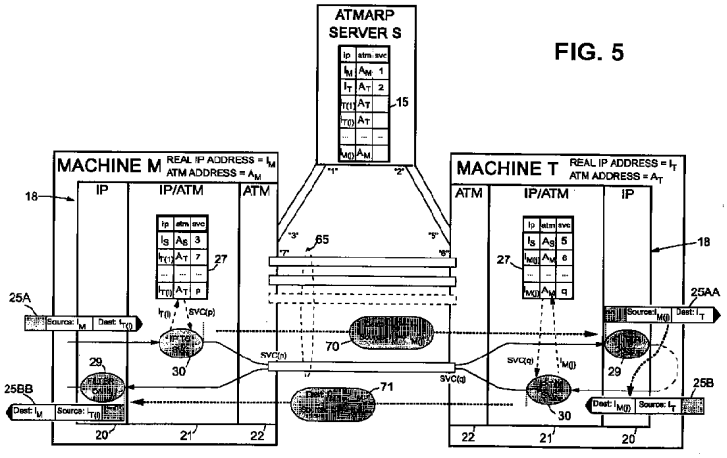


FIG. 5

EP 0 836 306 A1

Petitioner Apple Inc. - Exhibit 1026, p. 1062

Description

Field of the Invention

The present invention relates to a system providing for multiple virtual circuits between two network entities for use in particular, but not exclusively, in the testing of network node apparatus providing IP messaging over an ATM network.

Background of the Invention

As is well-known, the Internet Protocol (IP) uses a scheme of IP addresses by which every connection of a node to the Internet has a unique IP address. IP addresses are high-level addresses in the sense that they are independent of the technology used for the underlying network to which a node is connected. Each node will also have a low-level, network-dependent address (often callled the MAC address) that is actually used for addressing at the network level and the IP protocol suite includes a address reolution protocol (ARP), logically positioned below the IP layer itself, that is responsible for translating between IP addresses contained in a message and the local MAC addresses.

An increasingly important technology for local area networks is ATM. ATM (Asynchronous Transfer Mode) is a multiplexing and switching technique for transferring data across a network using fixed sized cells that are synchronous in the sense that they appear strictly periodically on the physical medium. Each cell comprises a payload portion and a header, the latter including a label that associates the cell with an instance of communication between sending and receiving network end systems; this instance of communication may involve the transfer of many cells from the sending end system, possibly to multiple receiving end systems. ATM is asynchronous in the sense that cells belonging to the same instance of communication will not necessarily appear at periodic intervals.

In ATM, the labels appended to the cells are fixed-size context dependent labels, that is, they are only understandable in the light of context information already established at the interpreting network node, the label generally being replaced at one node by the label required for the next node. In other words, ATM is a virtual circuit technology requiring a set up phase for each instance of communication to establish the appropriate label knowledge at each node. Of course, to set up a desired communication, it is still necessary to identify uniquely the nodes forming the communication end points and this is achieved by using ATM addresses, generally of a significance limited to the particular ATM network concerned.

The process of sending IP messages (datagrams) over a ATM network, including the operation of the required ATM ARP system, is set out in RFC 1577 of the IETF Internet Engineering Task Force) dated January 1993. This RFC assumes an arrangement in which a sending node will only establish a single vircuit circuit to a given destination IP address (of course, this one vircuit circuit may carry multiple connections between respective pairings of high-level end points in the nodes).

Figure 1 of the accompanying drawings is a diagram illustrating the basic mechanism by which two machines M and T exchange IP datagrams over a switched virtual circuit (SVC) established across an ATM network. The machines M and T have respective IP addresses I_M and I_T and respective ATM addresses A_M and A_T; each machine knows its own addresses. An ATMARP server S knows the IP and ATM addresses of all active nodes on the network, including machines M and T; more particularly, server S maintains an ARP table 15 associating the IP address of each node with its ATM address. The server S maintains open a respective SVC (switched virtual circuit) to each active node and the identity of this SVC is held in the ARP table 15; thus, in the Figure 1 example, the server S is in communication with machine M over an SVC identified as SVC "1" at the server, and the server S is in communication with machine T over an SVC identified as SVC "2" at the server S. At machines M and T these virtual circuits are independently identified - thus at machine M its SVC to the server S is identified as SVC "3" whilst at machine T its SVC to the server S is identified as SVC "5".

The communications interface 18 in each of the machines M and T comprises three main layers, namely: an IP layer 20 responsible for forming IP datagrams (including source and destination IP addresses) for transmission ad for filtering incoming datagrams; an intermediate IP/ATM layer 21 for determining the SVC corresponding to the destination IP address of an outgoing datagram; and an ATM layer 22, including the low-level network interface hardware, for sending and receiving datagrams packaged in ATM cells over SVCs.

The IP/ATMlayer 21 maintains an ARP cache table 27 which like the table 15 of the server S contains associations between IP address, ATM address and SVC. Thus, table 27 of machine M contains an entry of the IP address I_S, ATM address A_S, and SVC identity "3" for the server S, and similarly, table 27 of machine T contains an entry of the IP address I_S, ATM address A_S, and SVC identity "5" for the server S. The cache table 27 only holds information relevant to current SVCs of the machine concerned so that during the initial establishment of a SVC to a new destination, the cache table must be updated with relevant information from the ATMARP server S; this general process will be described in more detail hereinafter with reference to Figure 2. For the present, it will be assumed that an SVC has already been established between machines M and T and that the cache tables contain the relevant information (in particular, cache table 27 of machine M contains an entry with the IP address I_T, ATM address A_T, and SVC identity "4" for machine T, and cache table

Petitioner Apple Inc. - Exhibit 1026, p. 1063

27 of machine T contains an entry with the IP address I_M, ATM address A_M, and SVC identity "9" for machine M).

Considering now the case of a high-level application in machine M wanting to send a message to machine T, this application passes the message to the IP layer 20 together with the destination IP address I_T. IP layer 20 packages the message in one (or more) datagrams 25A with a destination IP address of I_T and source I_P address of I_M. Datagram 25A is then passed to the IP/ATM layer 21 which executes an IP-to-SVC lookup task 30 to determine from table 27 the SVC to be used for sending the datagram to its destination address I_T; in the present case, table 27 returns the SVC identity "4" and the layer 21 passes this identity together with the datagram 25A to the ATM layer 22 which then sends the datagram in ATM cells on SVC "4". The datagram is in due course received by machine T and passed up by layers 22 and 21 to the IP layer 20 where a filtering task 29 determines from the datagram destination address that the datagram is indeed intended for machine T; the contents of the datagram are then passed to the relevant high-level application. In the present example, this high-level application produces a reply message which it passes to the IP layer 20 together with the required return address, namely the source IP address in the received datagram 25A. IP layer 20 generates datagram 25B with the received return address as the destination address, the IP address I_T of machine T being included as the source address. The datagram 25B is passed to IP/ATM layer 21 where IP-to-SVC lookup task 30 determines from cache table 27 that the required destination can be reached over SVC "9". This information together with datagram 25B is then passed to ATM layer 22 which transmits the datagram in ATM cells over SVC "9" to machine M. When the datagram is received at machine M it is passed up to the IP layer 20 where it is filtered by task 29 and its contents then passed on to the relevant high-level application.

Figure 2 of the accompanying drawings illustrates in more detail the functioning of the IP/ATM layers 21 of machines M and T in respect of datagram transmission from machine M to machine T, it being appreciated that the roles of the two layers 21 are reversed for transmission in the opposite direction. More particularly, upon the IP-to-SVC lookup task 30 being requested to send a datagram to IP address I_T, it first carries out a check of the cache table 27 (step 31) to determine if there is an existing entry for I_T (and thus an SVC, assuming that entries are only maintained whilst an SVC exists). Step 32 checks the result of this lookup - if an SVC already exists (in this case, SVC "4"), then step 39 is executed in which the datagram is passed together with the identity of the relevant SVC to the ATM layer 22; however, if the lookup was unsuccessful, task 30 executes steps 33 to 38 to set up an SVC to destination I_T before executing step 39.

The first step 33 of the setup process involves the sending of an ARP request to the ATMARP server S over the relevant SVC requesting the ATM address corresponding to I_T. Server responds with ATM address A_T which is received by task 30 at step 34.

Task 30 now updates the cache table 27 with the IP address I_T and ATM address A_T (step 35). Next, task 30 requests (step 36) the ATM layer 22 to establish a new SVC to ATM address A_T and this initiates an SVC setup process 28 which may be executed in any appropriate manner and will not be described in detail herein. In due course, process 28 returns the identity of the SVC that has been set up to A_T (in this case, SVC "4"), this identity being received at step 37 of task 30. Finally, cache table 30 is updated at step 38 by adding the SVC identity ("4") to the entry already containing I_T and A_T.

In machine T, the setup of the new SVC to the machine from machine M is handled by the setup process 28 of machine T. The process 28 informs the IP/ATM layer that a new SVC has been setup and this triggers execution of an update task 40 to update the cache table 27 of machine T. More particularly, on the new SVC indication being received (step 41), a first update step 42 is carried out to add an entry to the table confining the identity of the new SVC (in the present example "9"), and the ATM address A_M of the node at the other end of the SVC; at this stage, the corresponding IP address is not known to machine T. In order to obtain this IP address, an inverse ARP request is now made to machine M (step 43). In due course a response is received (step 44) containing the IP address of machine M. The cache table 27 is then updated at step 45 with the IP address I_M of machine M and the IP/ATM layer is now ready to effect IP-to-SVC translations for datagrams intended for machine M.

The inverse ARP request sent by machine T to machine M is handled by an inverse ARP task 50 that examines the request (step 51) and on finding that it contains the ATM address A_M, responds with the IP address I_M of machine M (step 52).

To facilitate explanation of the preferred embodiment of the invention hereinafter, the messages across the boundary between the IP/ATM layer 21 and the ATM layer 22 have been labelled in Figure 2 as follows where superscript "T" indicates an outgoing message (that is, from the IP/ATM layer to the ATM layer) and the superscript "R" indicates incoming messages (that is, from the ATM layer to the IP/ATM layer):

- $X1^T$ - outgoing ARP request;
- $X2^R$ - incoming ARP response;
- $X3^T$ - outgoing SVC setup request;
- $X4^R$ - incoming SVC setup done indication;
- $X5^R$ - incoming new SVC indication;
- $X6^T$ - outgoing INARP request;
- $X6^R$ - incoming INARP request;
- $X7^T$ - outgoing INARP response;
- $X8^T$ - outgoing datagram;
- $X8^R$ - incoming datagram.

Petitioner Apple Inc. - Exhibit 1026, p. 1064

It will be appreciated that machines connecting to an ATM network, such as machines M and T as well as the server S, are designed to handle a large number of virtual circuits simultanteously. If in testing such a machine (machine M in the following discussion) it is desired to fully stress the machine under test, then the design limit of concurrently operating virtual circuits must be simultaneously used. However, as already indicated, current practice is that only one virtual circuit is established to each distinct IP address. As a result, since generally each machine that might be used to test machine M has only one network connection and therefore only one IP address, if machine M is designed to operate up to N virtual circuits simultaneously, then it requires N machines to test machine M. Such an arrangement is illustrated in Figure 3 where the N machines are constituted by the server S and (N-1) other machines here represented as machines T1 to T(N-1). Such an arrangement is generally impractical as N may be as high as 1024 or more.

It is an object of the present invention to provide a mechanism that enables, inter alia, the foregoing test problem to be overcome.

Summary of the Invention

According to the present invention, there is provided a system in which a plurality of entities are connected to a network ad can exchange messages across virtual circuits set up over the network between said entities, each entity having a operative high-level address on the network, and each entity comprising:

-- high-level messaging means for handling message transmission and receipt on the basis of the aforesaid high-level addresses, the high-level messaging means comprising means for including in outgoing messages the operative high-level address of the entity as a source identifier and the operative high level address of the intended recipient entity as a destination identifier, and means for filtering incoming messages according to the destination identifier contained in the message:

-- virtual-circuit means for providing virtual circuits between the entity and other entities, there being a respective virtual circuit for each different destination identifier in use, and

-- intermediate means for passing an outgoing message from the high-level messaging means to that one of the virtual circuits provided by the virtual-circuit means which corresponds to the destination identifier of the message;

characterised in that each of a first and a second one of the entities has a plurality of virtual high-level addresses associated with it that are different from the operative high-level address of the entity, the virtual high-level addresses being usable by the messaging means of the first and second entities as destination identifiers in outgoing messages; **and in that** between the intermediate means of the first and second entities, there are provided address-changing means responsive to each of at least some of the messages sent between these entities with a said virtual high-level address as its destination identifier, to change that address to the operative high-level address of the corresponding entity and to change the operative high-level address provided as the source identifier of the message into one of the said virtual high-level addresses associated with the sending entity in dependence on the virtual high-level address initially provided as the destination identifier of the same message.

By virtue of this arrangement, it is possible to establish a plurality of virtual circuits between the first and second entities by using the different virtual high-level addresses of the entities as the destination identifiers in messages exchanged between the entities, the receiving high-level adressing means accepting such messages due to the address-changing means having changed the destination identifier to the operative high-level address of the receiving entity. By also changing the source identifier, it is possible to retain in the message information sufficient to associate any reply message with a particular one of the virtual circuits established with the sending entity (in particular, the reply message can be sent back over the same virtual circuit as the message to which it is a reply - however, if desired, it is also possible to use a separate virtual circuit for the reply messages).

Preferably, the address-changing means comprises first address-changing functionality for effecting the aforesaid changes for messages sent from the first entity to the second entity, and second address-changing functionality for effecting these changes for messages sent from the second entity to the first entity, both the first and second address-changing functionalities being provided in the second entity. This configuration is well suited for testing the ability of network node apparatus to concurrently operate a plurality of virtual circuits where the network node apparatus is operative to establish a virtual circuit for each different high-level destination address being handled; more particularly, the network node apparatus serves as the aforesaid first entity, and is caused to send messages to at least some of the vial high-level addresses associated with the second entity. By placing the address-changing means in the second entity, no modifications are needed to the network node apparatus in order for it to be able to establish a plularity of virtual circuits with the second entity.

Advantageously, the address-changing means effects a predetermined transformation on the virtual high-level address forming the initial destination identifier of a said message in order to form the virtual high-level address to be used for the source identifier of that message. For example, this transformation may simply

Petitioner Apple Inc. - Exhibit 1026, p. 1065

involved changing the address by one (where the address is numeric in form).

The present invention is particularly applicable to systems in which the high-level addresses are IP addresses and the network is an ATM network.

Brief Description of the Drawings

A system embodying the invention will now be described, by way of non-limiting example, with reference to the accompanying diagrammatic drawings, in which:

- **Figure 1** is a diagram of a known system for sending IP datagrams over a ATM network between two machines M and T;
- **Figure 2** is a diagram illustrating the steps carried out by the Figure 1 system in establishing a virtual circuit between machines M and T;
- **Figure 3** is a diagram of a known test arrangement for testing the ability of a machine M to concurrently operate multiple virtual circuits;
- **Figure 4** is a diagram showing a test arrangement embodying the invention for testing the ability of a machine M to concurrently operate multiple virtual circuits;
- **Figure 5** is a diagram similar to Figure 1 but showing a system embodying the invention in which multiple virtual circuits are established between machines M and T;
- **Figure 6** is a diagram illustrating the processing effected by a module VNS disposed in machine T of the Figure 5 system when machine M initiates the opening of a new virtual circuit between machines M and T; and
- **Figure 7** is a diagram illustrating the processing effected by a module VNS disposed in machine T of the Figure 5 system when machine T initiates the opening of a new virtual circuit between machines M and T.

Best Mode of Carrying Out the Invention

The embodiment of the invention now to be described provides a system in which it is possible to establish a plurality of SVCs (switched virtual circuits) across an ATM network for the exchange of IP datagrams between two machines M and T whereby it is possible to test the ability of machine M to concurrently operate a plurality of virtual circuits without needing to provide a respective destination machine for each SVC operated by machine M. The overall test arrangement is illustrated in Figure 4 where machine M operates N SVCs over ATM network 10, one SVC being with ATMARP server S and (N-1) SVCs being with machine T. According to the preferred embodiment, the establishment of multiple concurrent SVCs between machine M and T is effected without modification to machine M.

Figure 5 shows a system embodying the present invention, this system being similar to that of Figure 1 but being operative to provide a plurality of concurrent SVCs 65 between machines M and T. In the Figure 5 system, the machines M and T and the server S are assumed to operate in the same way and have the same IP and ATM addresses as in Figure 1; in addition, in Figure 5 the same SVCs are established between the server S and the machines M and T as in Figure 1. The Figure 5 system includes, however, added functionality provided by processes 70 and 71 which in Figure 5 are shown independent of machines M and T but in practice would be provided either distributed between machines M and T or wholly in one of these machines; in a preferred embodiment, the processes 70 and 71 are provided in machine T.

In accordance with the present invention, each machine M and T is allocated a number of virtual IP addresses different from its operative (or "real") IP address (this latter address being the one which the IP layer knows about for inclusion as the source address in outgoing datagrams and upon which filtering is carried out by task 29). Thus, machine M is allocated virtual IP addresses $I_{M(1)}$, $I_{M(2)}$,.....$I_{M(j)}$...; similarly, machine T is allocated virtual IP addresses $I_{T(1)}$, $I_{T(2)}$,.....$I_{T(i)}$....

Each of these virtual IP addresses is entered into table 15 of ATMARP server S together with the ATM address of the corresponding one of the machines M,T; thus virtual IP address $I_{M(j)}$ is associated with ATM address A_M and virtual IP address $I_{T(i)}$ is associated with ATM address A_T.

Now, if the communications interface 18 of machine M is asked to send a message to IP address $I_{T(i)}$, IP layer 20 will construct a datagram 25A having a destination address of $I_{T(i)}$ and a source address of I_M. The IP-to-SVC task 30 of IP/ATM layer 21 then acts in the manner already described to fetch the ATM address corresponding to $I_{T(i)}$ from server S and set up an SVC (here identified by "p") towards machine T; the cache table 27 is updated appropriately. The datagram 25A is now sent by ATM layer over SVC(p) to machine T.

If no further action is taken, the datagram 25A, after receipt at machine T, will be rejected by the filter task 29 as the destination address $I_{T(i)}$ of the datagram differs from the operative IP address I_T known to task 29 of machine T. Accordingly, a process 70 is provided that recognises the destination address of datagram 25A as being a virtual IP address of machine T and substitutes the real IP address of machine T for the virtual address in the destination field of the datagram 25A. The datagram will now be allowed through by filter task 29 of machine T.

However, a further difficultly remains. If only the destination address is changed, the resultant datagram contains no indication that the datagram was not ordi-

Petitioner Apple Inc. - Exhibit 1026, p. 1066

narily sent with the real IP address of machine T; any reply will therefore be sent on an SVC set up to take datagrams from machine M to the real IP address of machine M. This SVC would end up taking all the reply messages for messages sent from machine M to machine T over all the SVCs set up in respect of the virtual IP addresses allocated to machine T. This is clearly undesirable. To avoid this, the source address of datagram 25A is also changed by process 70. More particularly, the source address is changed from the real IP address of machine M to one of the virtual IP addresses $I_{M(j)}$ of this machine, the virtual address chosen being dependent on the original virtual IP address forming the destination address of the datagram. As a result, all datagrams 25A having the same virtual destination address end up after operation of process 70 as datagrams 25AA with the same virtual source address, whereas datagrams 25A having different initial virtual destination addresses end up as datagrams 25AA with different source addresses. The process of changing the source address preferably involves a predetermined transformation of the virtual destination address - for example, to obtain the required virtual source address, the virtual destination address can simply be incremented by one (there would thus exist, for example, a set of even virtual IP addresses for machine M and a corresponding set of odd virtual IP addresses for machine T, each even virtual IP address of machine M being associated with the immediately adjacent, lower-valued, odd virtual IP address of machine T).

The address-changing process 70 must be carried out on datagram 25A after operation of the IP-to-SVC task 30 in machine M and prior to the filter task 29 in machine T. In addition, whilst the two address-hanging operations of process 70 need not be carried out at the same time or at the same location (though it is, of course, convenient to do so), the changing of the source address must be done whilst the initial virtual destination address is still available.

The contents of datagram 25AA are passed by IP layer 20 of machine T to a high-level application which, in the present example, produces a reply that it passes to layer 20 for sending back to IP address $I_{M(j)}$, that is, to the source address contained in datagram 25AA. Layer 20 produces a datagram 25B with source address I_T and destination address $I_{M(j)}$. Next, IP-to-SVC task 30 of layer 21 looks up the destination address in the cache table 27 to find out the SVC to be used for the reply. If, as will normally be the case, the same SVC is to be used for the reply as carried the original datagram 25A with destination address $I_{T(i)}$, then the SVC setup process will have been arranged to enter the address $I_{M(j)}$ in cache table 27 against that SVC (in present case, identified to machine T by "q"); a lookup on $I_{M(j)}$ will thus return "q" as the required SVC. However, if it is desired to use a different SVC for datagrams 25B passing from T to M as used for datagrams 25A passing from M to T, then the first lookup on $I_{M(j)}$ by task 30 will not identify an SVC and task 30 must then initiate set up of a new SVC.

Assuming that the same SVC is to be used for the datagrams 25B with destination address $I_{M(j)}$ as for the datagrams 25A with destination address $I_{T(i)}$, then alter task 30 has identified SVC(q) as the appropriate SVC, the datagram 25B is passed to the ATM layer 22 for sending out over SVC(q). In due course, machine M receives this datagram and passes it up to IP layer 20; however, before the datagram reaches this layer, it must undergo address-change processing similar to that carried out on datagram 25A. More particularly, the virtual destination address $I_{M(j)}$ must be changed to the real IP address I_M of machine M, and the real source address I_T of machine T must be changed to the virtual IP address $I_{T(i)}$ of machine T associated with the virtual destination address $I_{M(j)}$. This address-change processing is carried out by process 71.

With regard to the source address change, where the corresponding change was effected for datagram 25A by incrementing by one the virtual destination address $I_{T(i)}$ of that datagram, then for datagram 25B, the source address is changed to the destination address $I_{M(j)}$ decremented by one.

In a similar manner to process 70, process 71 must be carried out on datagram 25B after operation of the IP-to-SVC task 30 in machine T and prior to the filter task 29 in machine M. In addition, whilst the two address-changing operations of process 71 need not be carried out at the same time or at the same location, the changing of the source address must be done whilst the initial virtual destination address is still available.

Following operation of process 71, datagram 25BB with source address $I_{T(i)}$ and destination address I_M is allowed through by filter task 29 and the contents of the datagram are passed to the relevant high-level application.

Having described the general mechanism by which virtual IP addresses can be used for exchanging datagrams 25A and 25B across a SVC between machines M and T, the issue will now be addressed as to how the cache table 27 in machine T is updated on SVC setup to associate the new SVC (that is, SVC(q) at machine T) with the virtual IP address $I_{M(j)}$ of machine M (this is required where the same SVC is to be used for the reply datagram 25B as for the original datagram 25A). It will be appreciated that when the task 40 (see Figure 2) is executed, the INARP request sent to machine M will only return the real IP address I_M of machine M, there being no other information available to the update task 40 by which any other result could be obtained from the INARP task 50; clearly, something additonal needs to be done for update task 40 to be able to associate the virtual IP address $I_{M(j)}$ with the newly created SVC(q) in table 27. In fact, there are a number of ways in which the update task could be informed that the IP address to be associated with SVC(q) is $I_{M(j)}$. For example, the update task 40 could be arranged to send a request back over the newly-created SVC(q) asking machine M to identify

Petitioner Apple Inc. - Exhibit 1026, p. 1067

the destination IP address $I_{T(i)}$ it associates with that SVC; from this information, the update task could determine the associated virtual IP address $I_{M(j)}$ of machine M (assuming there is a predetermined relation between the two as is the case in the described embodiment) and then update table 27 accordingly. An alternative approach that avoids sending a special request to machine M is to wait for machine M to supply the destination IP address $I_{T(i)}$ in the first IP datagram 25A sent over the new SVC(q), the update task then deriving the required address $I_{M(j)}$ as described above.

A variant of this latter approach is to leave the update task 40 unchanged but provide an additional process that:

(a) delays the INARP request until the destination address $I_{T(i)}$ of the first datagram from machine M to machine T can be captured;
(b) uses the captured address $I_{T(i)}$ as the source address of the INARP request that is now sent on to machine M.

The INARP response from machine M will therefore have a destination address $I_{T(i)}$ and a source address (that forms the substance of the INARP response) of I_M. By ensuring that this response datagram is subject to the processing effected by process 70, the source data in the INARP response will be changed to $I_{M(j)}$ by the time the response reaches the update task 40. Thus, the required updating of the table 27 of machine T can be achieved without modification to the existing tasks of machines M and T but simply by the addition of a further process for effecting steps (a) and (b) described above. This approach is the preferred one for updating table 27 and is the one used in the module described below with reference to Figures 6 and 7.

The above-described system involving the allocation of multiple virtual IP addresses to machines M and T and the provision of the address-changing processes 70 and 71, permits multiple SVCs to be concurrently operated between the machines M and T thereby enabling implementation of the test arrangement depicted in Figure 4. Of course, when testing the machine M, it is desirable that no changes are made to this machine; accordingly, it is preferred for such a test arrangement to implement the address-changing processes 70 and 71 in machine T.

The implementation of the address-changing processes 70 and 71, and of the INARP request modification process, can conveniently by done by inserting a module (hereinafter called the VNS module) between the IP/ATM layer 21 and the ATM layer 22 of machine T; in fact, an instance of this module is created for each SVC, this being relatively easy to implement when using a STREAMS type I/O implementation as provided in most UNIX systems (conveniently one stream is provided for each SVC and the VNS module is pushed onto each stream when the stream is created).

The messages passing across the boundary between layers 21 and 22 have already been described above with reference to Figure 2 and the processing effected by the VNS module on each of these messages will next be described. First, the situation of Figure 5 will be considered where it is machine M that initiates the setting up of a new SVC to machine T. The first message received by the VNS module will be the SVC setup indication message $X5^R$ and this is passed through the VNS module without modification (see Figure 6). Next, the INARP request $X6^T$ is received and is subject to the modification process 82 described above, namely it is delayed until the first IP datagram 25A is received and the address $I_{T(i)}$ extracted and used for the source address of the INARP request. The INARP response $X7^R$ is then received and subject to the address-changing process 70.IP datagrams $X8^R$ from machine M to machine T are also subject to the address-changing process 70. IP datagrams $X8^T$ from machine T to machine M are subject to address-changing process 71.

Figure 7 depicts the processing effected by the VNS module in the situation where it is the machine T rather than the machine M that initiates SVC setup. The messages passing through the VNS module in this case are those shown crossing the boundary between layers 21 and 22 in Figure 2 for machine M. The first four messages $X1^T$, $X3^T$, $X2^R$, and $X4^R$ are passed through without modification. The INARP request received from machine M is subject to the modification process 82, being delayed until the destination address of the first IP datagram from machine T to machine M can be captured and used as the source address of the INARP request. The INARP response $X7^T$ is subjected to process 71 as are IP datagrams $X8^T$ from machine T to machine M. IP datagrams $X8^R$ from machine M to machine T are subjected to process 70.

It will be appreciated that many variants are possible to the above-described embodiment of the invention. It will also be appreciated that the invention is not limited to switched virtual circuits but can equally be applied to permanent virtual circuits. Furthermore, the setting up of multiple virtual circuits between two machines can be used not only for implementing the test arrangement described above with reference to Figure 4 but also for other purposes.

Although the present invention has been described in the context of high-level addresses constituted by IP addresses and virtual circuits set up across an ATM network, the invention can be applied to other types high-level addresses and other types of virtual-circuit network. For example, the high-level addresses could be MAC addresses in the case of a network in the form of a emulated LAN (ELAN) over an ATM network.

Claims

1. A system in which a plurality of entities are con-

Petitioner Apple Inc. - Exhibit 1026, p. 1068

nected to a network and can exchange messages across virtual circuits set up over the network between said entities, each entity having an operative high-level address on the network, and each said entity comprising:

-- high-level messaging means for handling message transmission and receipt on the basis of said high-level addresses, said high-level messaging means comprising means for including in outgoing ones of said messages the operative high-level address of the entity as a source identifier and the operative high level address of the intended recipient entity as a destination identifier, and means for filtering incoming ones of said messages according to the destination identifier contained in the message:
-- virtual-circuit means for providing virtual circuits between the entity and other said entities, there being a respective virtual circuit for each different destination identifier in use, and
-- intermediate means for passing an outgoing message from said high-level messaging means to that one of the virtual circuits provided by the virtual-circuit means which corresponds to the destination identifier of the message;

characterised in that each of a first and a second said entity has a plurality of virtual high-level addresses associated with it that are different from said operative high-level address of the entity, said virtual high-level addresses being usable by the messaging means of said first and second entities as destination identifiers in outgoing messages; **and in that** between said intermediate means of said first and second entities, there are provided address-changing means responsive to each of at least some of said messages sent between these entities with a said virtual high-level address as its destination identifier to change that address to the said operative high-level address of the corresponding entity, and to change the operative high-level address provided as the source identifier of the message into one of the said virtual high-level addresses associated with the sending entity in dependence on the virtual high-level address initially provided as the destination identifier of the same message.

2. A system according to claim 1, wherein said address-changing means effects a predetermined transformation on the virtual high-level address forming the initial destination identifier of a said message to which the address-hanging means is responsive in order to form the virtual high-level address to be used for the source identifier of that message.

3. A system according to claim 2, wherein said address-changing means is responsive to messages sent in both directions between said first and second entities with virtual high-level addresses as destination identifiers, the said transformation effected in respect of such messages sent in one said direction being the reverse of the transformation effected in respect of other such messages sent in the opposite said direction.

4. A system according to claim 1, wherein said address-changing means comprises first address-changing functionality for effecting said changes for messages sent from said first entity to said second entity, and second address-changing functionality for effecting said changes for messages sent from said second entity to said first entity, both said first and second address-changing functionalities being provided in said second entity.

5. A system according to claim 1, wherein said address-changing means comprises first address-changing functionality for effecting said changes for messages sent from said first entity to said second entity, and second address-changing functionality for effecting said changes for messages sent from said second entity to said first entity, the two said address-changing functionalities being provided in respective ones of said first and second entities.

6. A system according to claim 1, wherein:

-- each said entity has a low-level address on the network;
-- said intermediate means of each entity further comprises:

-- first association means for providing an association between the destination identifier of a outgoing message and the low-level address of the corresponding said entity,
-- second association means for providing an association between the destination identifier of an outgoing message and a said virtual circuit,

said intermediate means using its second association means to identify from the destination identifier of a said outgoing message which virtual circuit is to be passed the message where such virtual circuit exists, and otherwise first passing a request to the said virtual circuit means of the same entity to establish a virtual circuit to the entity having the low-level address identified by said first association means as

Petitioner Apple Inc. - Exhibit 1026, p. 1069

associated with the destination identifier of the outgoing message; and

-- the said virtual-circuit means of each entity includes setup means responsive to a said request from the intermediate means of the same entity to establish a virtual circuit to the said entity having the low-level address provided in said request, said setup means causing the intermediate means to update its second association means to associate the newly-established virtual circuit with the said destination identifier relevant to said request;

the first association means of each of said first and second entities serving to provide an association between the virtual high-level addresses of the other of said first and second entities and the low-level address of that other entity.

8. A system according to claim 7, further comprising a network server containing associations between high-level addresses and low-level addresses, said first association means of each said entity comprising means for interrogating said network server for a required association.

9. A system according to claim 7, wherein said second association means comprises cache means for temporarily holding said associations between said destination identifiers and currently corresponding virtual circuits.

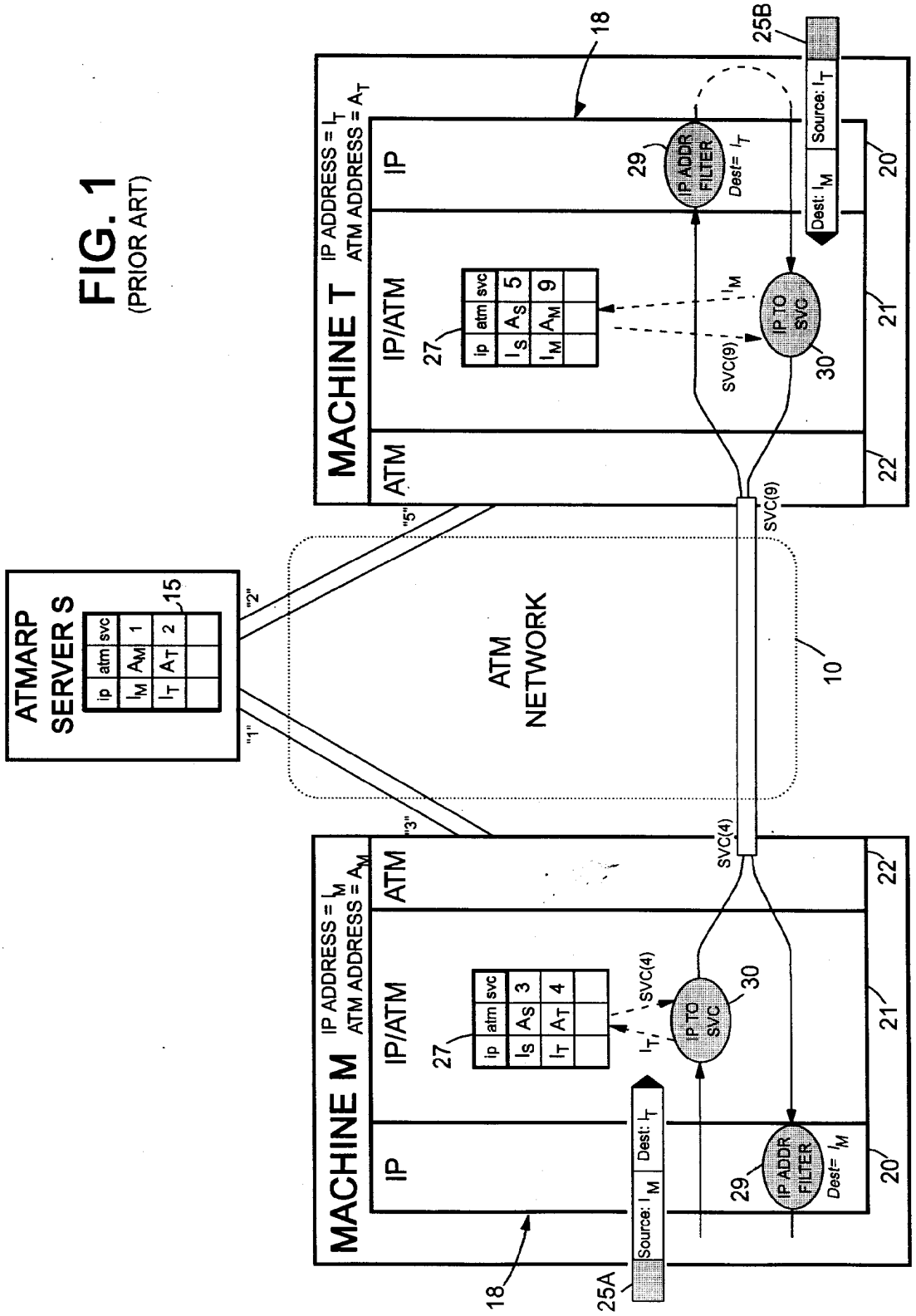
10. A system according to any one of claims 1 to 9, wherein said high-level addresses are IP addresses and said network is a ATM network.

11. A system according to any one of claims 1 to 9, wherein said high-level addresses are MAC addresses and said network is a emulated LAN over an ATM network.

12. A method of testing the ability of network node apparatus to operate a plurality of virtual circuits at the same time, said network node apparatus being arranged to establish a virtual circuit for each different high-level destination address being handled, said method involving setting up a system according to claim 4 with said network node apparatus as said first entity, and causing the network node apparatus to send messages to at least some of said virtual high-level addresses associated with said second entity.

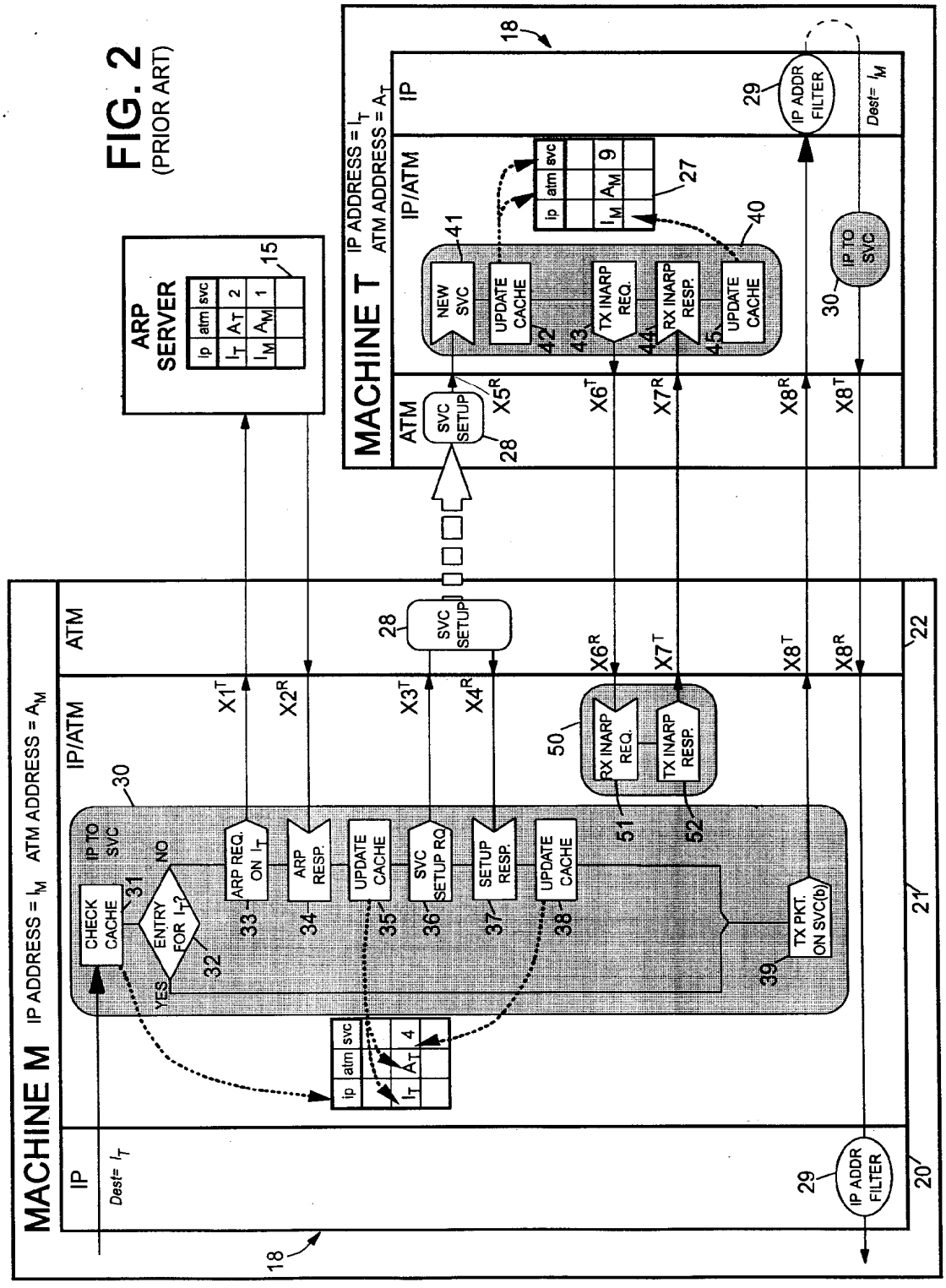
Petitioner Apple Inc. - Exhibit 1026, p. 1070

FIG. 1
(PRIOR ART)



Petitioner Apple Inc. - Exhibit 1026, p. 1071

FIG. 2
(PRIOR ART)



Petitioner Apple Inc. - Exhibit 1026, p. 1072

FIG. 3
(PRIOR ART)

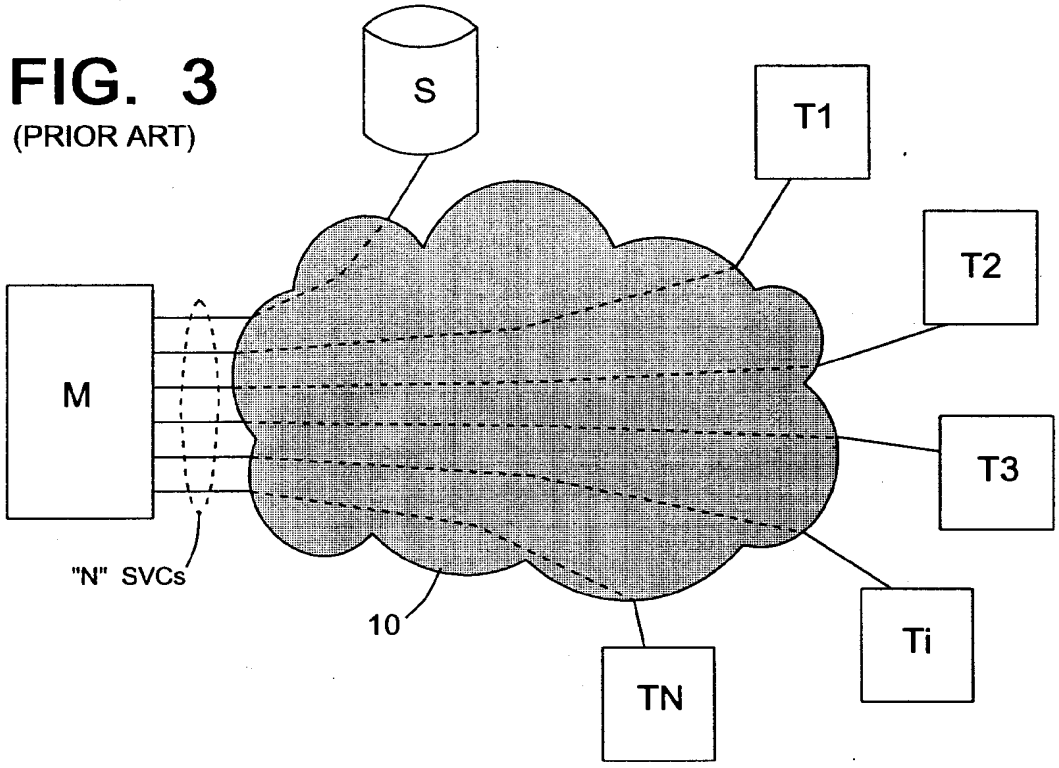
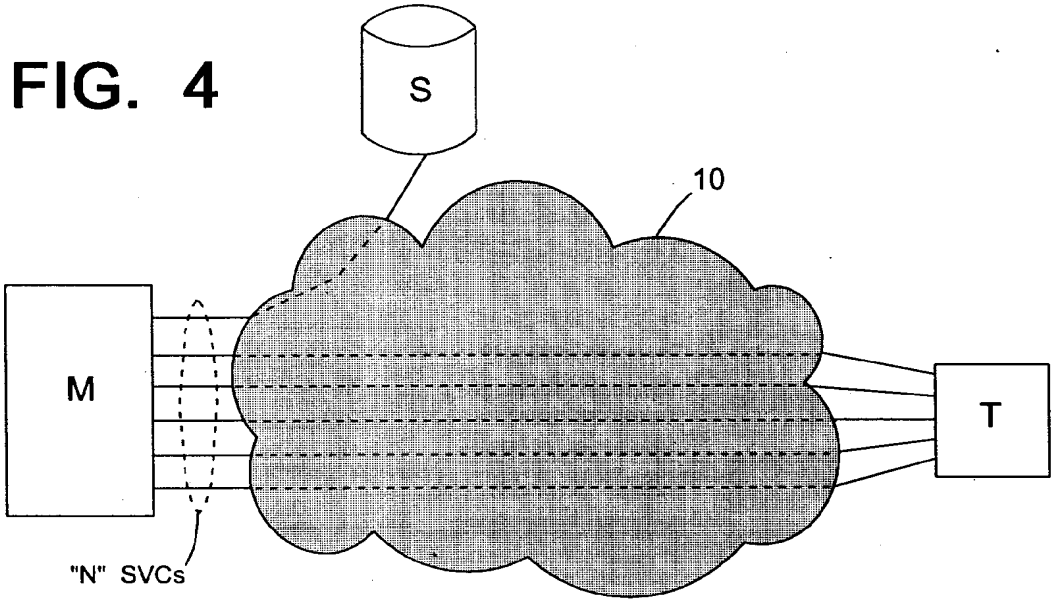
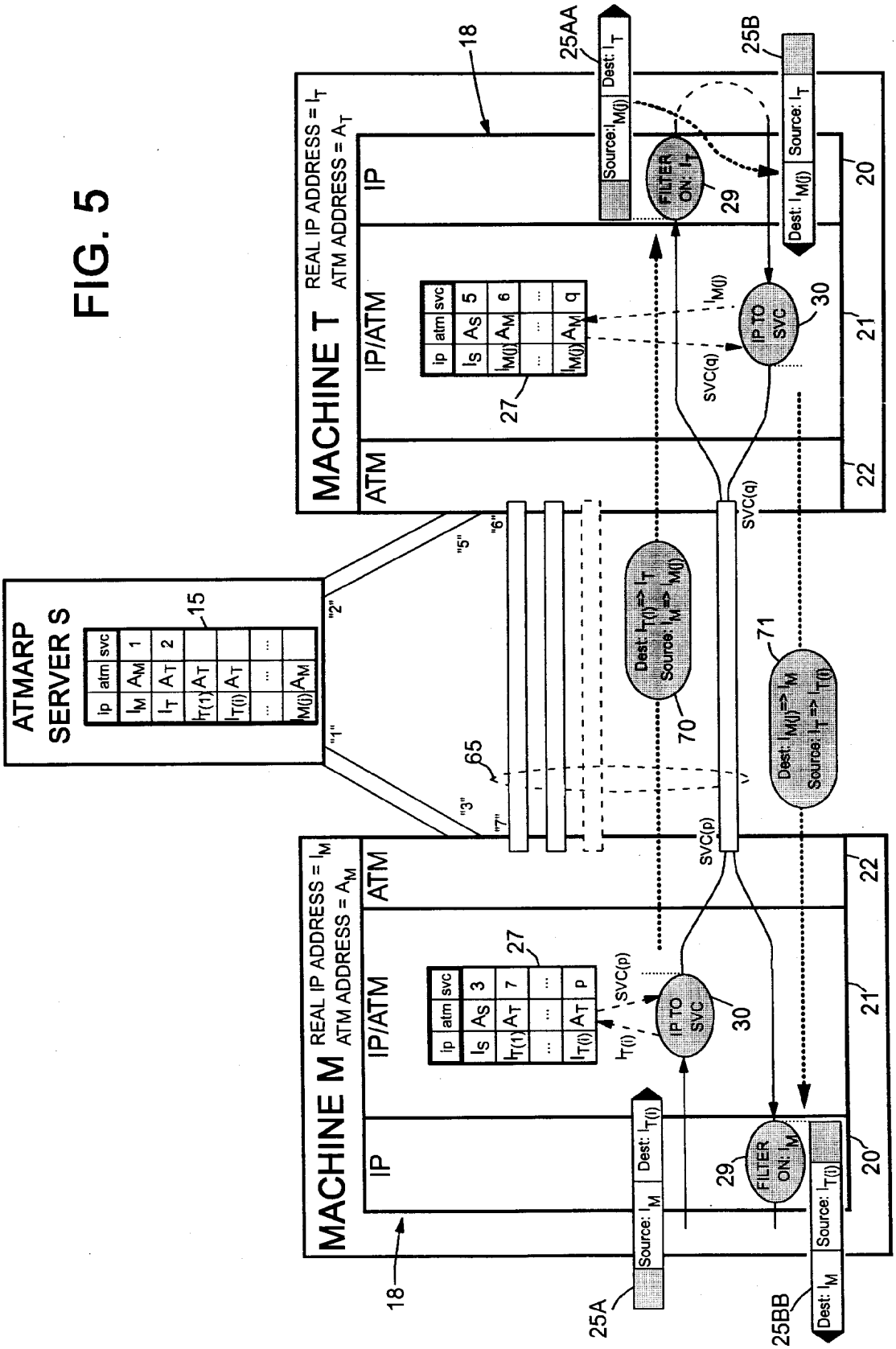


FIG. 4



Petitioner Apple Inc. - Exhibit 1026, p. 1073

FIG. 5



Petitioner Apple Inc. - Exhibit 1026, p. 1074

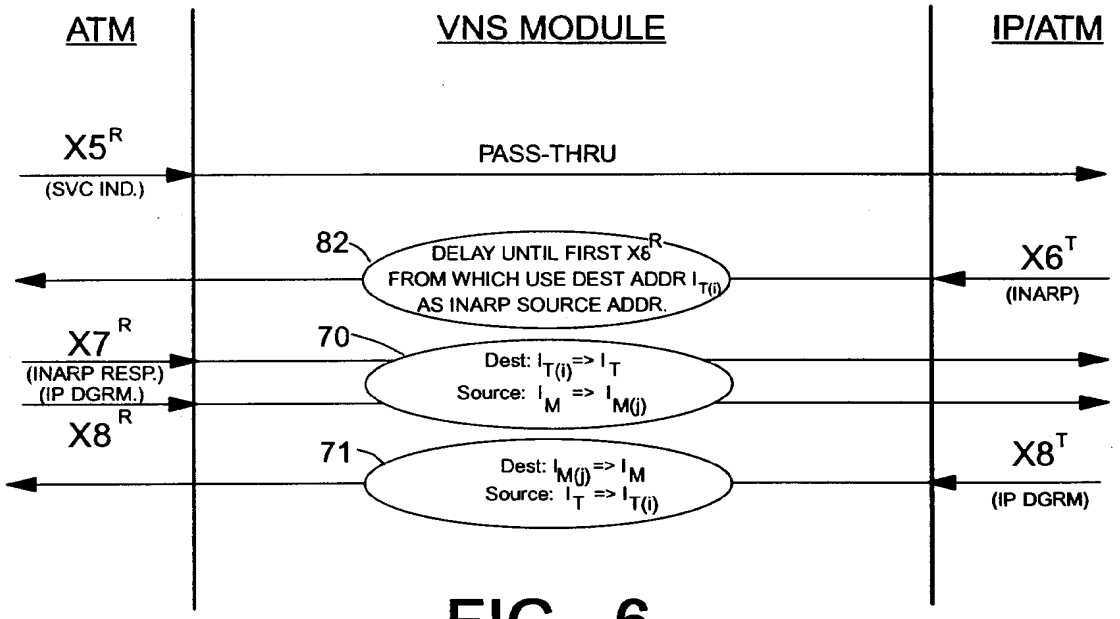


FIG. 6

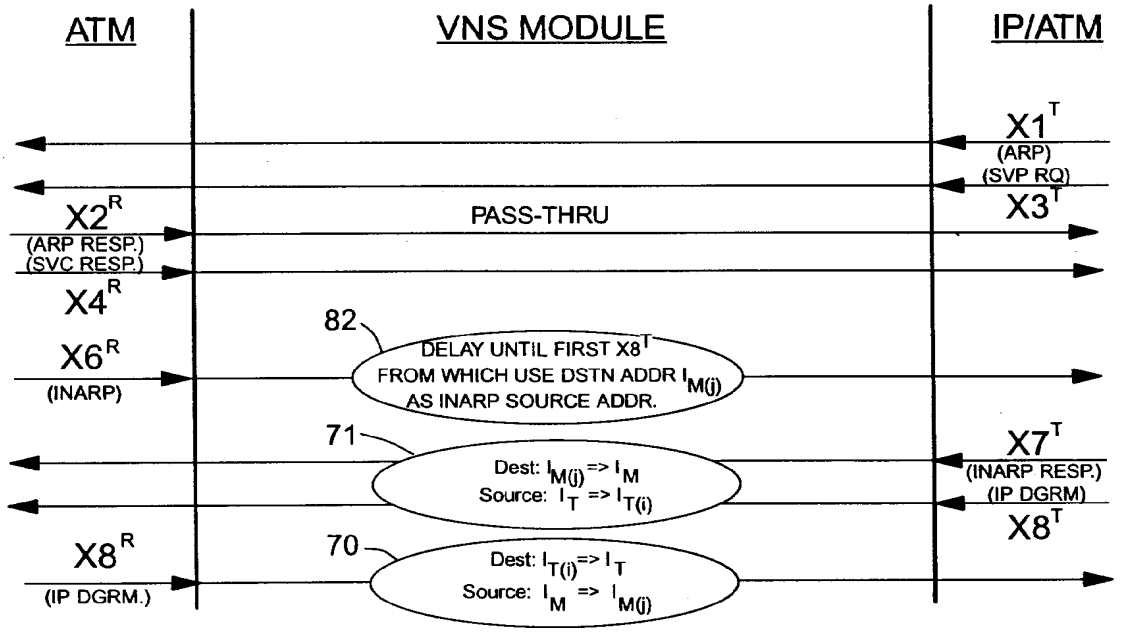


FIG. 7

Petitioner Apple Inc. - Exhibit 1026, p. 1075

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 96 41 0106

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	COMPUTER COMMUNICATIONS REVIEW, vol. 25, no. 4, 1 October 1995, pages 49-58, XP000541650 PARULKAR G ET AL: "AITPM: A STRATEGY FOR INTEGRATING IP WITH ATM" * paragraph 2.1 * ---	1,10	H04L29/06 H04Q11/04
A	PROCEEDINGS OF THE ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIE, SANTA FE, NOV. 20 - 22, 1994, no. SYMP. 35, 20 November 1994, GOLDWASSER S (EDITOR), pages 424-434, XP000531950 LUND C ET AL: "IP OVER CONNECTION-ORIENTED NETWORKS AND DISTRIBUTIONAL PAGING" * paragraph 1 - paragraph 1.1 * ---	1,10	
A	DATA COMMUNICATIONS, vol. 24, no. 17, 1 December 1995, page 103/104, 106, 108, 110 XP000547618 MARSHALL G: "CLASSICAL IP OVER ARM:A STATUS REPORT" paragraph "Simple virtues"" ---	1,10,11	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L H04Q
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 35, no. 4A, 1 September 1992, pages 28-31, XP000314666 "COORDINATED ADDRESS RESOLUTION PROTOCOL PROCESSING" * the whole document * ---	6,8,9	
A	EP 0 523 386 A (FUJITSU) * page 4, line 20 - page 5, line 14; figure 3 * -----	12	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	13 March 1997	Staessen, B

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Petitioner Apple Inc. - Exhibit 1026, p. 1076

Electronic Patent Application Fee Transmittal

Application Number:	11679416
Filing Date:	27-Feb-2007
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Filer:	Toby H. Kusmer.
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
		Total in USD ($)		**180**

Electronic Acknowledgement Receipt

EFS ID:	9469713
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer.
Filer Authorized By:	
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)
Receipt Date:	18-FEB-2011
Filing Date:	27-FEB-2007
Time Stamp:	10:01:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$180
RAM confirmation Number	6918
Deposit Account	501133
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Foreign Reference	EP0836306.pdf	1181950 64509eaea8cb2638c08c1ef0f9a1fdcbfdc2ee9e	no	15
Warnings:					
Information:					
2	NPL Documents	ISR13261.pdf	299844 f32c2c93b8fa7465ae3b37beb08f3731dce9d2ce	no	8
Warnings:					
Information:					
3	NPL Documents	ISRPCTUS99025323.pdf	138031 3d4cd666baae720c984c79205472c8535b7a6f1a	no	3
Warnings:					
Information:					
4	NPL Documents	ISRPCTUS99025325.pdf	141886 2fd71d5653d4fc8a333aa7a5a65213dde2a53ef9	no	3
Warnings:					
Information:					
5	NPL Documents	1FinalOA0044.pdf	371403 6e85269b054838f1fc27a4ee3774a72a16390028	no	14
Warnings:					
Information:					
6	NPL Documents	1FOA0016.pdf	322936 afb8b1922dd09994b7dd951119c7359457318144	no	9
Warnings:					
Information:					
7	NPL Documents	1FOA0037.pdf	256341 79b8b6386825b06537adbdeb1249272dc7a7e88c	no	8
Warnings:					
Information:					
8	NPL Documents	1NFOA0012.pdf	251995 184fd07ab4ed6fc5bad9776525faf34b32474aff	no	6
Warnings:					
Information:					
9	NPL Documents	1NFOA0016.pdf	358100 beec30a5f5ebc1538521c4eb1548c73a3835a044	no	10
Warnings:					
Information:					

10	NPL Documents	1NFOA0037.pdf	274457 a61f5be1b26fd5912d159b61ac05ad4f6286a950	no	7
Warnings:					
Information:					
11	NPL Documents	1NFOA0038.pdf	198309 b29566c7f91ad7f4434c52fe82e131ad1f1bd830	no	6
Warnings:					
Information:					
12	NPL Documents	1NFOA0039.pdf	157064 c81a3db8199ddeebe0f547d41ce8ec9ce5434b7b	no	4
Warnings:					
Information:					
13	NPL Documents	1NFOA0042.pdf	286408 6af393892203986735 19a2cc709d52bbb9075f9b	no	7
Warnings:					
Information:					
14	NPL Documents	1NFOA0044.pdf	438581 fd3902ff90b5e77993c3e243006a766c6151c71c	no	14
Warnings:					
Information:					
15	NPL Documents	1NFOA0064.PDF	299990 0d715c403bbb101a2a12ea3caa2ec1bca4370866	no	10
Warnings:					
Information:					
16	NPL Documents	1NOA0012.pdf	460543 15719d6b53d2517e10cd744e814aa73bedbd7745	no	9
Warnings:					
Information:					
17	NPL Documents	1NOA0016.pdf	489537 66ee422cb81039180e68e87bf7973aeed110638b	no	13
Warnings:					
Information:					
18	NPL Documents	1NOA0037.pdf	306134 ab231a5d73bbda34e9693f4d92017c069114c63d	no	6
Warnings:					
Information:					

19	NPL Documents	1NOA0038.pdf	259777 797ddaeb623304528a4d92348af178b3b681aa44	no	4
Warnings:					
Information:					
20	NPL Documents	1NOA0039.pdf	309545 38207b9a7789d7b6d60d9723f1533cba93e8f9fc	no	5
Warnings:					
Information:					
21	NPL Documents	1NOA0040.pdf	360294 dc31da9b9e57c03c572011f5af1bd188e9e0db87	no	7
Warnings:					
Information:					
22	NPL Documents	1NOA0041.pdf	667120 c190059565f36fee3af8bb3c823e40a24e15acc5	no	13
Warnings:					
Information:					
23	NPL Documents	1NOA0042.pdf	453844 28e5d2f82edaee3484af1995d4c230731b52c85f	no	9
Warnings:					
Information:					
24	NPL Documents	1NOA0044.pdf	724222 777ae7755a783cced396d2e903d19baaf11d364f	no	18
Warnings:					
Information:					
25	NPL Documents	1NOA0057.pdf	754386 9a900f865150257d219ada8f208b00896c771832	no	16
Warnings:					
Information:					
26	NPL Documents	1NOA0065.pdf	339321 a7a2aaadaf5f277e3355417519807fae446fd0d5	no	7
Warnings:					
Information:					
27	NPL Documents	1NOA0066.pdf	512781 1d0be68a967aff58a84d8fb021ea5d9de8d4f502	no	10
Warnings:					
Information:					

28	NPL Documents	1NonFinalOA0057.pdf	170178 a8e6797a7ffef393155e12f9ff964265558d9498	no	5
Warnings:					
Information:					
29	NPL Documents	1NonFinalOA0063.pdf	295823 e6ec72f6b38b0571d24577c904f996b6bfe05585	no	7
Warnings:					
Information:					
30	NPL Documents	1NonFinalOA0065.pdf	236600 0c55c005668c2b71693871ae352b78009c5116c6	no	6
Warnings:					
Information:					
31	NPL Documents	1NonFinalOA0066.pdf	208075 c5301a5b7ce75c1e0ec4291a2d1e57db8eab56a9	no	5
Warnings:					
Information:					
32	NPL Documents	1NonFinalOA0073.pdf	303829 a6a723e3ac667a3da55f6e3cb49f67261a77bda8	no	8
Warnings:					
Information:					
33	NPL Documents	2FinalOA0044.pdf	267254 1e75f15d18f0b7144aa36fadc447eeac5fde10b3	no	9
Warnings:					
Information:					
34	NPL Documents	2FinalOA0063.pdf	263511 2446c629ae2dd906bd0b9861b51e533e84137e91	no	7
Warnings:					
Information:					
35	NPL Documents	2FinalOA0066.pdf	118820 8bfc68c850d1d625ff84d007c880a80c5e64d7eb	no	4
Warnings:					
Information:					
36	NPL Documents	2FOA0016.pdf	257069 7c7fb1bf1686132eb2c2ee6691c4410859627b87	no	7
Warnings:					
Information:					

37	NPL Documents	2NFOA0012.pdf	332065 1d8b7b1031460a352317242875d458835897f69f	no	9
Warnings:					
Information:					
38	NPL Documents	2NFOA0016.pdf	353492 126d54025757372eaf3d0be8302e46a9bef6fd3b	no	10
Warnings:					
Information:					
39	NPL Documents	2NFOA0037.pdf	441997 23c25d7fbe54c7a4050b5b85de419b7051a6b986	no	13
Warnings:					
Information:					
40	NPL Documents	2NOA0012.pdf	476792 88f7e4412687f2f2b615146f665def89a289849a	no	12
Warnings:					
Information:					
41	NPL Documents	2NOA0016.pdf	261219 e5c1f64ccb5409d95d08099de9f67d902a82f729	no	9
Warnings:					
Information:					
42	NPL Documents	2NOA0037.pdf	134374 f178961c33e0503ef5e11c9212f5009a40c08398	no	4
Warnings:					
Information:					
43	NPL Documents	2NOA0042.pdf	746444 145489cace42ff4888d251a10d46d7a943eea1dd	no	19
Warnings:					
Information:					
44	NPL Documents	2NonFinalOA0065.pdf	340763 96a8385a1e5faa5f2c3423c947fba8a97dc0c462	no	8
Warnings:					
Information:					
45	NPL Documents	2NonFinalOA0073.pdf	428799 97d2e677c0c43b1a8ed09a265cc6b67b5822c8e6	no	11
Warnings:					
Information:					

46	NPL Documents	3NFOA0012.pdf	238086 ca068249588eabbe753fe79517fabfae5556430a	no	6
Warnings:					
Information:					
47	NPL Documents	3NOA0037.pdf	153481 3f0794384d7965215a9e29a921cb89a1bc15366f	no	5
Warnings:					
Information:					
48	NPL Documents	3NOA0065.pdf	669688 36c0966cd6726ca8b4caf3af0e1519889599b952	no	11
Warnings:					
Information:					
49	NPL Documents	3NonFinalOA0066.pdf	341371 542b38a0c57d10825252bbe35a597043c8d7c732	no	8
Warnings:					
Information:					
50	NPL Documents	3NonFinalOA0073.pdf	432059 f1d0cff6f09ff3ca021b18811eba4aa8691e08c4	no	10
Warnings:					
Information:					
51	NPL Documents	4NFOA0012.pdf	278018 5719db306528ebec2b9f9d28832dfb2b42ea3131	no	8
Warnings:					
Information:					
52	NPL Documents	4NOA0065.pdf	249932 0a4f69ed1e6582dc49e7215e13927c119559250a	no	4
Warnings:					
Information:					
53	NPL Documents	4NOApdf0037.pdf	245918 3e81635e443e7c50af72385796adff0615e919b4	no	4
Warnings:					
Information:					
54	NPL Documents	5NFOA0012.pdf	276673 5ff6ce4b17fad949c3d66a2b5f1dfd43af58b281	no	7
Warnings:					
Information:					

55	NPL Documents	5NOA0037.pdf	256957 adf903f072f1875c8fc6a88d49db239669f506b9	no	4
Warnings:					
Information:					
56	NPL Documents	5NOA0065.pdf	249890 de3fcfc4c306aa6d3e121ea7ee1ffa950d770b30	no	4
Warnings:					
Information:					
57	NPL Documents	depogarytomlinson.pdf	3836799 17defcb699cf68c190c09efa8512cd6c4b47bf31	no	60
Warnings:					
Information:					
58	NPL Documents	Transcript3910Afternoon.pdf	496076 3978812c01cdd7ee0840769d632718e03e39b7a6	no	170
Warnings:					
Information:					
59	NPL Documents	Transcript3910Morning.pdf	421929 9a4c23ad59cc9d0c2642d124005105618742256 3	no	131
Warnings:					
Information:					
60	Fee Worksheet (PTO-875)	fee-info.pdf	30557 aad209bed801e0c9591ac388c2506a52b94e03f7	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	24429337	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Use as many sheets as necessary)

Complete if Known	
Application Number	**11/679,416**
Filing Date	**02/27/2007**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Lim, Krisna**
Docket Number	**077580-0015**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1036	4,920,484	04/24/1990	Ranade	
	A1037	5,164,988	11/17/1992	Matyas	
	A1038	5,790,548	08/04/1998	Sitaraman et al.	
	A1039	5,918,018	06/29/1999	Gooderum et al.	
	A1040	6,308,213	10/23/2001	Valencia	
	A1041	6,425,003	07/23/2002	Herzog et al.	
	A1042	6,606,708	08/12/2003	Devine et al.	
	A1043	6,751,738	06/15/2004	Wesinger, Jr. et al.	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	B1	US2003/0196122	10/16/2003	Wesinger, Jr. et al.	
	B2	US2006/0059337	03/16/2006	Polyhonen et al.	

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 -Number 4 -Kind Codes (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C8	EP836306	04/15/1998	Hewlett Packard Co.			

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D13	PCT International Search Report for related PCT Application No.: PCT/US01/13261, 8 pages (Our Ref. No. 077580-0032)	
	D14	PCT International Search Report for related PCT Application No.: PCT/US99/25323, 3 pages (Our Ref. No. 077580-0062)	
	D15	PCT International Search Report for related PCT Application No.: PCT/US99/25325, 3 pages (Our Ref. No. 077580-0061)	
	D16	Non-Final Office Action dated June 16, 2003 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016)	
	D17	Final Office Action dated February 11, 2004 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016)	
	D18	Notice of Allowance dated May 27, 2009 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/679,416**
	Filing Date	**02/27/2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0015**

	D19	Non-Final Office Action dated March 1, 2004 from corresponding US Application Number 10/401,888 (Our Ref. No. 077580-0038)	
	D20	Non-Final Office Action dated May 4, 2004 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016)	
	D21	Non-Final Office Action dated June 24, 2004 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D22	Notice of Allowance dated July 21, 2004 from corresponding US Application Number 10/401,888 (Our Ref. No. 077580-0038)	
	D23	Notice of Allowance dated August 16, 2004 from corresponding US Application Number 10/702,580 (Our Ref. No. 077580-0041)	
	D24	Notice of Allowance dated August 17, 2004 from corresponding US Application Number 10/702,522 (Our Ref. No. 077580-0040)	
	D25	Non-Final Office Action dated October 21, 2004 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D26	Final Office Action dated April 11,2005 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016)	
	D27	Non-Final Office Action dated June 3, 2005 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D28	Notice of Allowance dated August 10, 2005 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016)	
	D29	Non-Final Office Action dated October 18, 2005 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D30	Notice of Allowance dated December 5, 2005 from corresponding US Application Number 09/429,643 (Our Ref. No.077580-0016)	
	D31	Final Office Action dated December 7, 2005 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D32	Notice of Allowance dated February 16, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D33	Notice of Allowance dated March 17, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D34	Non-Final Office Action dated March 28, 2006 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/679,416**
	Filing Date	**02/27/2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0015**

	D35	Notice of Allowance dated April 5, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D36	Notice of Allowance dated April 18, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D37	Notice of Allowance dated May 9, 2006 from corresponding US Application Number 10/401,551 (Our Ref. No.077580-0037)	
	D38	Non-Final Office Action dated May 19, 2006 from corresponding US Application Number 10/702,486 (Our Ref. No.077580-0039)	
	D39	Non-Final Office Action dated October 30, 2006 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D40	Notice of Allowance dated November 21, 2006 from corresponding US Application Number 10/702,486 (Our Ref. No.077580-0039)	
	D41	Non-Final Office Action dated March 21, 2007 from corresponding US Application Number 10/714,849 (Our Ref. No. 077580-0042)	
	D42	Non-Final Office Action dated June 15, 2007 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D43	Notice of Allowance dated October 29, 2007 from corresponding US Application Number 10/714,849 (Our Ref. No. 077580-0042)	
	D44	Notice of Allowance dated January 11, 2008 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D45	Notice of Allowance dated April 10, 2008 from corresponding US Application Number 10/714,849 (Our Ref. No. 077580-0042)	
	D46	Notice of Allowance dated July 1, 2008 from corresponding US Application Number 10/259,494 (Our Ref. No. 077580-0012)	
	D47	Non-Final Office Action dated September 17, 2008 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D48	Deposition Transcript for Gary Tomlinson dated February 27, 2009	
	D49	Non-Final Office Action dated March 5, 2009 from corresponding US Application Number 11/301,022 (Our Ref. No.077580-0044)	
	D50	Notice of Allowance dated April 3, 2009 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/679,416**
	Filing Date	**02/27/2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0015**

	D51	Non-Final Office Action dated June 9, 2009 from corresponding US Application Number 11/839,987 (Our Ref. No.077580-0066)	
	D52	Non-Final Office Action dated September 2, 2009 from corresponding US Application Number 11/924,460 (Our Ref. No.077580-0073)	
	D53	Notice of Allowance dated September 16, 2009 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D54	Notice of Allowance dated November 19, 2009 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D55	Final Office Action dated January 6, 2010 from corresponding US Application Number 11/839,987 (Our Ref. No.077580-0066)	
	D56	Notice of Allowance dated January 13, 2010 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D57	Notice of Allowance dated January 28, 2010 from corresponding US Application Number 11/840,508 (Our Ref. No.077580-0057)	
	D58	Final Office Action dated February 9, 2010 from corresponding US Application Number 11/301,022 (Our Ref. No.077580-0044)	
	D59	Notice of Allowance dated February 24, 2010 from corresponding US Application Number 11/839,987 (Our Ref. No.077580-0066)	
	D60	Non-Final Office Action dated March 19, 2010 from corresponding US Application Number 11/840,560 (Our Ref. No.077580-0063)	
	D61	Non-Final Office Action dated June 7, 2010 from corresponding US Application Number 11/924,460 (Our Ref. No.077580-0073)	
	D62	Non-Final Office Action dated June 9, 2010 from corresponding US Application Number 11/924,460 (Our Ref. No.077580-0073)	
	D63	Non-Final Office Action dated July 1, 2010 from corresponding US Application Number 11/839,969 (Our Ref. No.077580-0065)	
	D64	Non-Final Office Action dated July 8, 2010 from corresponding US Application Number 11/839,987 (Our Ref. No.077580-0066)	
	D65	Non-Final Office Action dated July 14, 2010 from corresponding US Application Number 11/840,508 (Our Ref. No.077580-0057)	
	D66	Final Office Action dated October 21, 2010 from corresponding US Application Number 11/840,560 (Our Ref. No.077580-0063)	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/679,416**
	Filing Date	**02/27/2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0015**

	D67	Non-Final Office Action dated December 14, 2010 from corresponding US Application Number 11/839,937 (Our Ref. No. 077580-0064)	
	D68	Notice of Allowance dated January 4, 2011 from corresponding US Application Number 11/301,022 (Our Ref. No. 077580-0044)	
	D69	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 9:00 AM	
	D70	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 10, 2010, 1:00 PM	
	D71	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 9:00 AM	
	D72	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 11, 2010, 1:30 PM	
	D73	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 9:00 AM	
	D74	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 12, 2010, 1:15 PM	
	D75	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 9:00 AM	
	D76	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 15, 2010, 12:35 PM	
	D77	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 8:45 AM	
	D78	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 8, 2010, 1:30 PM	
	D79	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 9:00 AM	
	D80	Trial Transcript, VirnetX vs. Microsoft Corporation dated March 9, 2010, 1:30 PM	

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	**11/679,416**
	Filing Date	**02/27/2007**
	First Named Inventor	**Victor Larson**
	Art Unit	**2453**
	Examiner Name	**Lim, Krisna**
	Docket Number	**077580-0015**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[ ] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[X] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[X] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Date: 2/17/11

Toby H. Kusmer; Reg. No.:26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 27283214-1.077580.0015

Electronic Acknowledgement Receipt

EFS ID:	9474127
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Kerrie Jones
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)
Receipt Date:	18-FEB-2011
Filing Date:	27-FEB-2007
Time Stamp:	10:17:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	NPL Documents	Transcript31010Afternoon.pdf	557496 77182e5b350291ef09e41df738360df5a5d1fd45	no	191

Warnings:	
Information:	

2	NPL Documents	Transcript31010Morning.pdf	398144 6aa135e6a22e92ec32af3f2f6c62872f0825979f	no	125
Warnings:					
Information:					
3	NPL Documents	Transcript31110Afternoon.pdf	571904 134c2bc8606058f0fee7be5b9555e224f7514055	no	178
Warnings:					
Information:					
4	NPL Documents	Transcript31110Morning.pdf	350449 999d42732e60cfd94507a8cd114e95e61675c77f	no	120
Warnings:					
Information:					
5	NPL Documents	Transcript31210Afternoon.pdf	545435 fcf8d2e98d23cf06da7a77181563184486252 90e	no	167
Warnings:					
Information:					
6	NPL Documents	Transcript31210Morning.pdf	430911 dbbb6593395ef47bb6539fc0cb16be7bfd6bd5ba	no	131
Warnings:					
Information:					
7	NPL Documents	Transcript31510Afternoon.pdf	693471 f9ba4bc92494c9aeb252fa67d3a058a363b8cb36	no	203
Warnings:					
Information:					
8	NPL Documents	Transcript31510Morning.pdf	514813 e6c7b4b57d1860f3c59e1537adabb2f9d4a52087	no	153
Warnings:					
Information:					
9	NPL Documents	Transcript3810Afternoon.pdf	473103 71a99540889d09ea542389ff1debd8e3cced675b	no	151
Warnings:					
Information:					
10	NPL Documents	Transcript3810Morning.pdf	371332 7d565afc267925e4e7888dc32bde6c9e61809933	no	119
Warnings:					
Information:					

11	NPL Documents	2NOA0065.pdf	300897 b66be01f064494dd688d64b12d429cdb91cde16e	no	7
Warnings:					
Information:					
12	Information Disclosure Statement (IDS) Filed (SB/08)	IDS.pdf	219177 bd89f7820b2d39d38a99efc671b61ae01cf5ac27	no	6
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
			Total Files Size (in bytes):	5427132	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

.Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	**11/679,416**
Filing Date	**02/27/2007**
First Named Inventor	**Victor Larson**
Art Unit	**2453**
Examiner Name	**Lim, Krisna**
Docket Number	**077580-0015**

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1044	5,590,285	12/31/19996	Krause et al.	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Code3 –Number 4 –Kind Code5 (*if known*)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
	C9	WO9843396	10/01/1998	Northern Telecom Limited			

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	D81	European Search Report dated January 24, 2011 from corresponding European Application Number 10011949.4	
	D82	European Search Report dated March 17, 2011 from corresponding European Application Number 10184502.2	
	D83	Hollenbeck et al., "Registry Registrar Protocol (RRP) Version 1.1.0; Internet Engineering Task Force, 34 pages (1999)	
	D84	Notice of Allowance dated March 14, 2011 from corresponding US Application Number 11/840,508 (Our Ref. No.077580-0057)	
	D85	Tannenbaum, "Computer Networks," pages 202-219 (1996)	

Subst. for form 1449/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** ***(Use as many sheets as necessary)***				**Complete if Known**	
				Application Number	**11/679,416**
				Filing Date	**02/27/2007**
				First Named Inventor	**Victor Larson**
				Art Unit	**2453**
				Examiner Name	**Lim, Krisna**
				Docket Number	**077580-0015**

CERTIFICATION STATEMENT

Please See 37 CFR 1.97 and 1.98 to make the appropriate selection(s)

[ ] Information Disclosure Statement is being filed with the filing of the application or before the receipt of a first office action.

[X] That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement; or

[ ] That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of the information disclosure statement.

[ ] The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $180.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] Information Disclosure Statement is being filed with the Request for Continued Examination. The Commissioner is hereby authorized to charge the fee pursuant to 37 CFR 1.17(P) in the amount of $810.00, or further fees which may be due, to Deposit Account 50-1133.

[ ] None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

/Hasan M. Rashid/ Date: March 29, 2011

Hasan M. Rashid; Reg. No.: 62,390
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Tel. (617) 535-4000
Fax (617) 535-3800

DM_US 27910070-1.077580.0015

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 12/66, H04Q 11/04

A1

(11) International Publication Number: **WO 98/43396**

(43) International Publication Date: 1 October 1998 (01.10.98)

(21) International Application Number: PCT/CA98/00197

(22) International Filing Date: 11 March 1998 (11.03.98)

(30) Priority Data:
08/821,145 20 March 1997 (20.03.97) US

(71) Applicant: NORTHERN TELECOM LIMITED [CA/CA]; World Trade Center of Montreal, 8th floor, 380 St. Antoine Street West, Montreal, Quebec H2Y 3Y4 (CA).

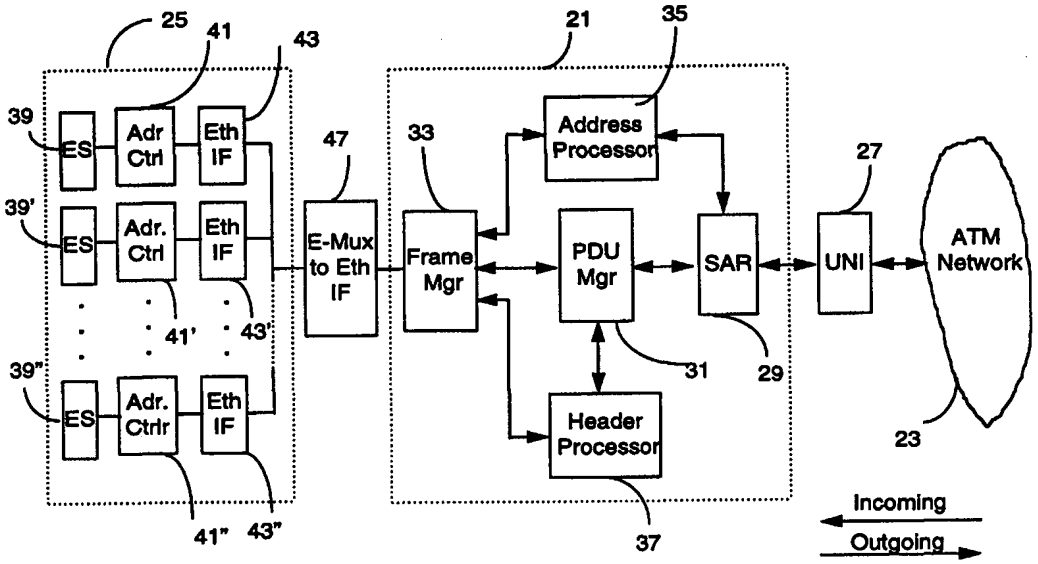
(72) Inventors: ALLAN, David, Ian; 852 Forest Street, Ottawa, Ontario K2B 5P9 (CA). CASEY, Liam, M.; 61 Aylmer Avenue, Ottawa, Ontario K1S 2X2 (CA). ROBERT, Andre, J.; 103 Sol Lane, R.R. #2, Woodlawn, Ontario K0A 3M0 (CA).

(74) Agent: DIACONESCU, Aprilia, U.; Northern Telecom Limited, Patent Dept., P.O. Box 3511, Station "C", Ottawa, Ontario K1Y 4H7 (CA).

(81) Designated States: AU, CA, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: A MECHANISM FOR MULTIPLEXING ATM AAL5 VIRTUAL CIRCUITS OVER ETHERNET



(57) Abstract

The invention provides for an E–Mux and a method for encapsulating/segmenting ATM cells into/from an Ethernet frame at the boundary between an ATM and an Ethernet network. An Ethernet end–station on the E–Mux is addressed using multiple MAC level identifiers, which are dynamically assigned according to the ATM virtual circuits which terminate on that end station, and have only transitory significance on the Ethernet. A unique ATM OUI identifies the frames carrying ATM–traffic.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

A MECHANISM FOR MULTIPLEXING ATM AAL5 VIRTUAL CIRCUITS OVER ETHERNET

Field of the Invention

The invention is directed to a system and method for carrying ATM network information over a local area network (LAN), and more particularly to a mechanism for multiplexing ATM AAL5 virtual circuits over Ethernet.

Background of The Invention

The asynchronous transfer mode (ATM) forms the basis for switching in broadband networks. ATM is a connection oriented data transport which is media independent. The key feature of ATM is the segmentation of data into fixed length units of data referred to as cells. Each cell is separately steered at each ATM switch via an identifier of local significance to the local transport leg provided in the header of each cell. The identifiers are reassigned during the transit of a cell from an input port to an output port on a switch. The identifier carried between a switch and an end system is 24 bits in length. For an ATM user network interface (UNI), this is a concatenation of a 16 bit virtual circuit identifier (VCI) and an 8 bit virtual path identifier (VPI).

This routing mechanism differs significantly from other networks, in that there is only one identifier specifying a local path vs. source and destination information. This path information in itself is insufficient to uniquely identify the real source and destination for the payload and therefore the connection is set up via signalling. As such, connection to a remote end-station is requested and upon connection set-up, the network informs the end station what the local identifier of the connection is.

Ethernet is a connectionless LAN technology designed for data applications in which all stations on the network share the communication medium. This medium, which could be twisted pairs,

fiber, or coaxial cables, is shared in a peer to peer fashion. All devices on the Ethernet can be reached by a single transmission of data. Ethernet operates typically at 10Mbs and the data are sent in the form of Ethernet "frames".

There is no central arbitrator of bandwidth to administer media access on an Ethernet. Every time an Ethernet end station sends message, it listens to the media to ensure that it is not in use by another station. If this is true, the end station commences sending its own message. During the message send phase, the end station monitors the media to detect if another station has also commenced sending at the same time. The minute delays imposed by the speed of light permit a relatively large window wherein multiple stations can believe that the media is idle, and therefore can commence sending an Ethernet frame. If the end station detects a collision, i.e. what it hears does not match what it sends, it switches to sending a short "jabber" sequence to ensure that all colliding end stations detect that contention has occurred. All end-stations detecting a collision will wait a random interval and will then retry sending their frame, once again applying the same rules to determine success, and to free up the channel as quickly as possible when a collision occurs. Additional error detection is built into each frame to ensure that errored frames are not propagated.

Ethernet end stations are addressed globally and uniquely by a 48 bit media access control (MAC) address. The MAC address is comprised of a 24 bit Organization Unique Identifier (OUI) and a 24 bit end station identifier (ID). OUI is a globally administered numbering plan which comprises a portion of a number identifying the organization administering the remainder of the number, which is IEEE for Ethernet. The ID is a unique identifier that a manufacturing organization can provide to all equipment that it manufactures. Further, this identifier is unique and staticaly assigned and well known to the station. Certain Ethernet addresses are reserved for broadcast and

multicast to all end-stations on the segment and for diagnostic purposes.

An Ethernet connected end station receives all data broadcast onto the media. By convention, the end station discards all traffic not directed to itself, all, or a subset of end stations, as identified in the destination MAC address.

All major emerging communication technologies rest on the layers of the OSI model. The OSI model defines a physical layer which specifies the standards for the transmission medium, a data link layer (layers 2 and 3) and a network layer (layers 4 to 7). Thus, in many cases, Ethernet operates on FDDI (fiber distributed data interface) physical layer, and the MAC layer, placed on top of FDDI, comprises the data layer. ATM operates on SONET, copper, twisted pairs, FDDI as physical layer, and the data layer is subdivided into an ATM layer and an ATM adaptation layer (AAL) providing the convergence function (called also convergence sublayer CS). Whatever the implementation of the AAL at the UNI, the ATM network is not concerned with the AAL operations, the ATM bearer service is masked from the convergence function.

It has become evident that LAN shared bus architecture is insufficient to meet the demands of applications that require more bandwidth, and that LANs are beginning to become a bottleneck in computing environments. For this reason, more economic local interfaces such as a Frame-Relay version (FUNI) and an Ethernet version, Cells-in-Frames (CIF), are used in the access network. In both cases, the separation of data into cells is deferred until within the network, but the higher level information is carried to the end station. In addition, according to the CIF version the AAL5, PDUs are pre-packaged at the end station and this implies changes in HW and SW at each Ethernet connected end station.

Switched Ethernet technology, developed to provide more capacity to an end-user, does not relay on shared medium, it rather

provides point-to-point bandwidth between the user station and the switch, so that instead of sharing a 10 Mbit/s medium, the user gets a dedicated 10 Mbits/s medium. As Ethernet hubs and switches are growing in use, they become an inexpensive means to provide more bandwidth to workstations. A switched Ethernet network is more flexible, in that it may include stations that are using a port at a given full rate, stations that share a port, or stations that have access to more than one port.

However, switched Ethernet provides only limited bandwidth and supports data traffic only. A more efficient solution for bursty traffic is needed. There is also a need to simplify and standardize the access link while also obtaining protection of the access traffic.

Although ATM provides a very rich environment with numerous traffic classes and the ability to multiplex many data streams with different handling requirements together, this functionality is mainly required in the network backbone. It is sought that ATM networks will be used by more general class end stations for delivering multi-media services. However, in the short term, the extra bandwidth and cost of ATM interfaces is probably not justified for general class end stations, such as desktop computers. It is possible to built ATM switches with lower speed ATM interfaces, but this solution presents a serious deployment problem in that it requires replacement of the substantial installed base of shared media LAN wiring and adapter cards.

An ATM-Ethernet concentrator is disclosed in United States Patent No. 5,457,681 (Gaddis et al., issued on October 10, 1995 and assigned to Washington University), which provides an interface between an ATM network and a plurality of Ethernet segments. Each Ethernet frame transmitted by any of the Ethernet segments is fragmented into a sequence of ATM cells, which are transmitted by an Ethernet controller associated with the respective segment over the ATM network and delivered to the interconnected Ethernet

controllers. When the cells are received, the controller re-assembles them into frames and transmits the frames over the respective Ethernet segment to the end stations. While this patent partially addresses the problems of bandwidth and cost, it does not provide a method and system for transmitting ATM cells in Ethernet frames, for taking advantage of the ATM capabilities.

There is a need to provide an improved network communication system with minimal displacement of existing network components, capable of providing large bandwidth to the end stations for data, video and voice traffic, and providing LAN access to switched point-to-point WAN links.

International application No. PCT/CA95/00029 (WO 95/20282) (by Burwell et al. published on July 27, 1995 and assigned to Newbridge Networks Corporation) discloses a communication network comprising ATM switches interfaced with LANs, the ATM cells being encapsulated in LAN frames and being delivered in encapsulated form over the Ethernet LAN direct to the end station. In another embodiment, the LAN interface adapter of the end station provide bridging, network layer functions and LAN emulation functions to permit transparent communication between the end stations over the ATM network. The interface adapter, also defined as a "ridge (bridge/router) creates frames from ATM cells and vice-versa.

However, the method disclosed in the above patent layers ATM carriage on top of the Ethernet layer. This is to say, ATM information only appears within the Ethernet payload, imposing an extra layer of indirection and frame processing on ATM handing at the LAN/WAN boundary.

Summary of the Invention

It is an object of this invention to provide a mechanism for transmitting ATM cells in Ethernet frames for interworking of ATM

backbone networks with the large base of legacy equipment, and for re-establishing access to an ATM network for a LAN.

It is another object of the invention to provide an addressing convention for carriage of ATM over Ethernet to a specified end station.

This invention is based on the fact that although an Ethernet MAC address is normally globally unique for universal interoperability, it does not absolutely have to be for a closed Ethernet to work. Uniqueness of the address within the Ethernet broadcast domain itself is necessary. According to this invention, an Ethernet end station is allowed to assume multiple MAC level identifiers on a single Ethernet interface. These identifiers which are dynamically assigned, have only transitory significance on the Ethernet.

Accordingly, the invention provides a multiplexer (E-Mux) for encapsulating ATM cells into a LAN frame, comprising a segmentation and reassembly unit for receiving a plurality of incoming ATM cells with a LAN destination address and generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU); a PDU manager for receiving the AAL5 PDU and extracting an AAL5 payload; a header processor for extracting a traffic type indicator from the header of the PDU; an address processor for extracting the LAN destination address from the header of an incoming ATM cell; and a frame manager for receiving the traffic type indicator, the AAL5 payload and the LAN destination address and generating an incoming LAN frame.

The invention also provides a multiplexer (E-Mux) for segmenting a LAN frame into a plurality of ATM cells, comprising: a frame manager for receiving an outgoing LAN frame with an ATM destination address and de-assembling it into a traffic type indicator, an AAL5 payload and an ATM destination address; a header processor for receiving the traffic type indicator from the frame manager; a PDU manager for receiving the AAL5 payload and the traffic type indicator and generating an ATM adaptation layer 5 (AAL5) protocol data unit

(PDU); an address processor for receiving the ATM destination address from the frame manager; and a segmentation and reassembly unit for receiving the PDU and the ATM destination address generating a plurality of ATM cells with the ATM destination address.

According to another aspect of the invention, there is provided a telecommunication network comprising a LAN with a plurality of end-stations connected over a transmission medium and an ATM network, comprising: a multiplexer (E-Mux) for encapsulating a plurality of ATM cells received from the ATM network into an incoming LAN frame and for segmenting a LAN frame received from the LAN network into a plurality of outgoing ATM cells; an E-Mux-to-LAN interface for adapting the transmission format of the LAN frame for transmission over the connection medium of an LAN network; an ATM-to-E-Mux interface for adapting the transmission format of the ATM cells received from an ATM network for processing by the E-Mux; an address controller at each end station for forwarding the incoming LAN frame to the end station when a destination address comprised in the destination MAC field of the LAN frame is recognized by the address controller, and for inserting an ATM destination address into the source MAC field of the outgoing frame.

A method for transmitting information from an ATM network to an Ethernet network using an E-Mux is also disclosed, the method performing the steps of: establishing connection between an ATM switch of the ATM network and an end station of the Ethernet network based on a VPI/VCI destination address in the header of an incoming ATM cell; receiving a plurality of incoming ATM cells with the destination address, and generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU) with a segmentation and reassembly unit; extracting an AAL5 payload from the PDU with a PDU manager; extracting a traffic type indicator from the header of the PDU with a header processor; generating with a frame manager an incoming Ethernet frame using the traffic type indicator, the AAL5 payload and

the destination address; and transmitting the Ethernet frame over the Ethernet network to the end station according to the destination address.

According to still another aspect of the invention, there is provided a method for transmitting information from an Ethernet network to an ATM network using an E-Mux performing the steps of: establishing connection between an end station of the Ethernet network and an ATM switch of the ATM network based on a VPI/VCI destination address provided by the end station; generating an outgoing Ethernet frame at the end station and transmitting same to the E-Mux; extracting from the Ethernet outgoing frame a traffic type indicator, a frame payload and a source address, with a frame manager; generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU) with a segmentation and reassembly unit from the frame payload and a traffic type indicator extracted from the type field of the outgoing frame with a header processor; segmenting the PDU into a plurality of outgoing ATM cells and inserting a VPI/VCI destination address in the header of the cells from an address processor.

Advantageously, the system and method of the invention provides a highly efficient carriage of ATM information to an end station using actual MAC address space in the Ethernet frame.

Because the frames are not pre-packaged into AAL5 PDUs at the end station, but at the E-Mux, the system of the invention is efficient, as custom hardware to perform this function does not need to be deployed at each Ethernet connected end station, and the end station software is not burdened with this task. Custom hardware to perform SAR (segmentation and reassembly) function is built into the E-Mux.

Still another advantage of the invention is that legacy Ethernet can coexist with ATM LAN to UNI traffic. ATM intelligence can be distributed in such a LAN segment. For meshed PVC/UBR type connections, standard packet formats and driver interfaces may be used between layer 3 and the Ethernet interface, making the invention

applicable to various LAN technologies. No additional information needs to be propagated outside the system of the invention. Therefore, this permits the system to be tailored as an application specific ATM to Ethernet interface.

Still another advantage of the invention is that the Ethernet frame is efficiently used since the ATM routing information is embedded in the Ethernet MAC addressing field. No additional ATM header within the Ethernet payload is necessary, since the entire ATM semantics is not carried to the end station. This does not preclude, however, additional semantics being packaged in a separate header in the Ethernet frame.

ATM virtual circuit (VC) address mapping is carried forward into the Ethernet domain. Intermediate steps are not required to map Ethernet MAC to VC, as VC information flows end-to-end. For uncommitted bit rate (UBR) data services, only the ATM path identifier need to be carried forward across an Ethernet LAN.

As a result, Ethernet traffic can coexist-exist with ATM LAN to UNI traffic. As indicated above, each Ethernet connected station may assume multiple IDs on the LAN at the MAC level. Thus, for traditional, non-ATM traffic, it retains the manufacturers MAC address built into the Ethernet interface at the factory. For ATM traffic, it assumes one or more IDs depending on the ATM virtual circuits which ultimately terminate at that particular end station interface.

Brief Description of the Drawings

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of the preferred embodiments, as illustrated in the appended drawings, where:

Figure 1A shows the convergence and segmentation and reassembly functions of ATM (prior art);

Figure 1B shows an ATM network for defining the terms virtual channel and virtual path (prior art);

Figure 1C shows an Ethernet frame (prior art);

Figure 2 shows the block diagram of the E-Mux;

Figure 3A shows the processing of the ATM cells to produce an incoming Ethernet frame;

Figure 3B shows the processing of an outgoing Ethernet frame to produce ATM cells;

Figure 4A is a the flow-chart illustrating the assembly of the ATM cells to produce an Ethernet frame;

Figure 4B is a the flow-chart illustrating the segmentation of the Ethernet frame to produce ATM cells;

Figure 5 shows the block diagram of a variant of the E-Mux;

Figure 6A shows the processing of the ATM cells to produce an incoming Ethernet frame according to the variant of Figure 5; and

Figure 6B shows the processing of an outgoing Ethernet frame to produce ATM cells according to the variant of Figure 5.

Description of the Preferred Embodiment

Figures 1A, 1B, and 1C are provided for defining and illustrating some of the terms necessary for describing the present invention and its mode of operation.

Figure 1A shows the convergence function, and the segmentation and reassembly (SAR) function of ATM. The convergence function is responsible for accepting the user traffic which could range from one to maximum 65,000 bytes, and placing a header **10** and a trailer **12** around it to obtain a protocol data unit (PDU) **2**. For this invention, the payload field of the PDU is limited to 1,500 bytes, which is the size of the Ethernet payload field. To push PDU beyond Ethernet limit of 1,500 bytes will require an additional header in the Ethernet frame. The length of the header and trailer is between 6 and 40 bytes. Once the header and the trailer have been added to the user

payload, the traffic is segmented into 44-48 bytes data units **14**. Next, the adaptation layer adds a header **16**, and possibly a trailer **18** to the data unit **14**, depending on the type of payload being supported. In any event, the final data unit from this operation is always a 48 octet block **20**. Finally, the last operation is performed by the data link layer which adds a five-octet header **22** to the 48-octet payload **20** resulting in a 53 bytes cell **24**. Each cell is transported over the physical layer between two ATM switches designated by the address information in header **22**.

Figure 1B shows a basic linear point-to-point ATM network configuration where the connections are identified through virtual channel identifiers (VCI) and virtual path identifiers (VPI) in the ATM cell header. Switching in the ATM network is illustrated at **5**, **7**, and **9**. A virtual channel connection (VCC) **11** has end-to-end significance between end users A and B. A virtual path connection (VPC) has significance between adjacent ATM devices, **5**, **7**, and **9**, and switching is performed very quickly through the use of a routing table.

Figure 1C illustrates an Ethernet frame. Ethernet end stations are addressed globally and uniquely by the MAC address. Field **28** comprises the destination MAC and field **30** comprises the source MAC. The MAC address is has a 24 bit organizationally unique identifier (OUI) **38**, **42** and a 24 bit end station identifier **40**, **44**.

A type field **32** is provided for specifying the traffic type.

The payload field **34** may comprise up to 1500 bytes. The frame begins with a training sequence **26** for allowing receiver synchronization and ends with a frame check sequence **36**, for determining the integrity of the data in the frame.

Figure 2 shows the block diagram of the system according to the invention. An E-Mux **21** exchanges ATM cells with an ATM UNI **27**, which is connected in turn to an ATM network **23**. E-Mux **21** is also connected to an Ethernet LAN **25** for exchanging frames. By convention, the traffic travelling from ATM network **23** to LAN **25** is

defined by the term "incoming", and the traffic travelling from LAN **25** to ATM network **23** is defined by the term "outgoing".

According to the invention, a unique MAC OUI is established for extending ATM path addressing into the Ethernet MAC address domain. This unique MAC OUI identifies the traffic as ATM UNI. The ATM OUI is inserted in both the destination and the source MAC fields **38** and **42**. The OUI field informs LAN **25** that the traffic is coming from a source not registered to it, so as to treat it accordingly. As indicated earlier, this permits the ATM traffic to coexist with traditionally addressed Ethernet traffic.

E-Mux **21** associated to LAN **25** also requires a unique ID in the destination MAC, such that incoming traffic can be uniquely addressed to it. The ID could be for example VPI=0, VCI=0, which is never used in the ATM network **23**. This unique address, ATM OUI, VPI=0,VCI=0, is mapped into the source MAC field **30** of an incoming frame and in the destination MAC of an outgoing frame. This is described next in connection with Figures 3A, which shows the processing of the ATM cells to produce an incoming Ethernet frame and Figure 3B, which shows the processing of an outgoing Ethernet frame to produce ATM cells.

Each end station has an VPI/VCI address for the ATM traffic used to establish connection between a switch in the ATM network and an end station through signalling in a known manner. For the incoming traffic, a flow of cells **24**, addressed to an end station **39, 39', 39"** in Ethernet network **25** is received at UNI **27** from network **23**. The cells are assembled into a PDU **2** by SAR unit **29** of E-Mux **21**.

PDU **2** comprises a AAL5 payload field **14** for receiving the payload from the incoming cells **24**, the size of the payload field being limited to the maximum size of field **34** (up to 1500 bytes) of an Ethernet frame **3**. Although the normal ATM AAL5 protocol data unit (PDU) is quite large, as discussed in connection to Figure 1, it can be constrained to fit within the 1500 bytes of an Ethernet frame.

Since the size of the PDU is restricted to the payload field length of a frame, the cell segmentation function is performed by SAR **29** at boundary to the ATM network, such that the need for additional PDU information to be carried in the payload portion of the Ethernet frame is obviated. This differs from the cell-in-frame (CIF) approach in which the SAR function is performed at the end station, and then the cells are reassembled into Ethernet frames for transmission.

A PDU manager **31** strips the LLC/SNAP (Logical link control, sub-network attachment point) header of the PDU **2** and provides it to a header processor **37**, which determines the type of the payload. The payload and the payload type are forwarded to a frame manager **33**.

Frame manager **33** generates the Ethernet frame **3** by mapping the payload into field **34** and the payload type into field **32**. Frame manager **33** also receives the address of the destination end station from an address processor **35**, and maps this information into field **40** of destination MAC. This address is a concatenation of the VPI/VCI address extracted from the cell header **22**. As well, address processor **35** maps the address of the E-Mux in the source MAC field **30**, namely ATM OUI and VPI=0, VCI=0 in fields **40** and **42**, respectively. As such, for the incoming traffic, the source MAC field of frame **3** comprises the address of the E-Mux, and the destination MAC comprises the address of the end station in the Ethernet.

Frame manager **33** sends frame **3** assembled as indicated above, over the Ethernet network **25**. An interface **47** is provided for adapting the format of the frame to the connection medium of Ethernet **25**.

In general, each "ATM aware" end station **39, 39', 39"** is provisioned with an address controller, as shown at **41, 41', 41"**, which allows the end station to signal the network to request/accept connections. As well, address controller **41, 41', 41"** provides the range of VPI/VCI values that could be assigned for such connections to the associated end station **39, 39', 39** to a defined subset of the whole VPI/VCIs allocated for UNI **27**. An address controller **41, 41', 41"**

recognizes a destination ID as being its own, using a look-up table, and directs frame **3** to the associated end station **39, 39', 39"**.

For the outgoing direction, an end station **39, 39', 39"** generates an outgoing frame **3**, with the destination MAC indicating the ATM OUI address of E-Mux **21**, rather than the address of another end station in the Ethernet network **25**. As such, the corresponding Ethernet interface transmits the outgoing frame to E-Mux **21**. The source MAC ID field **44** comprises the VCI/VCI address, of the destination ATM device in ATM network **23**.

Now, frame manager **33** receives the frame from interface **47**, segments the frame and provides the payload to PDU manager **31**, the VPI/VCI address to address processor **35** and the type information from field **32** to header processor **37**. PDU manager **31** generates a PDU **2** by inserting the payload received from frame manager **33** into field **14**, and the type information from header processor **37** into LLC/SNAP header field **16**. PDU is then forwarded to SAR **29** which segments the PDU **2** into cells **24**, for UNI **27**. Address processor **35** inserts the VPI/VCI address from the source MAC ID field **44** into each cell header, so that ATM network **23** switches the cell accordingly.

A simple example of this technique would be that end station **39** has established an ATM connection on VCI=5, VPI=7. For all traffic that is to be directed beyond the Ethernet onto the ATM network **23**, end station **39** would set the destination MAC address in the Ethernet frame to that of the E-Mux **21**, which is ATM-OUI, VPI=0, VCI=0, and would identify the virtual circuit via the source MAC, which will show ATM-OUI, VPI=7, VCI=5, identifying the source as the owner of that VCC. Traffic flowing in the direction from E-Mux **21** to end station **39**, would see the source and destination addresses reversed.

As a simple extension of this concept, an Ethernet station, when originating signalling, may use the source MAC field for the normal Ethernet MAC and the destination MAC field for the ATM-OUI and '0'. The source MAC field permits an E-164 encoded NSAP to give the

Ethernet connected end station a unique identification in the ATM network. In this way, the E-Mux can arbitrate and aggregate signalling onto a standard UNI from multiple Ethernet connected devices.

Additional overhead is eliminated by performing the ATM AAL5 protocol encapsulation at the E-Mux (e.g. normal protocol encapsulation for AAL5 as defined by RFC1483). Thus, an encapsulation of the cells into a PDU frame is effected by PDU manager **31**, and an encapsulation of the PDU into an Ethernet frame is effected by the frame manager **33**, such that the Ethernet end station does not have to be ATM protocol aware, or perform CRC (cyclic redundancy check) and SAR (segmentation and reassembly) functions.

Figure 4A is a the flow-chart illustrating the processing of the ATM cells to produce an Ethernet frame. In step **100**, a connection between the station in the ATM network and the E-Mux **21** is established based on the ATM address of the E-Mux. An address controller, lets say **41**, recognizes its associate end station as the owner of the VPI/VCI, and station **39** establishes communication with ATM network **2**, shown in step **110**.

When E-Mux **21** receives a flow of ATM cells over a specific VC, as shown in step **120**, it assembles the cells into a PDU, step **130**, verifies that the AAL5 **CRC** is correct, in step **140**, and maps the payload into the payload portion of the Ethernet frame in step **150**. The destination MAC is set in field **28** to ATM OUI, VCI/VPI in step **160** to uniquely identify the owner of that particular path on the LAN, and the source MAC is set to that of the E-Mux, namely ATM OUI 0x00, in step **170**.

The E-Mux broadcasts the Ethernet frame onto the Ethernet network in step **180**. Station **39** with ID VPI/VCI in the destination MAC receives the frame, while other stations **39'**, **39"** on the Ethernet, receive the frame and discard it as they are not addressed to them, as shown in step **190**.

Figure 4B shows a the flow-chart illustrating the processing of an Ethernet frame to produce ATM cells.

First, in step **200**, an end station, for example station **39** originates a message to be sent, for example, over VCI=5, VPI=7. It prepares an Ethernet frame as shown in Figure 3B directed to the E-Mux by inserting the ATM OUI in fields **38** and **42**, the VPI=0, VCI=0 address in the destination MAC field **40** and inserts the ATM virtual circuit address information in the source MAC address field **44**.

In step **210**, station **39** broadcasts the frame on the Ethernet. Other stations on the Ethernet receive the frame, check the destination MAC in step **220**, and discard it in step **230**, as they are not the addressed recipients of this frame.

E-Mux **21** receives the frame in step **240**, and as the recipient, keeps the frame. It performs ATM AAL5 PDU and SAR processing on the payload steps **250** and **260**, extracts the ATM virtual circuit address information from the frame source MAC and inserts it into the cells headers in step **270**. The resulting cells are transmitted in step **280** over the address specified by the VPI/VCI address information.

Additional processing could be performed during processing of the cells from the Ethernet frames. For example, an Ethernet II/DIX format frame could be converted to RFC1483 encapsulation prior to AAL5 and SAR handling as an additional interworking step.

The invention may be used for providing ATM WAN (wide area network) access from a LAN. This permits a LAN connected computer to establish unique and private WAN connections, while maintaining access to all legacy services deployed on the non-ATM aware portions of the local LAN.

Use of Ethernet networks as a distributed multiplexer backbone over several shelves of equipment, permits an Ethernet to be used as the media to demultiplex an ATM UNI over a collection of devices distributed over a large area (e.g. up to 6000 feet for 10BaseT). The typical application would see shelf and line card encoded in the ATM VPI/VCI addressing scheme to permit static de-multiplexing of the UNI.

A variation of the E-Mux of the invention can function as an ATM to Ethernet multiplexer, as shown in Figure 5.

This variant provides for a highly scaleable and optionally redundant UNI termination for IP (Internet Protocol). The automated association of IP to VCI/VPI can be utilized to produce ATM interfaces for IP protocol based devices which can support significantly more virtual circuits than are currently available. This eliminates the requirement for the address controllers **41, 41', 41"** residing in the attached end station **39, 39', 39"**. This also moves the IP->ATM association from the custom hardware in the Ethernet interface **43, 43', 43"**, to the traditional Ethernet ARP cache resident on the end station. Current ATM interfaces are limited to between 500 and 2000 VCs. This invention permits interfaces for relatively low bandwidth connections (as for an ATM based element management channel) to scale up to more than 50,000 virtual circuits.

In this case the E-Mux **50** assumes the OUI/VPI/VCI identifiers and the attached end station retains its normal MAC address. Figure 6A shows the processing of the ATM cells to produce an incoming Ethernet frame and Figure 6B illustrates the processing of an outgoing Ethernet frame to produce ATM cells, for E-Mux **50**.

For the incoming traffic source OUI field **42** contains the ATM OUI to indicate to the end station that traffic comes from the ATM network **23**. The VPI/VCI address form the cell header **22** is mapped by E-Mux **50** into the source ID field **44**. The destination MAC field **28** comprises the Ethernet MAC of the station recipient of the respective frame.

For the outgoing traffic, Figure 6B shows that the end station inserts the ATM OUI identification in field **38** of the destination MAC field **28** and the VPI/VCI address of the destination station in the ATM network **23** in field **40** of the destination MAC. The E-Mux **50** inserts the VPI/VCI address into the cell headers, so that the cells are switched accordingly in network **23**. The source MAC field **30** comprises the

Ethernet address of the end station in the Ethernet network that generated the respective frame.

There are numerous ways by which the embodiment of Figure 5 can learn the Ethernet MAC address of the attached end stations. Alternatively, the Ethernet all-stations broadcast address can be used.

The generalized operation is that an attached end station learns the IP->MAC association for devices remotely connected to the ATM network as it would for a normal Ethernet. However, the MAC addresses presented actually contain VPI/VCI information by which those devices can be reached. The attached host is "spoofed" into having an Ethernet layer 2 address mapping for ATM connected devices such that Ethernet address resolution and forwarding mechanisms make ATM attached devices reachable.

This invention can also be used to provide hot standby backup platforms. Normally an ATM connection is unique and cannot automatically be locally switched to another platform. The availability of Ethernet as a broadcast medium permits the ATM traffic to be fanned out to multiple devices simultaneously and only acted upon by the current "active" platform.

While the invention has been described with reference to particular example embodiments, further modifications and improvements which will occur to those skilled in the art, may be made within the purview of the appended claims, without departing from the scope of the invention in its broader aspect.

WE CLAIM:

1. A multiplexer (E-Mux) for encapsulating ATM cells into a LAN frame, comprising:

a segmentation and reassembly unit for receiving a plurality of incoming ATM cells with a LAN destination address, and generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU);

a PDU manager for receiving said AAL5 PDU and extracting an AAL5 payload;

a header processor for extracting a traffic type indicator from the header of said PDU;

an address processor for extracting said LAN destination address from the header of an incoming ATM cell; and

a frame manager for receiving said traffic type indicator, said AAL5 payload and said LAN destination address and generating an incoming LAN frame.

2. A multiplexer as claimed in claim 1, wherein said LAN is an Ethernet network and said incoming LAN frame is an Ethernet frame.

3. A multiplexer (E-Mux) for segmenting a LAN frame into a plurality of ATM cells, comprising:

a frame manager for receiving an outgoing LAN frame with an ATM destination address and de-assembling it into a traffic type indicator, an AAL5 payload and an ATM destination address;

a header processor for receiving said traffic type indicator from said frame manager;

a PDU manager for receiving said AAL5 payload and said traffic type indicator and generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU);

an address processor for receiving said ATM destination address from said frame manager; and

a segmentation and reassembly unit for receiving said PDU and said ATM destination address generating a plurality of ATM cells with said ATM destination address.

4. A multiplexer as claimed in claim 3, wherein said LAN is an Ethernet network and said outgoing LAN frame is an Ethernet frame.

5. A multiplexer as claimed in claim 2, further comprising:

an E-Mux-to-Ethernet interface for formatting said Ethernet frame for transmission over the connection medium of an Ethernet network; and

an ATM-to-E-Mux interface for formatting said ATM cells received from an ATM network for processing by said E-Mux.

6. A multiplexer as claimed in claim 4, further comprising:

an E-Mux-to-ATM interface for formatting said ATM cells for transmission over the medium of an ATM network; and

an Ethernet-to-E-Mux interface for formatting said Ethernet frame received over a transmission medium of an Ethernet network for processing by said E-Mux.

7. An Ethernet network comprising a plurality of end stations and an Ethernet/ATM interface connected over a transmission medium, each end station comprising an address controller for forwarding an incoming LAN frame received from said Ethernet/ATM interface ATM network to said end station when a destination address comprised in the destination MAC field of said frame is recognized by said address controller, and for inserting an ATM destination address into the source MAC field of an outgoing frame destined to said Ethernet/ATM interface.

8. A telecommunication network comprising a LAN with a plurality of end-stations connected over a transmission medium and an ATM network, comprising:

a multiplexer (E-Mux) for encapsulating a plurality of incoming ATM cells received from said ATM network into an incoming LAN frame and for segmenting an outgoing LAN frame received from said LAN network into a plurality of outgoing ATM cells;

an E-Mux-to-LAN interface for formatting said incoming LAN frame for transmission over the connection medium of said LAN network, and for formatting said outgoing Ethernet frame received over the connection medium of said LAN network for processing by said E-Mux;

an ATM-to-E-Mux interface for formatting of said incoming ATM cells received from said ATM network for processing by said E-Mux, and for formatting said outgoing cells for transmission over the medium of said Ethernet network; and

an address controller at each end station for forwarding said incoming LAN frame to said end station when a destination address comprised in the destination MAC field of said incoming LAN frame is recognized by said address controller, and for inserting an ATM destination address into the source MAC field of said outgoing LAN frame, when said outgoing LAN frame is destined to said ATM network.

9. A method for transmitting information from an ATM network to an Ethernet network using an E-Mux performing the steps of:

establishing connection between an ATM switch of said ATM network and an end station of said Ethernet network based on a VPI/VCI destination address in the header of an incoming ATM cell;

receiving a plurality of incoming ATM cells with said destination address, and generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU);

extracting an AAL5 payload from said PDU;

extracting a traffic type indicator from the header of said PDU;

generating an incoming Ethernet frame using said traffic type indicator, said AAL5 payload and said destination address; and

transmitting said Ethernet frame over said Ethernet network to said end station according to said destination address.

10. A method as claimed in claim 9, wherein said incoming Ethernet frame comprises:

a destination MAC field including:

a unique ATM OUI identifier indicating that said incoming Ethernet frame comprises ATM traffic; and

said VPI/VCI destination address specifying the address of said end station;

a source MAC field including:

said ATM OUI identifier indicating that said incoming Ethernet frame comprises ATM traffic; and

a unique address of said E-Mux.

11. A method for transmitting information from an Ethernet network to an ATM network using an E-Mux performing the steps of:

establishing connection between an end station of said Ethernet network and an ATM switch of said ATM network based on a VPI/VCI destination address provided by said end station;

generating an outgoing Ethernet frame at said end station and transmitting same to said E-Mux;

extracting from said Ethernet outgoing frame a traffic type indicator, a frame payload and a source address;

generating an ATM adaptation layer 5 (AAL5) protocol data unit (PDU) from said frame payload and a traffic type indicator extracted from the type field of said outgoing frame; and

segmenting said PDU into a plurality of outgoing ATM cells and inserting a VPI/VCI destination address in the header of said cells from an address processor.

12. A method as claimed in claim 11, wherein said outgoing Ethernet frame comprises:

a destination MAC field including:

a unique ATM OUI identifier indicating that said outgoing Ethernet frame comprises ATM traffic; and

a unique address of said E-Mux;

a source MAC field including:

said ATM OUI identifier indicating that said outgoing Ethernet frame comprises ATM traffic; and

said VPI/VCI destination address specifying the address of said ATM cell.

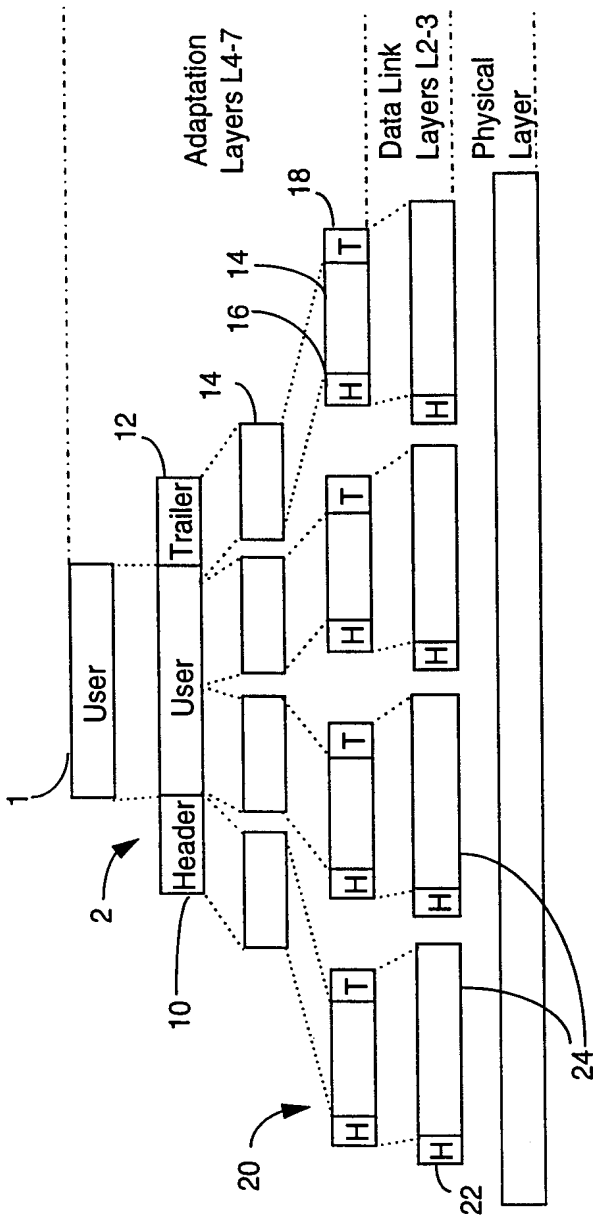


FIGURE 1A
(Prior Art)

FIGURE 1B (Prior Art)

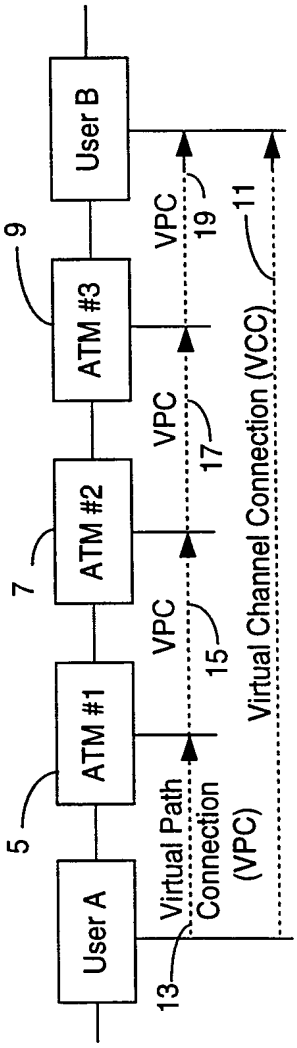


FIGURE 1C (Prior Art)

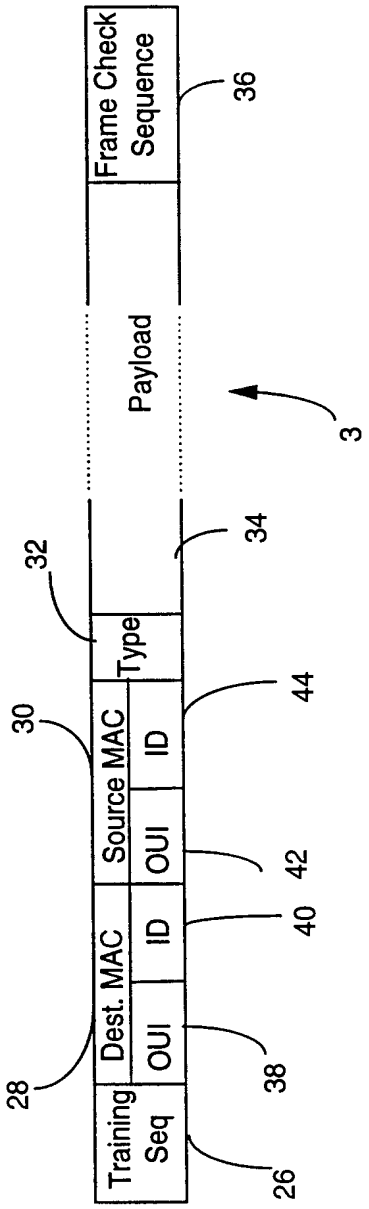


FIGURE 2

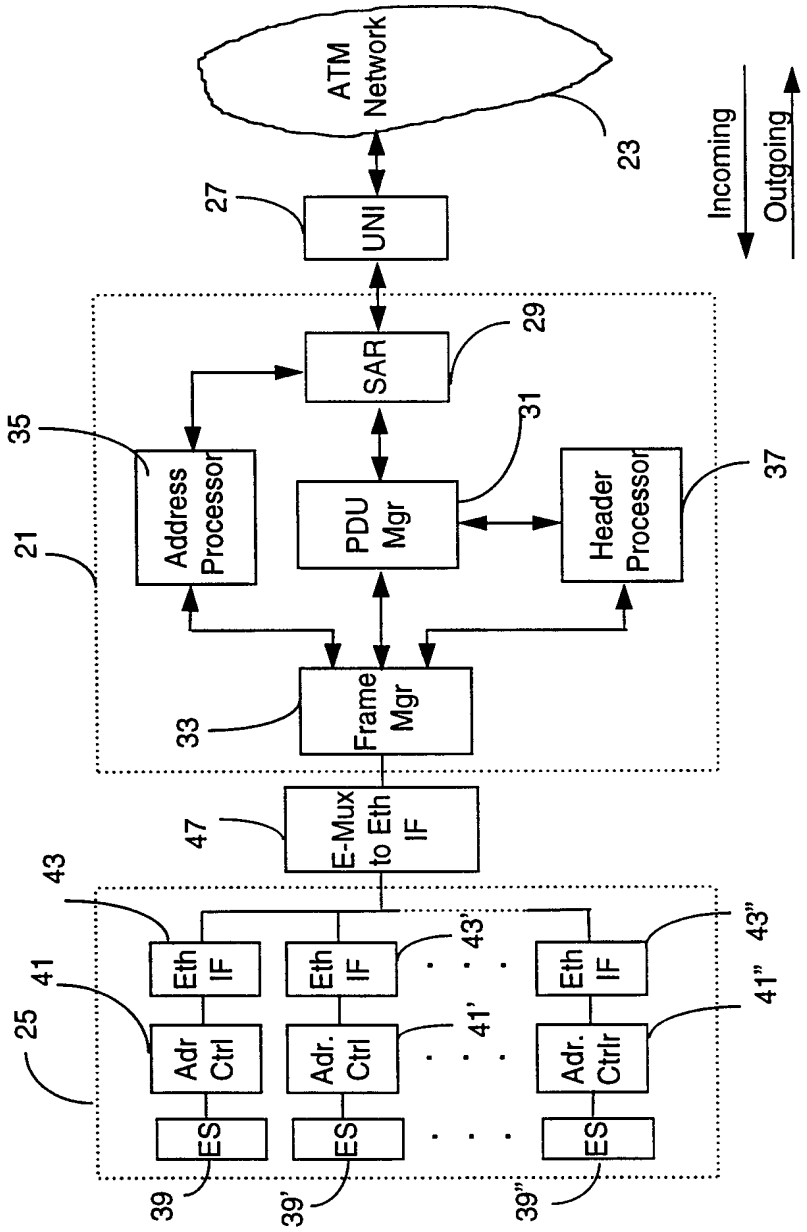

ATM Network
23
Incoming
Outgoing
27
UNI
29
SAR
31
35
Address Processor
PDU Mgr
Header Processor
37
21
33
Frame Mgr
47
E-Mux to Eth IF
43
43'
43"
Eth IF
41
41'
41"
25
Adr Ctrl
Adr. Ctrl
Adr. Ctrlr
ES
39
39'
39"

FIGURE 3A

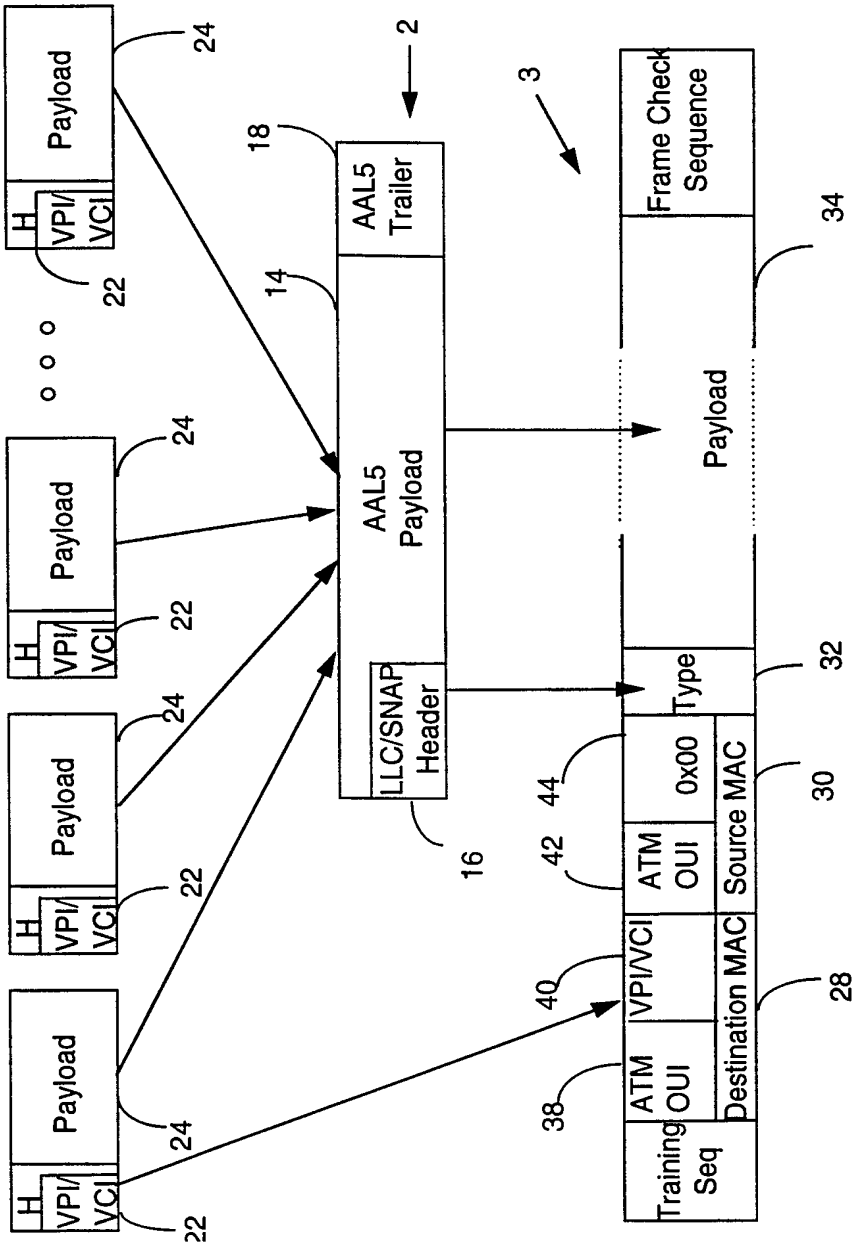

Payload
H
VPI/VCI
22
24
AAL5 Payload
AAL5 Trailer
LLC/SNAP Header
18
14
16
2
3
Frame Check Sequence
34
Type
32
0x00
ATM OUI
Source MAC
30
VPI/VCI
Destination MAC
28
Training Seq
ATM OUI
38
40
42
44

FIGURE 3B

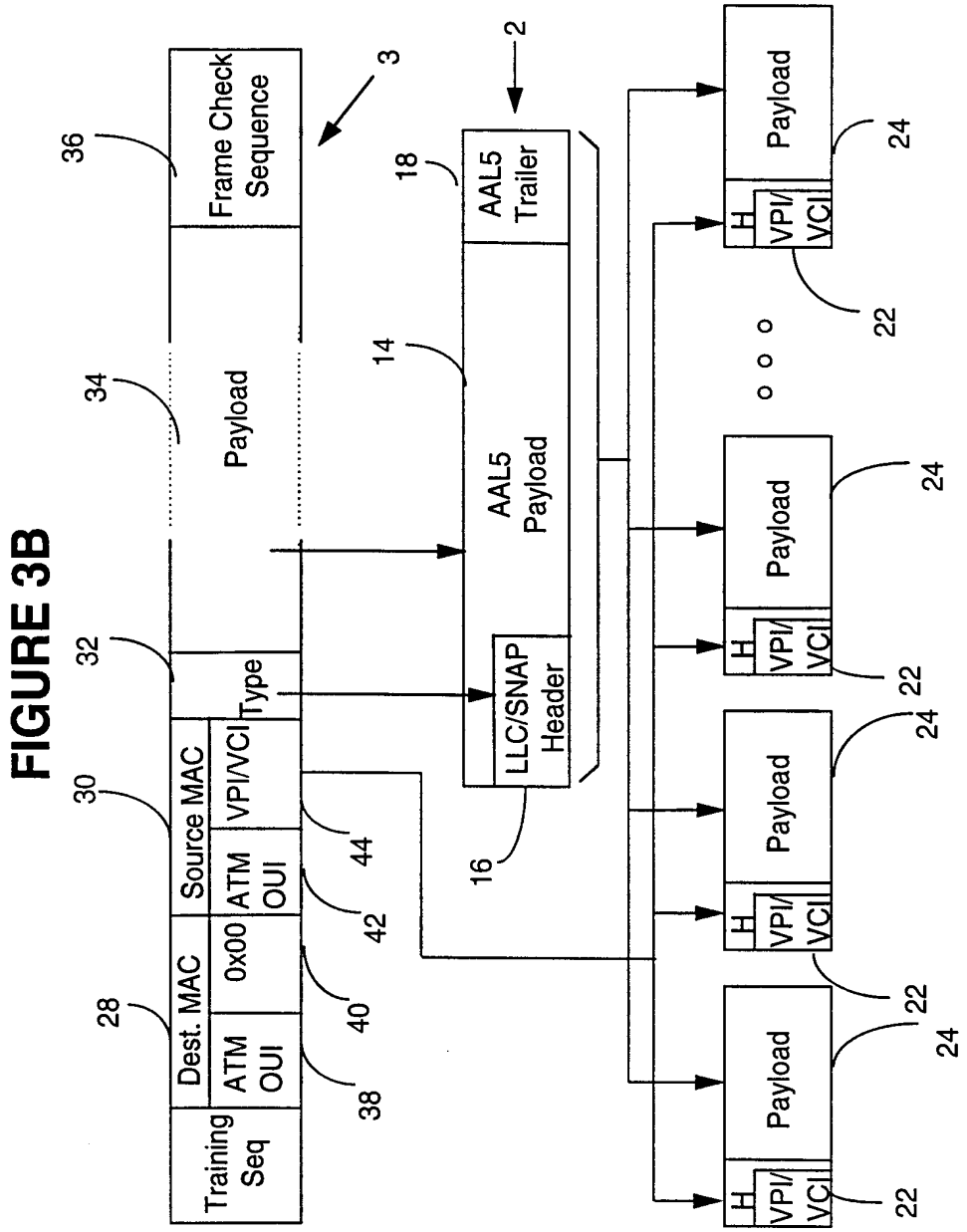

Training Seq
Dest. MAC
ATM OUI
0x00
Source MAC
ATM OUI
VPI/VCI
Type
Payload
Frame Check Sequence
AAL5 Payload
LLC/SNAP Header
AAL5 Trailer
H
VPI/VCI
Payload
28
30
32
34
36
38
40
42
44
14
16
18
22
24

FIGURE 4A

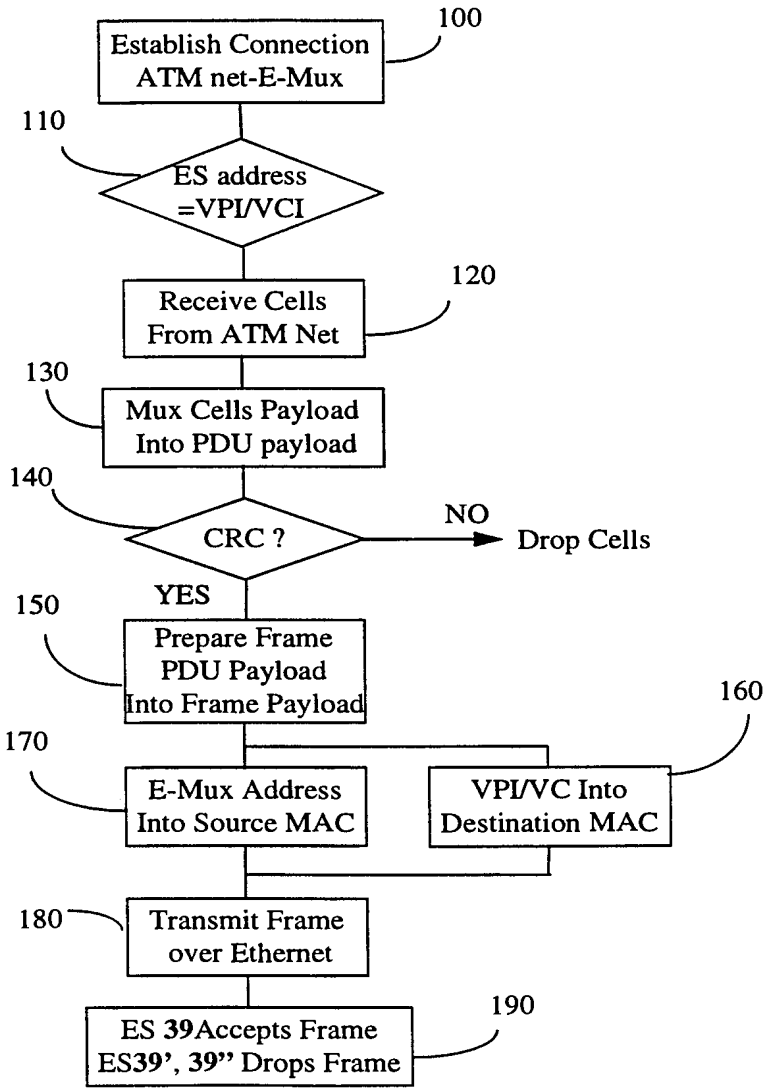

Establish Connection ATM net-E-Mux
100
110
ES address =VPI/VCI
120
Receive Cells From ATM Net
130
Mux Cells Payload Into PDU payload
140
CRC ?
NO
Drop Cells
YES
150
Prepare Frame PDU Payload Into Frame Payload
160
170
E-Mux Address Into Source MAC
VPI/VC Into Destination MAC
180
Transmit Frame over Ethernet
190
ES 39Accepts Frame ES39', 39" Drops Frame

FIGURE 4B

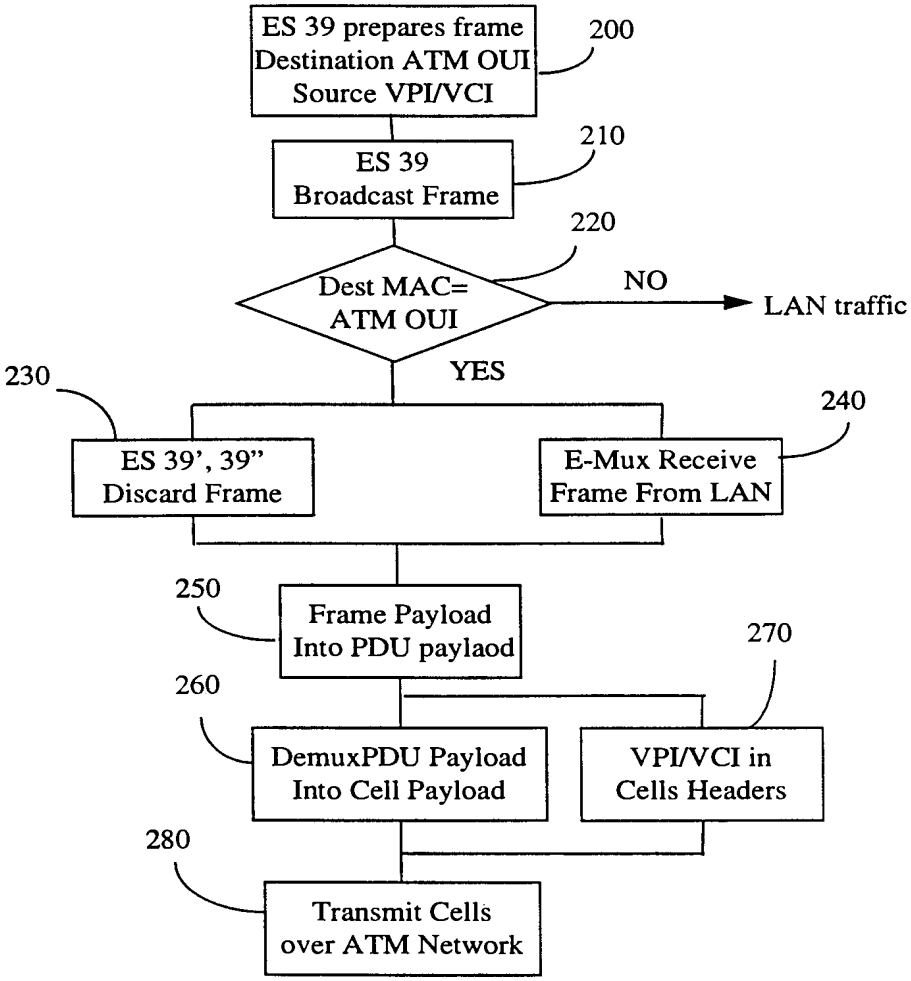

ES 39 prepares frame
Destination ATM OUI
Source VPI/VCI
200
ES 39
Broadcast Frame
210
220
Dest MAC=
ATM OUI
NO
LAN traffic
YES
230
240
ES 39', 39"
Discard Frame
E-Mux Receive
Frame From LAN
250
Frame Payload
Into PDU paylaod
270
260
DemuxPDU Payload
Into Cell Payload
VPI/VCI in
Cells Headers
280
Transmit Cells
over ATM Network

FIGURE 5

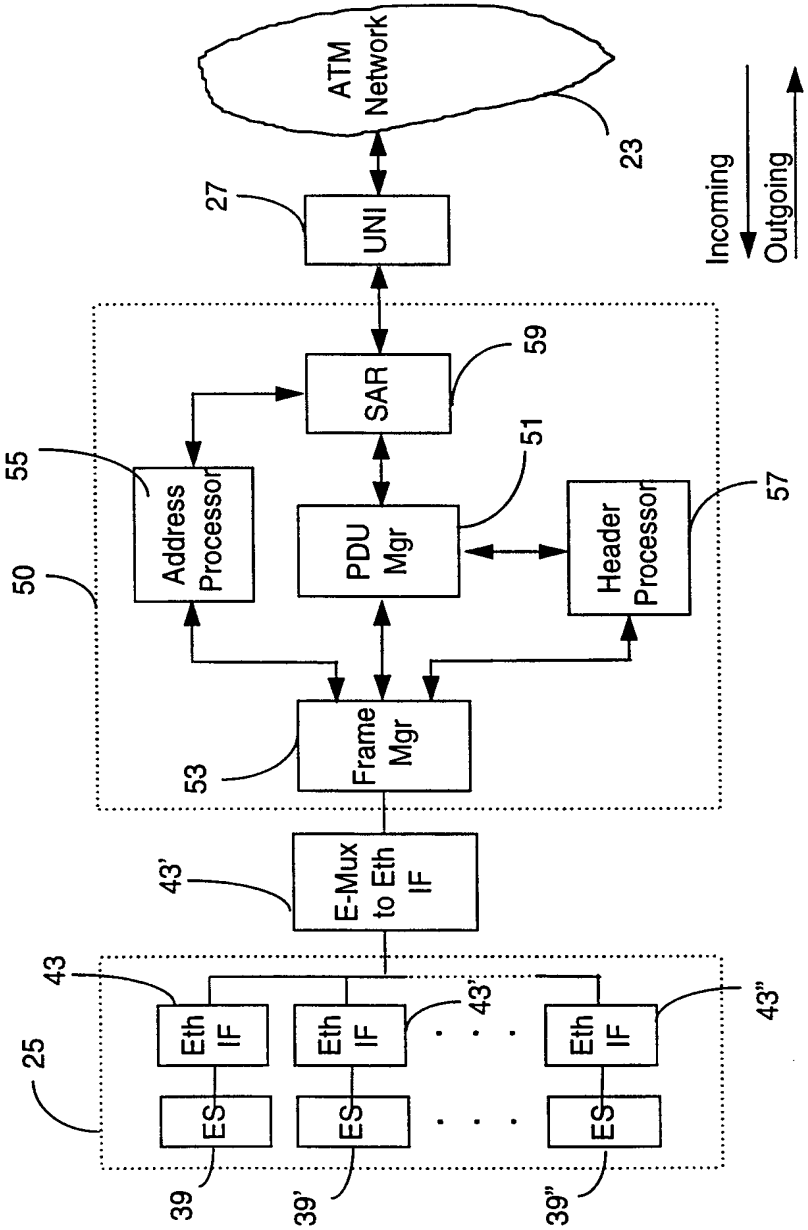
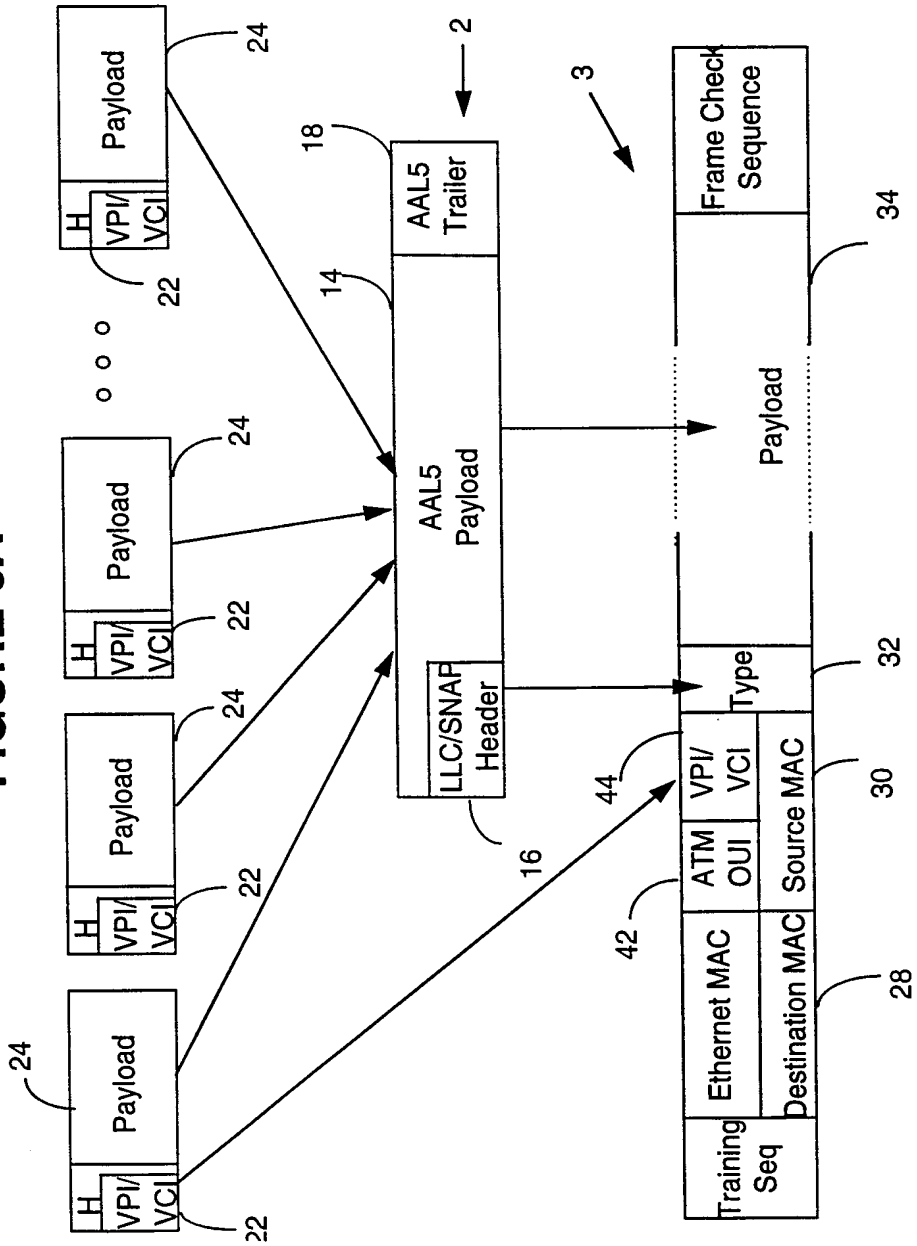

ATM Network
23
27
UNI
Incoming
Outgoing
59
SAR
55
Address Processor
51
PDU Mgr
Header Processor
57
50
53
Frame Mgr
43'
E-Mux to Eth IF
43
Eth IF
Eth IF
Eth IF
43"
25
ES
ES
ES
39
39'
39"

FIGURE 6A


Payload
H
VPI/
VCI
22
24
AAL5
Payload
AAL5
Trailer
LLC/SNAP
Header
18
14
16
2
3
Frame Check
Sequence
34
Payload
Type
32
VPI/
VCI
ATM
OUI
Source MAC
30
Ethernet MAC
Destination MAC
28
42
44
Training
Seq

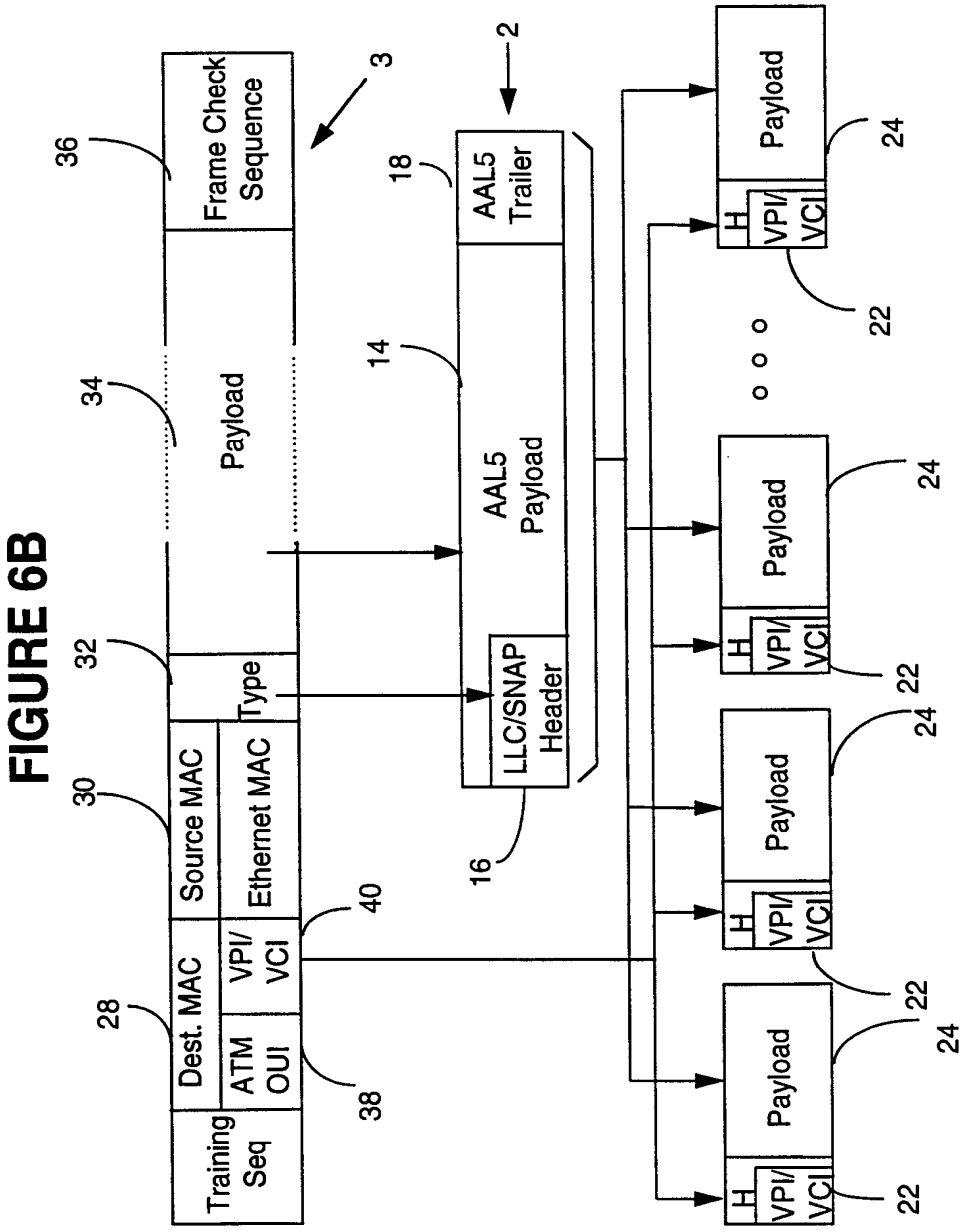

Training Seq
Dest. MAC
ATM OUI
VPI/ VCI
Source MAC
Ethernet MAC
Type
Payload
Frame Check Sequence
LLC/SNAP Header
AAL5 Payload
AAL5 Trailer
H
VPI/ VCI
Payload
28
30
32
34
36
38
40
14
16
18
22
24
2
3

FIGURE 6B

INTERNATIONAL SEARCH REPORT

Int. ..ational Application No
PCT/CA 98/00197

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/66 H04Q11/04

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04Q

Documentation searched other than minimumdocumentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CASTRO R ET AL: "SUPPORT OF DATA COMMUNICATIONS IN AN ATM LAN" INFORMATION NETWORKS AND DATA COMMUNICATION, PROCEEDINGS OF THE IFIP TC6 INTERNATIONAL CONFERENCE ON INFORMATION NETWORKS AND DATA COMMUNICATION, FUNCHAL, MADEIRA ISLAND, PORTUGAL, APR. 18 - 21, 1994, no. CONF. 5, 18 April 1994, VEIGA P;DIPAK KHAKHAR (EDS), pages 277-295, XP000593298 see paragraph 2.3.4 --- -/--	1-9,11

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of theinternational search	Date of mailing of the international search report
17 June 1998	26/06/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Staessen, B

2

Form PCT/ISA/210 (second sheet) (July 1992)

Petitioner Apple Inc. - Exhibit 1026, p. 1134

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 98/00197

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	SMITH J C: "10MBPS TO 155MBPS ATM USING THE IDT SARAMTM AS A CONCENTRATOR BROUTER CORE" WESCON '94. WESTERN ELECTRONIC SHOW AND CONVENTION, ANAHEIM, SEPT. 27 - 29, 1994, 27 September 1994, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, pages 495-502, XP000532615 paragraph "ATM Packet structuring" ---	1-12
A	MIRCHANDANI V ET AL: "AN INTERNETWORKING ARCHITECTURE FOR INTEGRATED VOICE AND DATA COMMUNICATIONS" PROCEEDINGS OF THE REGION 10 ANNUAL INTERNATIONAL CONFERENCE (TENCO, SINGAPORE, 22 - 26 AUG., 1994, vol. VOL. 2, no. CONF. 9, 22 August 1994, CHAN T K Y (ED), pages 749-753, XP000528218 see paragraph 3 ---	1-12
A	CAMARDA P ET AL: "A ROUTER FOR THE INTERCONNCETION OF ETHERNET LOCAL AREA NETWORKS VIA AN ATM NETWORK" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON INTEGRATED BROADBAND SERVICES AND NETWORKS, LONDON, 15 - 18 OCT., 1990, no. -, 15 October 1990, INSTITUTION OF ELECTRICAL ENGINEERS, pages 283-288, XP000410619 paragraph "Router Description"; ---	1-12
A	PAONE R ET AL: "FEASIBILITY MODEL OF A FLEXIBLE BUSINESS CUSTOMER PREMISES NETWORK" ELECTRONICS AND COMMUNICATION ENGINEERING JOURNAL, vol. 4, no. 4, 1 August 1992, pages 215-224, XP000307899 see page 222 see page 223 -----	1-12

2

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

Petitioner Apple Inc. - Exhibit 1026, p. 1135

Electronic Acknowledgement Receipt

EFS ID:	9761875
Application Number:	11679416
International Application Number:	
Confirmation Number:	3528
Title of Invention:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Hasan M. Rashid/Melissa Molchan
Filer Authorized By:	Hasan M. Rashid
Attorney Docket Number:	77580-015 (VRNK-1CP2DVCN)
Receipt Date:	29-MAR-2011
Filing Date:	27-FEB-2007
Time Stamp:	13:40:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	0015IDS.pdf	125624 1ff39a6fc9f504d42b6422961d90959001fc9b4e	no	2

Warnings:	
Information:	

This is not an USPTO supplied IDS fillable form					
2	Foreign Reference	WO9843396.pdf	1348054 02fb89aa88c9d669c72e526b2d6b8ded86400824	no	37
Warnings:					
Information:					
3	NPL Documents	101EPSearchReport.pdf	316610 3c556bd662e25af934512ea23fc10a393885c6e0	no	7
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
4	NPL Documents	105EPSearchReport.pdf	216885 f55eea81ea84e25bf6755cf8572244c2c2a61312	no	6
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
5	NPL Documents	Hollenbeck.pdf	2638150 c8d6d8db4c54893bb4e2b3e2e62315fb1adb77b5	no	34
Warnings:					
Information:					
6	NPL Documents	2NOA0057.pdf	2721824 f8e309ce9dee16e42daecb0b92faae39880f762a	no	34
Warnings:					
Information:					
7	NPL Documents	Tannenbaum.pdf	853980 aef4faaf476d56146d79ce1cc0a775fb29459767	no	18
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
Total Files Size (in bytes):			8221127		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Larson et al.
Application Serial No.:	11/679,416
Filing Date:	February 27, 2007
Title:	METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK
Examiner:	Lim, Krisna
Art Unit:	2453
Confirmation No.:	33528
Atty. Docket No.:	077580-0015 (VRNK-1CP2DVCON)

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE AND REQUEST FOR RECONSIDERATION

The Applicants responds to the non-final Office Action mailed December 7, 2010 ("the Office Action") as follows:

Remarks, beginning on page 2 of this paper.

Petitioner Apple Inc. - Exhibit 1026, p. 1139

Remarks

Applicants appreciate the Examiner's examination of the subject application. Claims 2-30 are currently pending. No claims have been amended or cancelled.

In the Office Action, the Examiner has rejected Claims 2-30 under 35 U.S.C. § 102(b), as being anticipated by Aventail Connect v 3.1/v2.6 Administrator's Guide ("Aventail").

Applicants respectfully traverse the outstanding rejection and requests reconsideration of the subject application in light of the following remarks.

Patentability under 35 U.S.C. § 102

The Examiner has rejected Claims 2-30 under 35 U.S.C. § 102(b), as being anticipated by Aventail. These rejections are respectfully traversed, and reconsideration and withdrawal of these rejections are respectfully requested.

Independent claim 2 recites the following:

> A method of using a first device to communicate with a second device having a **secure name**, the method comprising:
>
> from the first device, sending a message to a **secure name service**, the message requesting a network address associated with the **secure name** of the second device;
>
> at the first device, receiving a message containing the network address associated with the **secure name** of the second device; and
>
> from the first device, sending a message to the network address associated with the **secure name** of the second device using **a secure communication link**.

(emphasis added).

As a preliminary matter, Aventail has not been shown to be prior art to all pending claims in the present application, including claim 2. In fact, Aventail is not prior art. The present application claims priority to U.S. Patent Nos. 6,502,135 (hereinafter "the '135 patent") and 7,188,180 (hereinafter "the '180 patent"). The '135 and '180 Patents were subject to inter partes reexamination proceedings, Control Nos. 95/001,269 (hereinafter "the '269 Reexam") and

Petitioner Apple Inc. - Exhibit 1026, p. 1140

95/001,270 (hereinafter "the '270 Reexam"), respectively (collectively "Reexams"). In both Reexams, the USPTO determined that "Aventail cannot be relied upon as prior art to the [patents]." *See* Reexamination Control No. 95/001,269, Action Closing Prosecution, June 16, 2010, p. 3 (Exhibit A); Reexamination Control No. 95/001,270, Action Closing Prosecution, June 16, 2010, p. 3 (Exhibit B). This sound determination was based on the fact that no evidence was found to establish Aventail's publication date.

Indeed, Aventail's identification of a copyright date range of 1996 – 1999 is not equivalent to a publication date. The distinction between a publication date and a copyright date is critical. To establish a date of publication, the reference must be shown to have "been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it." *In re Wyre*, 655 F.2d 221 (C.C.P.A. 1981). Aventail, on its face, provides "© 1996-1999 Aventail Corporation." The copyright date does not meet this standard. Unlike a publication date, a copyright date merely establishes "the date that the document was created or printed." *Hilgraeve, Inc. v. Symantec Corp.*, 271 F. Supp. 2d 964, 975 (E.D. Mich. 2003).

Even presuming the author of the document accurately represented the date the document was created, a creation date alone is not evidence of any sort of publication or dissemination. Without more, this bald assertion of the creation of the document does not meet the "publication" standard required for a document to be relied upon as prior art.

Further exacerbating matters is the filing date of the '135 Patent: February 15, 2000. Suppose the relied upon sections of the Aventail reference were created on December 31, 1999, and the copyright date range were accordingly amended to read "1996-1999." Under these circumstances, it is possible that the document, although created, was not made publicly

Petitioner Apple Inc. - Exhibit 1026, p. 1141

available until after the filing date of the '135 Patent, six weeks after creation. And, under these circumstances, Aventail clearly would not be eligible to be relied upon as prior art to the '135 Patent.

As an aside, the Applicant notes that the present assignee (VirnetX Inc.) and its prosecution counsel have been accused of inequitable conduct during the '269 Reexam in a litigation proceeding, *VirnetX Inc. v. Cisco Systems, Inc., et al.*, United States District Court for the Eastern District of Texas, Tyler Division, Case No. 6:10-cv-417. Exhibits C-E. In its Original Answer, Affirmative Defenses, and Counterclaims to the Virnetx's Original Complaint, the Defendant Apple Inc. ("Apple") alleges that evidence of Aventail's publication as early as June 1999 was presented in a different trial involving Microsoft Corporation. Exhibit C at ¶ 23 (p. 14). Apple further alleges that "VirnetX was aware that the Aventail reference may have been published at least as early as June 1999." Exhibit C at ¶ 23. Defendants Aastra Technologies Limited and Aastra USA Inc. ("Aastra") have made similar allegations in their responsive pleadings. Exhibit D at ¶ 86 (p. 19); Exhibit E at ¶ 86 (p. 19).

To the contrary, the applicants are unaware of evidence establishing Aventail's publication date, and specifically are unaware of the June 1999 publication date alleged by Apple and Aastra in their pleadings. The trial transcript from the Microsoft trial does not discuss anything about a publication date for the Aventail reference. Exhibit F. While the trial transcript references the Aventail product, it does not mention anything about a publication date. *See e.g.* Exhibit F-2, pp. 112, 146; Exhibit F-3, pp. 115, 119-20; Exhibit F-10 pp. 21-40; Exhibit F-11, pp. 21-32, 120-150. The deposition of Gary Tomlinson (former employee of Aventail) taken during discovery prior to the Microsoft trial is inconclusive, at best. Exhibit H at pp. 33-36. Thus, although an allegation of knowledge has been made by a third party, the applicants, the

Petitioner Apple Inc. - Exhibit 1026, p. 1142

assignee and applicants' prosecution counsel have not had and do not have such knowledge. To be sure, the Applicants will notify the USPTO immediately if it becomes aware of evidence of Aventail's publication date.

Assuming *arguendo*, that Aventail is prior art to the present application, it is not understood to disclose the features of claim 2, particularly with respect to at least the features of "a **secure** communication link," "a **secure** name service," and a "**secure** name."

Aventail's disclosure was summarized in the Declaration of Professor Jason Nieh in support of the '270 Reexam. Reexamination Control No. 95/001,270, *Declaration of Jason Nieh, Ph.D., Pursuant to 37 C.F.R. § 1.132*, April 19, 2010, ¶¶ 14 – 29 (Exhibit G) (hereinafter "Nieh Decl."). The Nieh Decl. is cited herein to characterize the cited references and their deficiencies.

Aventail discloses a system and architecture for transmitting data between two computers using the SOCKS protocol. Nieh Decl. at ¶ 14. The system routes certain, predefined network traffic from a WinSock (Windows sockets) application to an extranet (SOCKS) server, possibly through successive servers. Aventail at 7; Nieh Decl. at ¶ 14. Upon receipt of the network traffic, the SOCKS server then transmits the network traffic to the Internet or external network. Aventail at 7; Nieh Decl. at ¶ 14. Aventail's disclosure is limited to connections created at the socket layer of the network architecture. Nieh Decl. at ¶ 14.

In operation, a component of the Aventail Connect software described in the reference resides between WinSock and the underlying TCP/IP stack. *See* Aventail at 9; Nieh Decl. at ¶ 15. The Aventail Connect software intercepts all connection requests from the user, and determines whether each request matches local, preset criteria for redirection to a SOCKS server. *See* Aventail at 10; Nieh Decl. at ¶ 15. If redirection is appropriate, then Aventail Connect

Petitioner Apple Inc. - Exhibit 1026, p. 1143

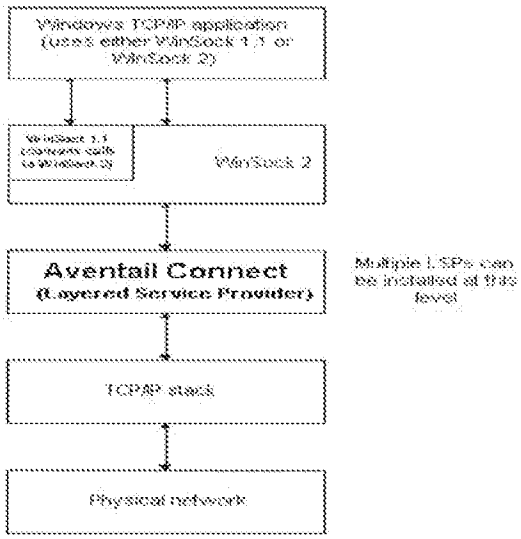
creates a false DNS entry to return to the requesting application. *See* Aventail at 12; Nieh Decl. at ¶ 16. Aventail discloses that Aventail Connect then forwards the destination hostname to the extranet SOCK server over a SOCKS connection. *See* Aventail at 12; Nieh Decl. at ¶ 16. The SOCKS server performs the hostname resolution. Aventail at 12; Nieh Decl. at ¶ 17. Once the hostname is resolved, the user can transmit data over a SOCKS connection to the SOCKS server. Nieh Decl. at ¶ 17. The SOCKS server, then, separately relays that transmitted data to the target. Nieh Decl. at ¶ 17.

Aventail fails to disclose "a **secure** name service" and a "**secure** name." Aventail discloses conventional domain name services and domain names. Indeed, in reexamination of the '180 Patent, the Patent Office found that Aventail discloses a conventional "DNS server and the creation of a secure tunnel to a secure remote site." Reexamination Control No. 95/001,270, Action Closing Prosecution, June 16, 2010, Exhibit B, at ¶¶ 6-7. Aventail does not disclose a non-conventional system. *Id.* In contrast to Aventail, paragraphs [0318] – [0320] of the present application distinguish the claimed invention from conventional systems. *See, generally,* Nieh Dec. at ¶ 10-13.

Aventail also does not teach the claimed secure communication link. First, Aventail has not been shown to demonstrate that computers connected via the Aventail system are able to communicate with each other as though they were on the same network. *Id.* at ¶ 25. Aventail discloses establishing point-to-point SOCKS connections between a client computer and a SOCKS server. *Id.* The SOCKS server then relays data received to the intended target. *Id.* Aventail does not disclose a secure communication link, where data can be addressed to a target, regardless of the location of the target. *See, generally, id.*, ¶¶ 24-27.

Petitioner Apple Inc. - Exhibit 1026, p. 1144

Second, according to Aventail, Aventail Connect's fundamental operation is incompatible with users transmitting data that are sensitive to network information. *Id.* at ¶ 28. As stated above, Aventail discloses that Aventail Connect operates between the WinSock and TCP/IP layers, as depicted on page 9:



Aventail at 9; *id.* Because Aventail discloses that Aventail Connect operates between these layers, it can intercept DNS requests. Nieh Decl. at ¶ 28. Aventail discloses that Aventail Connect intercepts certain DNS requests and returns a false DNS response to the user if the requested hostname matches a hostname on a user-defined list. *Id.* Accordingly, Aventail discloses that the user will receive false network information from Aventail Connect for these hostnames. *Id.* If the client computer hopes to transfer to the target data that is sensitive to network information, Aventail Connect's falsification of the network information would prevent the correct transfer of data. *Id.* Aventail has not been shown to disclose a secure communication link.

Petitioner Apple Inc. - Exhibit 1026, p. 1145

Third, Aventail has not been shown to disclose a secure communication link because computers connected according to Aventail do not communicate directly with each other. *Id.* at ¶ 29. Aventail discloses a system where a client on a public network transmits data to a SOCKS server via a singular, point-to-point SOCKS connection at the socket layer of the network architecture. *Id.* The SOCKS server then relays that data to a target computer on a private network on which the SOCKS server also resides. *Id.* All communications between the client and target stop and start at the intermediate SOCKS server. *Id.* The client cannot open a connection with the target itself. Therefore, one skilled in the art would not have considered the client and target to be virtually on the same private network. *Id.* Instead, the client computer and target computer are deliberately separated by the intermediate SOCKS server. *Id.* For these reasons, Aventail not only fails to disclose the claimed secure communication link.

For all these reasons, Applicant respectfully submits that Aventail does not disclose the elements of independent claim 2. Applicant respectfully submits that claim 2 is in condition for allowance. Reconsideration and withdrawal of the rejection of independent claim 2 is respectfully requested.

Independent claims 24, 26, and 28-30 recite one or more of "a secure name," "a secure name service," or "a secure communication link." For the reasons stated above, Applicant respectfully submits that claims 24, 26, and 28-30 are in condition for allowance. Reconsideration and withdrawal of the rejection of independent claim 2 is respectfully requested.

The other claims currently under consideration in the application are dependent from their respective independent claims discussed above and therefore are believed to be allowable over the applied references for at least the reasons provided above for their respective independent claims. Because each dependent claim is deemed to define an additional aspect of

Petitioner Apple Inc. - Exhibit 1026, p. 1146

the invention, the individual consideration of each on its own merits is respectfully requested. Reconsideration and withdrawal of the rejections of the dependent claims are respectfully requested.

The absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be other reasons for patentability of any or all claims that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede, or an actual concession of, any issue with regard to any claim, or any cited art, except as specifically stated in this paper, and the amendment or cancellation of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment or cancellation.

Petitioner Apple Inc. - Exhibit 1026, p. 1147

CONCLUSION

In light of the Amendments and Remarks herein, the Applicant submits that the pending claims, claims 2-30, are in condition for allowance and respectfully requests a notice to this effect. Should the Examiner have any questions, please call the undersigned at the phone number listed below.

To the extent necessary, a petition for an extension of time (3 months) under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 501133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

/Toby H. Kusmer/ Date: June 7, 2011

Toby H. Kusmer
Registration No. 26,418
28 State Street
Boston, MA 02109
Phone: 617-535-4065
Facsimile: 617-535-3800
Date: June 7, 2011

Please recognize our Customer No. 23630 as our correspondence address.

DM_US 28866337-1.077580.0015

Petitioner Apple Inc. - Exhibit 1026, p. 1148

EXHIBIT A

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,269	12/08/2009	6502135	77580-89	2038

23630 7590 06/16/2010

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
06/16/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
1425 K STREET N.W.
SUITE 800
WASHINGTON, D.C.

Date: MAILED

JUN 16 2010

CENTRAL REEXAMINATION UNIT

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001269
PATENT NO. : 6502135
TECHNOLOGY CENTER : 3999
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified Reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

PTOL-2070(Rev.07-04)

ACTION CLOSING PROSECUTION (37 CFR 1.949)	Control No.	Patent Under Reexamination	
	95/001,269	6502135	
	Examiner	Art Unit	
	ANDREW L. NALVEN	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Responsive to the communication(s) filed by:
Patent Owner on 15 April 2010
Third Party(ies) on 18 May 2010

Patent owner may once file a submission under 37 CFR 1.951(a) within 1 month(s) from the mailing date of this Office action. Where a submission is filed, third party requester may file responsive comments under 37 CFR 1.951(b) within 30-days (not extendable- 35 U.S.C. § 314(b)(2)) from the date of service of the initial submission on the requester. **Appeal cannot be taken from this action.** Appeal can only be taken from a Right of Appeal Notice under 37 CFR 1.953.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

PART I. THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☐ Notice of References Cited by Examiner, PTO-892
2. ☒ Information Disclosure Citation, PTO/SB/08
3. ☐ _____

PART II. SUMMARY OF ACTION:

1a. ☒ Claims 1-10,12 and 18 are subject to reexamination.
1b. ☐ Claims _____ are not subject to reexamination.
2. ☐ Claims _____ have been canceled.
3. ☒ Claims 1-10 and 12 are confirmed. [Unamended patent claims]
4. ☒ Claims 18 are patentable. [Amended or new claims]
5. ☐ Claims _____ are rejected.
6. ☐ Claims _____ are objected to.
7. ☐ The drawings filed on _____ ☐ are acceptable ☐ are not acceptable.
8 ☐ The drawing correction request filed on _____ is: ☐ approved. ☐ disapproved.
9 ☐ Acknowledgment is made of the claim for priority under 35 U.S.C. 119 (a)-(d). The certified copy has:
☐ been received. ☐ not been received. ☐ been filed in Application/Control No _____
10. ☐ Other _____

ACTION CLOSING PROSECUTION

This Action Closing Prosecution is responsive to the amendment and arguments filed by the patent owner on April 15, 2010 and the notice of non-participation filed by Third Party Requestor on May 18, 2010.

Receipt of Papers

1. On April 15, 2010, Patent Owner filed a response to the 1/15/2010 office action.

2. On May 18, 2010, Third Party Requestor ("Requestor") filed a notice of non-participation in the present *inter partes* reexamination. The notice indicated that no response to the 1/15/2010 office action would be submitted by the Requestor and that the Requestor will not be further participating in this proceeding.

Rejections Proposed by Requestor – Previously Adopted, Now Not Adopted

3. Requestor proposed that claims 1, 3, 4, 6-10 and 12 be rejected under 35 US C 102(a) as being anticipated by Aventail. This proposed rejection was adopted in the first Office action mailed on 1/15/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

4. Patent owner argues that the rejection of claims 1, 3, 4, 6-10, and 12 as anticipated by Aventail should be withdrawn because Aventail is not prior art to the patent under reexamination, US Patent No. 6,502,135 ("the '135 patent"). Specifically, Patent Owner argued that the request and the 1/15/2010 office action did not show that Aventail was published prior to the priority date of the '135 patent. The request asserts that Aventail was published between

1996 and 1999. This assertion was based on the document's copyright date. The request did not set forth any further evidence of the date of publication.

5. A search was conducted to determine the publication date of the Aventail reference. However, no evidence was found that established the publication date. Accordingly, Aventail cannot be relied upon as prior art to the '135 patent and all rejections based upon Aventail are hereby withdrawn and not adopted.

Rejections Proposed by Requestor – Previously Not Adopted That Remain Not Adopted

6. The non-final action mailed on January 15, 2010 is hereby incorporated by reference.

7. Requestor proposed that claims 2 and 5 be rejected under 35 US C 102(a) as being anticipated by Aventail. This proposed rejection was not adopted for the reasons set forth on Pages 9-12 of the January 15, 2010 non-final office action.

8. Requestor proposed that claims 1-10 and 12 be rejected under 35 US C 102(b) as being anticipated by Kosiuer. This proposed rejection was not adopted for the reasons set forth on Pages 12-14 of the January 15, 2010 non-final office action.

9. Requestor proposed that claims 3, 6, and 8 be rejected under 35 US C 103(a) as being rendered obvious by VPN Overview in view of Aventail. This proposed rejection was not adopted for the reasons set forth on Page 14 of the January 15, 2010 non-final office action.

STATEMENT OF REASONS FOR PATENTABILITY AND/OR CONFIRMATION

The following is an examiner's statement of reasons for patentability and/or confirmation of the claims found patentable in this reexamination proceeding:

Claims 1, 3, 4, 6-10, 12, and 18 are confirmed as patentable for the following reasons. As noted above, Aventail is not prior art to the '135 patent. Accordingly, the remaining cited prior art includes the Gauntlet, Kosiur, Microsoft VPN, VPN Overview, and RFC 1035 references. These references do not anticipate or render obvious claims 1, 3, 4, 6-10, 12, and 18 because they fail to teach or suggest the feature of "in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer" as set forth in claim 1 and similarly set forth in claims 10 and 18.

Claims 2 and 5 are confirmed as patentable for the reasons set forth in the January 15, 2010 non-final office action on pages 10-12. New claim 18 is further confirmed as patentable because of its inclusion of the subject matter of claims 2 and 5.

Any comments considered necessary by the PATENT OWNER regarding the above statement must be submitted promptly to avoid processing delays. Such submission by the patent owner should be labeled: "Comments on Statement of Reasons for Patentability and/or Confirmation" and will be placed in the reexamination file.

ACTION CLOSING PROSECUTION

This is an ACTION CLOSING PROSECUTION (ACP); see MPEP § 2671.02.

(1) Pursuant to 37 CFR 1.951(a), the patent owner may once file written comments limited to the issues raised in the reexamination proceeding and/or present a proposed amendment to the claims which amendment will be subject to the criteria of 37 CFR 1.116 as to whether it shall be entered and considered. Such comments and/or proposed amendments must

be filed within a time period of 30 days or one month (whichever is longer) from the mailing date of this action. Where the patent owner files such comments and/or a proposed amendment, the third party requester may once file comments under 37 CFR 1.951(b) responding to the patent owner's submission within 30 days from the date of service of the patent owner's submission on the third party requester.

(2) If the patent owner does not timely file comments and/or a proposed amendment pursuant to 37 CFR 1.951(a), then the third party requester is precluded from filing comments under 37 CFR 1.951(b).

(3) Appeal **cannot** be taken from this action, since it is not a final Office action.

All correspondence relating to this *inter partes* reexamination proceeding should be directed:

By Mail to: Mail Stop *Inter Partes* Reexam
Attn: Central Reexamination Unit
Commissioner of Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany St.
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:

/Andrew Nalven/

Andrew Nalven
CRU Examiner
GAU 3992
(571) 272-3839

Conferee: ESK

Conferee: JBF

EXHIBIT B

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/001,270	12/08/2009	7188180	077580-0090	2128

23630 7590 06/16/2010

McDermott Will & Emery
600 13th Street, NW
Washington, DC 20005-3096

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
06/16/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
1425 K STREET N.W.
SUITE 800
WASHINGTON, D.C. 20005

Date:

MAILED

JUN 16 2010

CENTRAL REEXAMINATION UNIT

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NO. : 95001270
PATENT NO. : 7188180
TECHNOLOGY CENTER : 3999
ART UNIT : 3992

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified Reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the inter partes reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an ex parte reexamination has been merged with the inter partes reexamination, no responsive submission by any ex parte third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the Central Reexamination Unit at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

PTOL-2070(Rev.07-04)

ACTION CLOSING PROSECUTION (37 CFR 1.949)	Control No.	Patent Under Reexamination	
	95/001,270	7188180	
	Examiner	Art Unit	
	ANDREW L. NALVEN	3992	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Responsive to the communication(s) filed by:
Patent Owner on 19 April 2010
Third Party(ies) on 18 May 2010

Patent owner may once file a submission under 37 CFR 1.951(a) within 1 month(s) from the mailing date of this Office action. Where a submission is filed, third party requester may file responsive comments under 37 CFR 1.951(b) within 30-days (not extendable- 35 U.S.C. § 314(b)(2)) from the date of service of the initial submission on the requester. **Appeal cannot be taken from this action.** Appeal can only be taken from a Right of Appeal Notice under 37 CFR 1.953.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

PART I. THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☐ Notice of References Cited by Examiner, PTO-892
2. ☒ Information Disclosure Citation, PTO/SB/08
3. ☐ _____

PART II. SUMMARY OF ACTION:

1a. ☒ Claims 1,4,10,12-15,17,20,26,28-31,33 and 35 are subject to reexamination.
1b. ☒ Claims 2,3,5-9,11,16,18,19,21-25,27,32,34 and 36-41 are not subject to reexamination.
2. ☐ Claims _____ have been canceled.
3. ☒ Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are confirmed. [Unamended patent claims]
4. ☐ Claims _____ are patentable. [Amended or new claims]
5. ☐ Claims _____ are rejected.
6. ☐ Claims _____ are objected to.
7. ☐ The drawings filed on _____ ☐ are acceptable ☐ are not acceptable.
8 ☐ The drawing correction request filed on _____ is: ☐ approved. ☐ disapproved.
9 ☐ Acknowledgment is made of the claim for priority under 35 U.S.C. 119 (a)-(d). The certified copy has:
☐ been received. ☐ not been received. ☐ been filed in Application/Control No _____
10. ☐ Other _____

ACTION CLOSING PROSECUTION

This Action Closing Prosecution is responsive to the amendment and arguments filed by the patent owner on April 19, 2010 and the notice of non-participation filed by Third Party Requestor on May 18, 2010.

Receipt of Papers

1. On April 19, 2010, Patent Owner filed a response to the 1/19/2010 office action.

2. On May 18, 2010, Third Party Requestor ("Requestor") filed a notice of non-participation in the present *inter partes* reexamination. The notice indicated that no response to the 1/19/2010 office action would be submitted by the Requestor and that the Requestor will not be further participating in this proceeding.

Rejections Proposed by Requestor – Previously Adopted, Now Not Adopted

3. Requestor proposed that claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 be rejected under 35 US C 102(a) as being anticipated by Aventail. This proposed rejection was adopted in the first Office action mailed on 1/19/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

4. Patent owner argues that the rejection of claims 1, 10, 12, 14, 17, 26, 28, 30, 31, and 33 as anticipated by Aventail should be withdrawn because Aventail is not prior art to the patent under reexamination, US Patent No. 7,188,180 ("the '180 patent"). Specifically, Patent Owner argued that the request and the 1/19/2010 office action did not show that Aventail was published

prior to the priority date of the '180 patent. The request asserts that Aventail was published between 1996 and 1999. This assertion was based on the document's copyright date. The request did not set forth any further evidence of the date of publication.

5. A search was conducted to determine the publication date of the Aventail reference. However, no evidence was found that established the publication date. Accordingly, Aventail cannot be relied upon as prior art to the '180 patent and all rejections based upon Aventail are hereby withdrawn and not adopted.

6. Further, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

7. Aventail does not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. Aventail teaches the use of a DNS server and the creation of a secure tunnel to a secure remote site. However, Aventail does not teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. For this additional reason the proposed rejection is not adopted.

8. Requestor proposed that claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 be rejected under 35 USC 103(a) as being rendered obvious by the combination of VPN Overview in view of RFC 1035. This proposed rejection was adopted in the first Office action mailed on 1/19/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

9. Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent

distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

10. VPN Overview and RFC 1035 do not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. RFC 1035 describes the framework for a conventional domain name system (*RFC 1035, Page 3*), but does not disclose an implementation including a secure domain name service and secure domain names as claimed by the '180 patent. Similarly, VPN Overview provides an overview of virtual private networks including their basic requirements. However, neither RFC 1035 or VPN Overview teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. Accordingly, the proposed rejection is not adopted.

11. Requestor proposed that claims 1, 10, 12-15, 17, 26, 28-31, and 33 be rejected under 35 USC 102(a) as being anticipated by Kaufman. This proposed rejection was adopted in the first Office action mailed on 1/19/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

12. Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain

name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

13. Kaufman does not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. Kaufman describes the implementation of virtual private networks and IPsec security, but does not disclose an implementation including a secure domain name service and secure domain names as claimed by the '180 patent. Kaufman does not teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. Accordingly, the proposed rejection is not adopted.

14. Requestor proposed that claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 be rejected under 35 USC 103(a) as being rendered obvious by the combination of Kaufman in view of Galvin. This proposed rejection was adopted in the first Office action mailed on 1/19/2010.

However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

15. Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

16. Kaufman and Galvin do not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. Kaufman describes the implementation of virtual private networks and IPsec security, but does not disclose an implementation including a secure domain name service and secure domain names as claimed by the '180 patent. Galvin describes a domain name service that uses public keys to prove the integrity of a domain name service record (*Galvin, Page 1*). However, this type of domain name service is a conventional type of

domain name service that is different from the claimed secure domain name service because it still relies on conventional domain names and does not provide security for secure domains. Instead, it seeks to prove the authenticity of a domain name service record to prove to a client that that the record was not forged. Kaufman and Galvin do not teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. Accordingly, the proposed rejection is not adopted.

17. Requestor proposed that claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 be rejected under 35 USC 102(a) as being anticipated by Gauntlet. This proposed rejection was adopted in the first Office action mailed on 1/19/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

18. Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent

distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

19. Gauntlet does not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. Gauntlet describes the implementation of a software based firewall system that provides for tunneling where the addresses of the secure tunneling servers must be advertised, but does not disclose an implementation including a secure domain name service and secure domain names as claimed by the '180 patent. Gauntlet does not teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. Accordingly, the proposed rejection is not adopted.

20. Requestor proposed that claims 1, 4, 10, 12-15, 17, 26, 28-31, 33, and 35 be rejected under 35 USC 103(a) as being rendered obvious by the combination of Hands-On in view of Installing NT. This proposed rejection was adopted in the first Office action mailed on 1/19/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

21. Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain

name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

22. Hands-On and Installing NT do not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. Hands-On describes the implementation of secure communications using PPTP tunneling protocols and describes the use of a conventional DNS system, but does not disclose an implementation including a secure domain name service and secure domain names as claimed by the '180 patent. Installing NT describes the use of a PPTP server to set up a secure connection, but does not describe the use of a secure domain name service using a secure domain name. Hands-On and Installing NT do not teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. Accordingly, the proposed rejection is not adopted.

23. Requestor proposed that claims 1, 10, 12-15, 17, 26, 28-31, and 33 be rejected under 35 USC 102(a) as being anticipated by Microsoft VPN. This proposed rejection was adopted in the first Office action mailed on 1/19/2010. However, upon consideration of the remarks submitted by Patent Owner, this proposed rejection is hereby withdrawn and not adopted for the following reasons.

24. Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*). Similarly, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that can resolve domain names of computers that are used to establish secure connections. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." For example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*).

25. Microsoft VPN does not teach the claimed "secure domain name" or "secure domain name service" as defined by the '180 patent. Microsoft VPN describes the implementation of a virtual private network to allow a remote client to gain access to a corporate network using a

PPTP tunnel through a VPN server, but does not disclose an implementation including a secure domain name service and secure domain names as claimed by the '180 patent. Microsoft VPN does not teach the claimed secure domain name or secure domain name service as defined by the '180 patent as being a part of a non-conventional domain name system. Accordingly, the proposed rejection is not adopted.

Rejections Proposed by Requestor – Previously Not Adopted That Remain Not Adopted

26. The non-final action mailed on January 19, 2010 is hereby incorporated by reference.

27. Requestor proposed that claims 4, 13, 15, 20, 29, 31, and 35 be rejected under 35 USC 102(a) as being anticipated by Aventail. This proposed rejection was not adopted for the reasons set forth on Pages 12-15 of the January 19, 2010 non-final office action.

28. Requestor proposed that claims 4, 20, and 35 be rejected under 35 USC 103(a) as being rendered obvious by the combination of VPN Overview in view of RFC 1035. This proposed rejection was not adopted for the reasons set forth on Pages 16-17 of the January 19, 2010 non-final office action.

29. Requestor proposed that claims 4, 20, and 35 be rejected under 35 USC 102(a) as being anticipated by Kaufman. This proposed rejection was not adopted for the reasons set forth on Pages 20-21 of the January 19, 2010 non-final office action.

30. Requestor proposed that claims 4, 20, and 35 be rejected under 35 USC 103(a) as being rendered obvious by the combination of Kaufman in view of Galvin. This proposed rejection

was not adopted for the reasons set forth on Pages 22-23 of the January 19, 2010 non-final office action.

31. Requestor proposed that claims 4, 20, and 35 be rejected under 35 USC 102(a) as being anticipated by Gauntlet. This proposed rejection was not adopted for the reasons set forth on Page 24 of the January 19, 2010 non-final office action.

32. Requestor proposed that claims 4, 20, and 35 be rejected under 35 USC 103(a) as being rendered obvious by the combination of Hands-On in view of Installing NT. This proposed rejection was not adopted for the reasons set forth on Pages 25-26 of the January 19, 2010 non-final office action.

STATEMENT OF REASONS FOR PATENTABILITY AND/OR CONFIRMATION

The following is an examiner's statement of reasons for patentability and/or confirmation of the claims found patentable in this reexamination proceeding:

Claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35 are confirmed as patentable for the following reasons. The cited prior art fails to teach or suggest the claimed features of a "secure domain name" and a "secure domain name service." Instead, the cited prior art teaches the use of a conventional domain name system and conventional domain names where some of the domain names correspond to a host that requires authentication. The '180 patent distinguishes the claimed secure domain names and secure domain name service from a conventional domain name service by explaining that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return

message indicating that the URL is unknown (*'180 patent, column 51 lines 25-35*) and that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name (*'180 patent, column 51 lines 25-35*). Accordingly, the cited prior art fails to anticipate or render obvious claims 1, 4, 10, 12-15, 17, 20, 26, 28-31, 33, and 35.

Any comments considered necessary by the PATENT OWNER regarding the above statement must be submitted promptly to avoid processing delays. Such submission by the patent owner should be labeled: "Comments on Statement of Reasons for Patentability and/or Confirmation" and will be placed in the reexamination file.

ACTION CLOSING PROSECUTION

This is an ACTION CLOSING PROSECUTION (ACP); see MPEP § 2671.02.

(1) Pursuant to 37 CFR 1.951(a), the patent owner may once file written comments limited to the issues raised in the reexamination proceeding and/or present a proposed amendment to the claims which amendment will be subject to the criteria of 37 CFR 1.116 as to whether it shall be entered and considered. Such comments and/or proposed amendments must be filed within a time period of 30 days or one month (whichever is longer) from the mailing date of this action. Where the patent owner files such comments and/or a proposed amendment, the third party requester may once file comments under 37 CFR 1.951(b) responding to the patent owner's submission within 30 days from the date of service of the patent owner's submission on the third party requester.

(2) If the patent owner does not timely file comments and/or a proposed amendment pursuant to 37 CFR 1.951(a), then the third party requester is precluded from filing comments under 37 CFR 1.951(b).

(3) Appeal **cannot** be taken from this action, since it is not a final Office action.

All correspondence relating to this *inter partes* reexamination proceeding should be directed:

By Mail to: Mail Stop *Inter Partes* Reexam
Attn: Central Reexamination Unit

Commissioner of Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany St.
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the examiner, or as to the status of this proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

Signed:

/Andrew Nalven/

Andrew Nalven
CRU Examiner
GAU 3992
(571) 272-3839

Conferee: ESK

Conferee: JF

Subst. for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	95/001,270
Filing Date	12-08-2009
First Named Inventor	Victor Larson
Art Unit	3992
Examiner Name	Andrew L. Nalven
Docket Number	007580-0090

U.S. PATENTS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
AN	A1	5,764,906	06/1998	Edelstein et al.	
	A2	5,864,666	01/1999	Shrader, Theodore Jack London	
	A3	5,898,830	04/1999	Wesinger et al.	
	A4	6,052,788	04/2000	Wesinger et al.	
	A5	6,061,346	05/2000	Nordman, Mikael	
	A6	6,081,900	06/2000	Subramaniam et al.	
	A7	6,101,182	08/2000	Sistanizadeh et al.	
	A8	6,199,112	03/2001	Wilson, Stephen K.	
	A9	6,202,081	03/2001	Naudus, Stanley T.	
	A10	6,298,341	10/2001	Mann et al.	
	A11	6,262,987	07/2001	Mogul, Jeffrey C.	
	A12	6,314,463	11/2001	Abbott et al.	
	A13	6,338,082	01/2002	Schneider, Eric	
	A14	6,502,135	12/2002	Munger et al.	
	A15	6,557,037	04/2003	Provino, Joseph E.	
	A16	6,687,746	02/2004	Shuster et al.	
	A17	6,757,740	06/2004	Parkh et al.	
	A18	7,039,713	05/2006	Van Gunter et al.	
	A19	7,167,904	01/2007	Devarajan et al.	
	A20	7,188,175	03/2007	McKeeth, James A.	
	A21	7,461,334	12/2008	Lu et al.	
	A22	7,490,151	02/2009	Munger et al.	
	A23	7,493,403	02/2009	Shull et al.	

U.S. PATENT APPLICATION PUBLICATIONS

EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
AN	B1	US2001/0049741	12/2001	Skene et al.	
	B2	US2004/0199493	10/2004	Ruiz et al.	
	B3	US2004/0199520	10/2004	Ruiz et al.	
	B4	US2004/0199608	10/2004	Rechterman et al.	
	B5	US2004/0199620	10/2004	Ruiz et al.	
	B6	US2007/0208869	09/2007	Adelman et al.	
	B7	US2007/0214284	09/2007	King et al.	

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Application Number	95/001,270
	Filing Date	12-08-2009
	First Named Inventor	Victor Larson
	Art Unit	3992
	Examiner Name	Andrew L. Nalven
	Docket Number	007580-0090

U.S. PATENT APPLICATION PUBLICATIONS					
EXAMINER'S INITIALS	CITE NO.	Patent Number	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
AN	B8	US2007/0266141	11/2007	Norton, Michael Anthony	
AN	B9	US2008/0235507	09/2008	Ishikawa et al.	

FOREIGN PATENT DOCUMENTS							
EXAMINER'S INITIALS	CITE NO	Foreign Patent Document Country Code-Number-Kind Codes (if known)	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation	
						Yes	No
AN	C1	JP04-363941	12/16/1992	Nippon Telegr & Teleph Corp		English Abstract	
	C2	JP09-018492	01/17/1997	Nippon Telegr & Teleph Corp		English Abstract	
	C3	JP10-070531	03/10/1998	Brother Ind Ltd.		English Abstract	
	C4	JP62-214744	9/21/1987	Hitachi Ltd.		English Abstract	

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)			
EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AN	D1	Yuan Dong Feng, "A novel scheme combining interleaving technique with cipher in Rayleigh fading channels," Proceedings of the International Conference on Communication technology, 2:S47-02-1-S47-02-4 (1998)	
AN	D2	D.W. Davies and W.L. Price, edited by Tadahiro Uezono, "Network Security", Japan, Nikkei McGraw-Hill, December 5, 1958, First Edition, first copy, p. 102-108	
EXAMINER		DATE CONSIDERED 6/8/10	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	95/001,270
	Patent No.	7,188,180
	Issued Date	March 6, 2007
	First Named Inventor	Victor Larson
	Docket Number	077580-0090
Sheet 1 of 19		

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
AW	A1000	5,303,302	04/12/1994	Burrows	
	A1000	5,311,593	05/10/1994	Carmi	
	A1001	5,384,848	01/24/1995	Kikuchi	
	A1002	5,511,122	04/23/1996	Atkinson	
	A1003	5,629,984	05/13/1997	McManis	
	A1004	5,771,239	06/23/1998	Moroney, et al.	
	A1005	5,805,803	09/08/1998	Birrell et al.	
	A1006	5,822,434	10/13/1998	Caronni et al.	
	A1007	5,898,830	04/27/1999	Wesinger, Jr. et al.	
	A1008	5,950,195	09/07/1999	Stockwell et al.	
	A1009	60/134,547	05/17/1999	Victor Sheymov	
	A1010	60/151,563	08/31/1999	Bryan Whittles	
	A1011	6,119,171	09/12/2000	Alkhatib	
	A1012	6,937,597	08/30/2005	Rosenberg et al.	
	A1013	7,072,964	07/04/2006	Whittle et al.	
	A1014	09/399,753	09/22/1998	Graig Miller et al.	
	A1015	6,079,020	06/20/2000	Liu	
	A1016	6,173,399	01/09/2001	Gilbrech	
	A1017	6,223,287	04/24/2001	Douglas, et al.	
	A1018	6,226,748	05/01/2001	Bots et al.	
	A1019	6,226,751	05/01/2001	Arrow et al.	
	A1020	6,701,437	03/02/2004	Hoke et al.	
	A1021	6,055,574	04/25/2000	Smorodinsky et al.	
	A1022	6,246,670	06/12/2001	Karlsson, et al.	
	A1023	7,461,334	12/02/08	Lu, et al.	
	A1024	7,353,841	04/08/08	Kono, et al.	
	A1025	7,188,175	03/06/07	McKeeth, James A.	
	A1026	7,167,904	01/23/07	Devarajan, et al.	
	A1027	7,039,713	05/02/06	Van Gunter, et al.	
	A1028	6,757,740	06/29/04	Parekh, et al.	
	A1029	6,752,166	06/22/04	Lull, et al.	
	A1030	6,687,746	02/03/04	Shuster, et al.	
	A1031	6,338,082	01/08/02	Schneider, Eric	
	A1032	6,333,272	12/25/01	McMillin, et al.	

EXAMINER: GC

DATE CONSIDERED: 6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 2 of 19		

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Document Number Number-Kind Code2 (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
AN	A1033	6,314,463	11/06/01	Abbott, et al.	
	A1034	6,298,341	10/02/01	Mann, et al.	
	A1035	6,262,987	07/17/01	Mogul, Jeffrey C.	
	A1036	6,199,112	03/06/04	Wilson, Stephen K.	
	A1037	6,052,788	04/18/00	Wesinger, et al	
	A1038	2,895,502	07/21/59	Garland Roper Charles, et al.	
	A1039	2001/0049741	12/06/01	Skene, et al.	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	95/001,270
	Patent No.	7,188,180
	Issued Date	March 6, 2007
	First Named Inventor	Victor Larson
	Docket Number	077580-0090
Sheet 3 of 19		

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	CITE NO.	Foreign Patent Document Country Codes-Number-Kind Codes (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	Translation Yes	Translation No
AV	B1000	WO 001/17775	03-30-2000	Science Applications International Corporation		Yes	No
↓	B1001	WO 00/70458	11-23-2000	Comsec Corporation			
↓	B1002	WO 01/016766	03-08-2001	Science Applications International Corporation			

EXAMINER: C

DATE CONSIDERED: 6/8/10

if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 4 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AN	C998	Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation,	
	C999	Appendix A of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1000	Concordance Table For the References Cited in Tables on pages 6-15, 71-80 and 116-124 of the Microsoft Corporation's Fourth Amended Invalidity Contentions dated Jan. 5, 2009.	
	C1001	1. P. Mockapetris, "DNS Encoding of Network Names and Other Types," Network Working Group, RFC 1101 (April 1989) (RFC1101, DNS SRV)	
	C1002	DNS-related correspondence dated September 7, 1993 to September 20, 1993. (Pre KX, KX Records)	
	C1003	R. Atkinson, "An Internetwork Authentication Architecture," Naval Research Laboratory, Center for High Assurance Computing Systems (8/5/93). (Atkinson NRL, KX Records)	
	C1004	Henning Schulzrinne, *Personal Mobility For Multimedia Services In The Internet*, Proceedings of the Interactive Distributed Multimedia Systems and Services European Workshop at 143 (1996). (Schulzrinne 96)	
	C1005	Microsoft Corp., *Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet* (1996) (printed from 1998 PDC DVD-ROM). (Point to Point, Microsoft Prior Art VPN Technology)	
	C1006	"Safe Surfing: How to Build a Secure World Wide Web Connection," IBM Technical Support Organization, (March 1996). (Safe Surfing, WEBSITE ART)	
	C1007	Goldschlag, et al., "Hiding Routing Information," Workshop on Information Hiding, Cambridge, UK (May 1996). (Goldschlag II, Onion Routing)	
	C1008	"IPSec Minutes From Montreal", IPSEC Working Group Meeting Notes, http://www.sandleman.ca/ipsec/1996/08/msg00018.html (June 1996). (IPSec Minutes, FreeS/WAN)	
	C1009	J. M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose, California, July 1996. (Galvin, DNSSEC)	
	C1010	J. Gilmore, et al. "Re: Key Management, anyone? (DNS Keying)," IPSec Working Group Mailing List Archives (8/96). (Gilmore DNS, FreeS/WAN)	
	C1011	H. Orman, et al. "Re: 'Re: DNS? was Re: Key Management, anyone?" IETF IPSec Working Group Mailing List Archive (8/96-9/96). (Orman DNS, FreeS/WAN)	
	C1012	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2052 (October 1996). (RFC 2052, DNS SRV)	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 5 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AN	C1013	Freier, et al. "The SSL Protocol Version 3.0," Transport Layer Security Working Group (November 18, 1996). (SSL, UNDERLYING SECURITY TECHNOLOGY)	
	C1014	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/02/1996). (RFC 2543 Internet Draft 1)	
	C1015	M.G. Reed, et al. "Proxies for Anonymous Routing," 12th Annual Computer Security Applications Conference, San Diego, CA, Dec. 9-13, 1996. (Reed, Onion Routing)	
	C1016	Kenneth F. Alden & Edward P. Wobber, *The AltaVista Tunnel: Using the Internet to Extend Corporate Networks*, Digital Technical Journal (1997) (Alden, AltaVista	
	C1017	Automative Industry Action Group, "ANX Release 1 Document Publication," AIAG (1997). (AIAG, ANX)	
	C1018	Automative Industry Action Group, "ANX Release 1 Draft Document Publication," AIAG Publications (1997). (AIAG Release, ANX)	
	C1019	Aventail Corp., "AutoSOCKS v. 2.1 Datasheet," *available at* http://www.archive.org/web/19970212013409/www.aventail.com/prod/autosk2ds.html (1997). (AutoSOCKS, Aventail)	
	C1020	Aventail Corp. "Aventail VPN Data Sheet," *available at* http://www.archive.org/web/19970212013043/www.aventail.com/prod/vpndata.html (1997).(Data Sheet, Aventail)	
	C1021	Aventail Corp., "Directed VPN Vs. Tunnel," *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/directvpn.html (1997). (Directed VPN, Aventail)	
	C1022	Aventail Corp., "Managing Corporate Access to the Internet," Aventail AutoSOCKS White Paper *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/ipmwp.html (1997). (Corporate Access, Aventail)	
	C1023	Aventail Corp., "Socks Version 5," Aventail Whitepaper, *available at* http://web.archive.org/web/19970620030312/www.aventail.com/educate/whitepaper/sockswp.html (1997). (Socks, Aventail)	
	C1024	Aventail Corp., "VPN Server V2.0 Administration Guide," (1997). (VPN, Aventail)	
	C1025	Goldschlag, et al. "*Privacy on the Internet,*" Naval Research Laboratory, Center for High Assurance Computer Systems (1997). (Goldschlag I, Onion Routing)	

EXAMINER	DATE CONSIDERED
EXAMINER	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 6 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	C1026	Microsoft Corp., *Installing Configuring and Using PPTP with Microsoft Clients and Servers* (1997). (Using PPTP, Microsoft Prior Art VPN Technology)	
	C1027	Microsoft Corp., *IP Security for Microsoft Windows NT Server 5.0* (1997) (printed from 1998 PDC DVD-ROM). (IP Security, Microsoft Prior Art VPN Technology)	
	C1028	Microsoft Corp., *Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Services* (1997) (printed from 1998 PDC DVD-ROM). (Directory, Microsoft Prior Art VPN Technology)	
	C1029	Microsoft Corp., *Routing and Remote Access Service for Windows NT Server NewOpportunities Today and Looking Ahead* (1997) (printed from 1998 PDC DVD-ROM).(Routing, Microsoft Prior Art VPN Technology)	
	C1030	Microsoft Corp., *Understanding Point-to-Point Tunneling Protocol PPTP* (1997) (printed from 1998 PDC DVD-ROM). (Understanding PPTP, Microsoft Prior Art VPN Technology)	
	C1031	J. Mark Smith et.al., *Protecting a Private Network: The AltaVista Firewall*, Digital Technical Journal (1997). (Smith, AltaVista)	
	C1032	Naganand Doraswamy *Implementation of Virtual Private Networks (VPNs) with IPSecurity*, <draft-ietf-ipsec-vpn-00.txt> (March 12, 1997). (Doraswamy)	
	C1033	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (03/27/1997). (RFC 2543 Internet Draft 2)	
	C1034	Aventail Corp., "Aventail and Cybersafe to Provide Secure Authentication For Internet and Intranet Communication," Press Release, April 3, 1997. (Secure Authentication, Aventail)	
	C1035	D. Wagner, et al. "Analysis of the SSL 3.0 Protocol," (April 15, 1997). (Analysis, UNDERLYING SECURITY TECHNOLOGIES)	
	C1036	Automotive Industry Action Group, "ANXO Certification Authority Service and Directory Service Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Defintion, ANX)	
	C1037	Automotive Industry Action Group, "ANXO Certification Process and ANX Registration Process Definition for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (May 9, 1997). (AIAG Certification, ANX)	
	C1038	Aventail Corp., "Aventail Announces the First VPN Solution to Assure Interoperability Across Emerging Security Protocols," June 2, 1997. (First VPN, Aventail)	
	C1039	Syverson, et al. "Private Web Browsing," Naval Research Laboratory, Center for High 8 Assurance Computer Systems (June 2, 1997). (Syverson, Onion Routing)	
	C1040	Bellcore, "Metrics, Criteria, and Measurement Technique Requirements for ANX Release 1," AIAG Telecommunications Project Team and Bellcore (June 16, 1997). (AIAG Requirements, ANX)	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 7 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AN	C1041	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/31/1997). (RFC 2543 Internet Draft 3)	
	C1042	R. Atkinson, "Key Exchange Delegation Record for the DNS," Network Working Group, RFC 2230 (November 1997). (RFC 2230, KX Records)	
	C1043	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/11/1997). (RFC 2543 Internet Draft 4)	
	C1044	1998 Microsoft Professional Developers Conference DVD ("1998 PDC DVD-ROM") (including screenshots captured therefrom and produced as MSFTVX 00018827-00018832). (Conference, Microsoft Prior Art VPN Technology)	
	C1045	Microsoft Corp., *Virtual Private Networking An Overview* (1998) (printed from 1998 PDC DVD-ROM) (Overview, Microsoft Prior Art VPN Technology)	
	C1046	Microsoft Corp., *Windows NT 5.0 Beta Has Public Premiere at Seattle Mini-Camp Seminar attendees get first look at the performance and capabilities of Windows NT 5.0* (1998) (available at hap //www.microsoft.com/presspass/features/1998/10-19nt5.mspxpftrue) (NT Beta, Microsoft Prior Art VPN Technology)	
	C1047	"What ports does SSL use" *available at* stason.org/TULARC/security/ssl-talk/3-4-What-ports-does-ssl-use.html (1998). (Ports, DNS SRV)	
	C1048	Aventail Corp., "Aventail VPN V2.6 Includes Support for More Than Ten Authentication Methods Making Extranet VPN Development Secure and Simple," Press Release, January 19, 1998. (VPN V2.6, Aventail)	
	C1049	R. G. Moskowitz, "Network Address Translation Issues with IPsec," Internet Draft, Internet Engineering Task Force, February 6, 1998. (Moskowitz)	
	C1050	H. Schulzrinne, et al, "Internet Telephony Gateway Location," Proceedings of IEEE INfocom '98, The Conference on Computer Communications, Vol. 2 (March 29 – April 2, 1998). (Gateway, Schulzrinne)	
	C1051	C. Huitema, 45 al. "Simple Gateway Control Protocol," Version 1.0 (May 5, 1998). (SGCP)	
	C1052	DISA "Secret Internet Protocol Router Network," SIPRNET Program Management Office (D3113) DISN Networks, DISN Transmission Services (May 8, 1998). (DISA, SIPRNET)	
	C1053	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (05/14/1998). (RFC 2543 Internet Draft 5)	
	C1054	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (06/17/1998). (RFC 2543 Internet Draft 6)	
	C1055	D. McDonald, et al. "PF_KEY Key Management API, Version 2," Network Working Group, RFC 2367 (July 1998). (RFC 2367)	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 8 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AN	C1056	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (07/16/1998). (RFC 2543 Internet Draft 7)	
	C1057	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (08/07/1998). (RFC 2543 Internet Draft 8)	
	C1058	Microsoft Corp., *Company Focuses on Quality and Customer Feedback* (August 18, 1998). (Focus, Microsoft Prior Art VPN Technology)	
	C1059	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (09/18/1998). (RFC 2543 Internet Draft 9)	
	C1060	Atkinson, et al. "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998). (RFC 2401, UNDERLYING SECURITY TECHNOLOGIES)	
	C1061	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (11/12/1998). (RFC 2543 Internet Draft 10) 9	
	C1062	Donald Eastlake, *Domain Name System Security Extensions*, IETF DNS Security Working Group (December 1998). (DNSSEC-7)	
	C1063	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (12/15/1998). (RFC 2543 Internet Draft 11)	
	C1064	Aventail Corp., "Aventail Connect 3.1/2.6Administrator's Guide," (1999). (Aventail Administrator 3.1, Aventail)	
	C1065	Aventail Corp., "Aventail Connect 3.1/2.6 User's Guide," (1999). (Aventail User 3.1, Aventail)	
	C1066	Aventail Corp., "Aventail ExtraWeb Server v3.2 Administrator's Guide," (1999). (Aventail ExtraWeb 3.2, Aventail)	
	C1067	Kaufman et al, "Implementing IPsec," (Copyright 1999). (Implementing IPSEC, VPN REFERENCES)	
	C1068	Network Solutions, Inc. "Enabling SSL," NSI Registry (1999). (Enabling SSL, UNDERLYING SECURITY TECHNOLOGIES)	
	C1069	Check Point Software Technologies Ltd. (1999) (Check Point, Checkpoint FW)	
	C1070	Arnt Gulbrandsen & Paul Vixie, *A DNS RR for specifying the location of services (DNS SRV)*, <draft-ietf-dnsind-frc2052bis-02.txt> (January 1999). (Gulbrandsen 99, DNS SRV)	
	C1071	C. Scott, et al. *Virtual Private Networks*, O'Reilly and Associates, Inc., 2nd ed. (Jan. 1999). (Scott VPNs)	
	C1072	M. Handley, H. Schulzrinne, E. Schooler, Internet Engineering Task Force, Internet Draft, (01/15/1999). (RFC 2543 Internet Draft 12)	
	C1073	Goldschlag, et al., "Onion Routing for Anonymous and Private Internet Connections," Naval Research Laboratory, Center for High Assurance Computer Systems (January 28, 1999). (Goldschlag III, Onion Routing)	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 9 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AN	C1074	H. Schulzrinne, "Internet Telephony: architecture and protocols – an IETF perspective," Computer Networks, Vol. 31, No. 3 (February 1999). (Telephony, Schulzrinne)	
	C1075	M. Handley, et al. "SIP: Session Initiation Protocol," Network Working Group, RFC 2543 and Internet Drafts (12/96-3/99). (Handley, RFC 2543)	
	C1076	FreeS/WAN Project, *Linux FreeS/WAN Compatibility Guide* (March 4, 1999). (FreeS/WAN Compatibility Guide, FreeS/WAN)	
	C1077	Telcordia Technologies, "ANX Release 1 Document Corrections," AIAG (May 11, 1999). (Telcordia, ANX)	
	C1078	Ken Hornstein & Jeffrey Altman, *Distributing Kerberos KDC and Realm Information with DNS* <draft-eitf-cat-krb-dns-locate-oo.txt> (June 21, 1999). (Hornstein, DNS SRV)	
	C1079	Bhattacharya et. al. "An LDAP Schema for Configuration and Administration of IPSec Based Virtual Private Networks (VPNs)", IETF Internet Draft (October 1999). (Bhattcharya LDAP VPN)	
	C1080	B. Patel, et al. "DHCP Configuration of IPSEC Tunnel Mode," IPSEC Working Group, Internet Draft 02 (10/15/1999). (Patel)	
	C1081	Goncalves, et al. *Check Point FireWall -1 Administration Guide*, McGraw-Hill Companies (2000). (Goncalves, Checkpoint FW)	
	C1082	"Building a Microsoft VPN: A Comprehensive Collection of Microsoft Resources," FirstVPN, (Jan 2000). (FirstVPN Microsoft)	
	C1083	Gulbrandsen, Vixie, & Esibov, *A DNS RR for specifying the location of services (DNS SRV)*, IETF RFC 2782 (February 2000). (RFC 2782, DNS SRV)	
	C1084	MITRE Organization, "Technical Description," Collaborative Operations in Joint Expeditionary Force Experiment (JEFX) 99 (February 2000). (MITRE, SIPRNET)	
	C1085	H. Schulzrinne, et al. "Application-Layer Mobility Using SIP," Mobile Computing and Communications Review, Vol. 4, No. 3. pp. 47-57 (July 2000). (Application, SIP)	
	C1086	Kindred et al, "Dynamic VPN Communities: Implementation and Experience," DARPA Information Survivability Conference and Exposition II (June 2001). (DARPA, VPN SYSTEMS)	
	C1087	ANX 101: Basic ANX Service Outline. (Outline, ANX)	
	C1088	ANX 201: Advanced ANX Service. (Advanced, ANX)	
	C1089	Appendix A: Certificate Profile for ANX IPsec Certificates. (Appendix, ANX)	
	C1090	Assured Digital Products. (Assured Digital)	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 10 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AN	C1091	Aventail Corp., "Aventail AutoSOCKS the Client Key to Network Security," Aventail Corporation White Paper. (Network Security, Aventail)	
	C1092	Cindy Moran, "DISN Data Networks: Secret Internet Protocol Router Network (SIPRNet)." (Moran, SIPRNET)	
	C1093	Data Fellows F-Secure VPN+ (F-Secure VPN+)	
	C1094	"Interim Operational Systems Doctrine for the Remote Access Security Program (RASP) Secret Dial-In Solution. (RASP, SIPRNET)	
	C1095	*Onion Routing*, "Investigation of Route Selection Algorithms," *available at* http://www.onion-router.net/Archives/Route/index.html. (Route Selection, Onion Routing)	
	C1096	Secure Computing, "Bullet-Proofing an Army Net," Washington Technology. (Secure, SIPRNET)	
	C1097	SPARTA "Dynamic Virtual Private Network." (Sparta, VPN SYSTEMS)	
	C1098	Standard Operation Procedure for Using the 1910 Secure Modems. (Standard, SIPRNET)	
	C1099	Publically available emails relating to FreeS/WAN (MSFTVX00018833-MSFTVX00019206). (FreeS/WAN emails, FreeS/WAN)	
	C1100	Kaufman et al., "Implementing IPsec," (Copyright 1999) (Implementing IPsec)	
	C1101	Network Associates *Gauntlet Firewall For Unix User's Guide Version 5.0* (1999). (Gauntlet User's Guide – Unix, Firewall Products)	
	C1102	Network Associates *Gauntlet Firewall For Windows NT Getting Started Guide Version 5.0* (1999) (Gauntlet Getting Started Guide – NT, Firewall Products)	
	C1103	Network Associates *Gauntlet Firewall For Unix Getting Started Guide Version 5.0* (1999) (Gauntlet Unix Getting Started Guide, Firewall Products)	
	C1104	Network Associates *Release Notes Gauntlet Firewall for Unix 5.0* (March 19, 1999) (Gauntlet Unix Release Notes, Firewall Products)	
	C1105	Network Associates *Gauntlet Firewall For Windows NT Administrator's Guide Version 5.0* (1999) (Gauntlet NT Administrator's Guide, Firewall Products)	
	C1106	Trusted Information Systems, Inc. *Gauntlet Internet Firewall Firewall-to-Firewall Encryption Guide Version 3.1* (1996) (Gauntlet Firewall-to-Firewall, Firewall Products)	
	C1107	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1108	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1109	Dan Sterne *Dynamic Virtual Private Networks* (May 23, 2000) (Sterne DVPN, DVPN)	
	C1110	Darrell Kindred *Dynamic Virtual Private Networks (DVPN)* (December 21, 1999) (Kindred DVPN, DVPN)	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 11 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AN	C1111	Dan Sterne *et.al. TIS Dynamic Security Perimeter Research Project Demonstration* (March 9, 1998) (Dynamic Security Perimeter, DVPN)	
	C1112	Darrell Kindred *Dynamic Virtual Private Networks Capability Description* (January 5, 2000) (Kindred DVPN Capability, DVPN) 11	
	C1113	October 7, and 28 1997 email from Domenic J. Turchi Jr. (SPARTA00001712-1714, 1808-1811) (Turchi DVPN email, DVPN)	
	C1114	James Just & Dan Sterne *Security Quickstart Task Update* (February 5, 1997) (Security Quickstart, DVPN)	
	C1115	Virtual Private Network Demonstration dated March 21, 1998 (SPARTA00001844-54) (DVPN Demonstration, DVPN)	
	C1116	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.1 Plan* (March 10, 1998) (IFD 1.1, DVPN)	
	C1117	Microsoft Corp. Windows NT Server Product Documentation: Administration Guide – Connection Point Services, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cpsops.mspx (Connection Point Services) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows. Accordingly, upon information and belief, this reference is prior art to the patents-insuit.)	
	C1118	Microsoft Corp. Windows NT Server Product Documentation: Administration Kit Guide – Connection Manager, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/cmak.mspx (Connection Manager) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1119	Microsoft Corp. Autodial Heuristics, *available at* http://support.microsoft.com/kb/164249 (Autodial Heuristics) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1120	Microsoft Corp., Cariplo: Distributed Component Object Model, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms809332(printer).aspx (Cariplo I)	
	C1121	Marc Levy, COM Internet Services (Apr. 23, 1999), *available at* http://msdn2.microsoft.com/en-us/library/ms809302(printer).aspx (Levy)	
	C1122	Markus Horstmann and Mary Kirtland, DCOM Architecture (July 23, 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809311(printer).aspx (Horstmann)	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 12 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AN	C1123	Microsoft Corp., DCOM: A Business Overview (Apr. 1997), *available at* http://msdn2.microsoft.com/en-us/library/ms809320(printer).aspx (DCOM Business Overview I)	
	C1124	Microsoft Corp., DCOM Technical Overview (Nov. 1996), *available at* http://msdn2.microsoft.com/en-us/library/ms809340(printer).aspx (DCOM Technical Overview I)	
	C1125	Microsoft Corp., DCOM Architecture White Paper (1998) *available in* PDC DVD-ROM (DCOM Architecture)	
	C1126	Microsoft Corp, DCOM – The Distributed Component Object Model, A Business Overview White Paper (Microsoft 1997) *available in* PDC DVD-ROM (DCOM Business Overview II)	
	C1127	Microsoft Corp., DCOM—Cariplo Home Banking Over The Internet White Paper (Microsoft 1996) *available in* PDC DVD-ROM (Cariplo II)	
	C1128	Microsoft Corp., DCOM Solutions in Action White Paper (Microsoft 1996) *available in* PDC DVD-ROM (DCOM Solutions in Action)	
	C1129	Microsoft Corp., DCOM Technical Overview White Paper (Microsoft 1996) *available* 12 *in* PDC DVD-ROM (DCOM Technical Overview II)	
	C1130	125. Scott Suhy & Glenn Wood, DNS and Microsoft Windows NT 4.0, (1996) *available at* http://msdn2.microsoft.com/en-us/library/ms810277(printer).aspx (Suhy)	
	C1131	126. Aaron Skonnard, *Essential WinInet* 313-423 (Addison Wesley Longman 1998) (Essential WinInet)	
	C1132	Microsoft Corp. Installing, Configuring, and Using PPTP with Microsoft Clients and Servers, (1998) *available at* http://msdn2.microsoft.com/enus/library/ms811078(printer).aspx (Using PPTP)	
	C1133	Microsoft Corp., Internet Connection Services for MS RAS, Standard Edition, http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstart.mspx (Internet Connection Services I)	
	C1134	Microsoft Corp., Internet Connection Services for RAS, Commercial Edition, *available at*http://www.microsoft.com/technet/archive/winntas/proddocs/inetconctservice/bcgstrtc.mspx (Internet Connection Services II)	
	C1135	Microsoft Corp., Internet Explorer 5 Corporate Deployment Guide – Appendix B:Enabling Connections with the Connection Manager Administration Kit, *available at* http://www.microsoft.com/technet/prodtechnol/ ie/deploy/deploy5/appendb.mspx (IE5 Corporate Development)	
	C1136	Mark Minasi, *Mastering Windows NT Server 4* 1359-1442 (6th ed., January 15, 1999)(Mastering Windows NT Server)	
	C1137	*Hands On, Self-Paced Training for Supporting Version 4.0* 371-473 (Microsoft Press 1998) (Hands On)	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 13 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AV	C1138	Microsoft Corp., MS Point-to-Point Tunneling Protocol (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/maintain/featusability/pptpwp3.mspx (MS PPTP)	
	C1139	Kenneth Gregg, *et al.*, *Microsoft Windows NT Server Administrator's Bible* 173-206, 883-911, 974-1076 (IDG Books Worldwide 1999) (Gregg)	
	C1140	Microsoft Corp., Remote Access (Windows), *available at* http://msdn2.microsoft.com/en-us/library/bb545687(VS.85,printer).aspx (Remote Access)	
	C1141	Microsoft Corp., Understanding PPTP (Windows NT 4.0), *available at* http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx (Understanding PPTP NT 4) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1142	Microsoft Corp., Windows NT 4.0: Virtual Private Networking, *available at* http://www.microsoft.com/technet/archive/winntas/ deploy/confeat/vpntwk.mspx (NT4 VPN) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1143	Anthony Northrup, *NT Network Plumbing: Routers, Proxies, and Web Services* 299-399 (IDG Books Worldwide 1998) (Network Plumbing)	
	C1144	Microsoft Corp., Chapter 1 – Introduction to Windows NT Routing with Routing and Remote Access Service, *Available at* http://www.microsoft.com/technet/archive/winntas/proddocs/ rras40/rrasch01.mspx (Intro to RRAS) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.) 13	
	C1145	Microsoft Corp., Windows NT Server Product Documentation: Chapter 5 – Planning for Large-Scale Configurations, *available at* http://www.microsoft.com/technet/archive/winntas/proddocs/rras40/rrasch05.mspx (Large-Scale Configurations) (Although undated, this reference refers to the operation of prior art versions of Microsoft Windows such as Windows NT 4.0. Accordingly, upon information and belief, this reference is prior art to the patents-in-suit.)	
	C1146	F-Secure, *F-Secure Evaluation Kit* (May 1999) (FSECURE 00000003) (Evaluation Kit 3)	
	C1147	F-Secure, *F-Secure NameSurfer* (May 1999) (from FSECURE 00000003) (NameSurfer 3)	
	C1148	F-Secure, *F-Secure VPN Administrator's Guide* (May 1999) (from FSECURE 00000003) (F-Secure VPN 3)	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 14 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AN	C1149	F-Secure, *F-Secure SSH User's & Administrator's Guide* (May 1999) (from FSECURE 00000003) (SSH Guide 3)	
	C1150	F-Secure, *F-Secure SSH2.0 for Windows NT and 95* (May 1999) (from FSECURE 00000003) (SSH 2.0 Guide 3)	
	C1151	F-Secure, *F-Secure VPN+ Administrator's Guide* (May 1999) (from FSECURE 00000003) (VPN+ Guide 3)	
	C1152	F-Secure, *F-Secure VPN+ 4.1* (1999) (from FSECURE 00000006) (VPN+ 4.1 Guide 6)	
	C1153	F-Secure, *F-Secure SSH* (1996) (from FSECURE 00000006) (F-Secure SSH 6)	
	C1154	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (1998) (from FSECURE 00000006) (F-Secure SSH 2.0 Guide 6)	
	C1155	F-Secure, *F-Secure Evaluation Kit* (Sept. 1998) (FSECURE 00000009) (Evaluation Kit 9)	
	C1156	F-Secure, *F-Secure SSH User's & Administrator's Guide* (Sept. 1998) (from FSECURE 00000009) (SSH Guide 9)	
	C1157	F-Secure, *F-Secure SSH 2.0 for Windows NT and 95* (Sept. 1998) (from FSECURE 00000009) (F-Secure SSH 2.0 Guide 9)	
	C1158	F-Secure, *F-Secure VPN+* (Sept. 1998) (from FSECURE 00000009) (VPN+ Guide 9)	
	C1159	F-Secure, *F-Secure Management Tools, Administrator's Guide* (1999) (from FSECURE 00000003) (F-Secure Management Tools)	
	C1160	F-Secure, *F-Secure Desktop, User's Guide* (1997) (from FSECURE 00000009) (FSecure Desktop User's Guide)	
	C1161	SafeNet, Inc., *VPN Policy Manager* (January 2000) (VPN Policy Manager)	
	C1162	F-Secure, F-Secure VPN+ for Windows NT 4.0 (1998) (from FSECURE 00000009) (FSecure VPN+)	
	C1163	IRE, Inc., *SafeNet/Soft-PK Version 4* (March 28, 2000) (Soft-PK Version 4)	
	C1164	IRE/SafeNet Inc., *VPN Technologies Overview* (March 28, 2000) (Safenet VPN Overview)	
	C1165	IRE, Inc., *SafeNet / Security Center Technical Reference Addendum* (June 22, 1999) (Safenet Addendum)	
	C1166	IRE, Inc., *System Description for VPN Policy Manager and SafeNet/SoftPK* (March 30, 2000) (VPN Policy Manager System Description)	
	C1167	IRE, Inc., About SafeNet / VPN Policy Manager (1999) (About Safenet VPN Policy Manager)	
	C1168	IRE, Inc., *SafeNet/VPN Policy Manager Quick Start Guide Version 1* (1999) (SafeNet VPN Policy Manager)	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 15 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
GW	C1169	Trusted Information Systems, Inc., *Gauntlet Internet Firewall, Firewall Product Functional Summary* (July 22, 1996) (Gauntlet Functional Summary)	
	C1170	Trusted Information Systems, Inc., *Running the Gauntlet Internet Firewall, An Administrator's Guide to Gauntlet Version 3.0* (May 31, 1995) (Running the Gauntlet Internet Firewall)	
	C1171	Ted Harwood, *Windows NT Terminal Server and Citrix Metaframe* (New Riders 1999) (Windows NT Harwood) 79	
	C1172	Todd W. Matehrs and Shawn P. Genoway, *Windows NT Thing Client Solutions: Implemetning Terminal Server and Citrix MetaFrame* (Macmillan Technial Publishing 1999) (Windows NT Mathers)	
	C1173	Bernard Aboba et al., *Securing L2TP using IPSEC* (February 2, 1999)	
	C1174	156. *Finding Your Way Through the VPN Maze* (1999) ("PGP")	
	C1175	Linux FreeS/WAN Overview (1999) (Linux FreeS/WAN) Overview)	
	C1176	TimeStep, *The Business Case for Secure VPNs* (1998) ("TimeStep")	
	C1177	WatchGuard Technologies, Inc., *WatchGuard Firebox System Powerpoint* (2000)	
	C1178	WatchGuard Technologies, Inc., *MSS Firewall Specifications* (1999)	
	C1179	WatchGuard Technologies, Inc., *Request for Information, Security Services* (2000)	
	C1180	WatchGuard Technologies, Inc., *Protecting the Internet Distributed Enterprise, White Paper* (February 2000)	
	C1181	WatchGuard Technologies, Inc., *WatchGuard LiveSecurity for MSS Powerpoint* (Feb. 14 2000)	
	C1182	WatchGuard Technologies, Inc., *MSS Version 2.5, Add-On for WatchGuard SOHO Releaset Notes* (July 21, 2000)	
	C1183	Air Force Research Laboratory, *Statement of Work for Information Assurance System Architecture and Integration, PR No. N-8-6106 (Contract No. F30602-98-C-0012)* (January 29, 1998)	
	C1184	GTE Internetworking & BBN Technologies *DARPA Information Assurance Program Integrated Feasibility Demonstration (IFD) 1.2 Report, Rev. 1.0* (September 21, 1998)	
	C1185	BBN Information Assurance Contract, *TIS Labs Monthly Status Report* (March 16-April 30, 1998)	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued.Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 16 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AN	C1186	DARPA, *Dynamic Virtual Private Network (VPN) Powerpoint* .	
	C1187	GTE Internetworking, *Contractor's Program Progress Report* (March 16-April 30, 1998)	
	C1188	Darrell Kindred, *Dynamic Virtual Private Networks (DVPN) Countermeasure Characterization* (January 30, 2001)	
	C1189	*Virtual Private Networking Countermeasure Characterization* (March 30, 2000)	
	C1190	*Virtual Private Network Demonstration* (March 21, 1998)	
	C1191	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks (VPNs) and Integrated Security Management* (2000)	
	C1192	Information Assurance/NAI Labs, *Create/Add DVPN Enclave* (2000)	
	C1193	NAI Labs, *IFE 3.1 Integration Demo* (2000)	
	C1194	Information Assurance, *Science Fair Agenda* (2000)	
	C1195	Darrell Kindred et al., *Proposed Threads for IFE 3.1* (January 13, 2000)	
	C1196	*IFE 3.1 Technology Dependencies* (2000)	
	C1197	*IFE 3.1 Topology* (February 9, 2000)	
	C1198	Information Assurance, *Information Assurance Integration: IFE 3.1, Hypothesis & Thread Development* (January 10-11, 2000)	
	C1199	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation* (2000)	
	C1200	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.2* (2000)	
	C1201	Information Assurance/NAI Labs, *Dynamic Virtual Private Networks Presentation v.3* (2000)	
	C1202	T. Braun et al., *Virtual Private Network Architecture*, Charging and Accounting Technology for the Internet (August 1, 1999) (VPNA)	
	C1203	Network Associates Products – *PGP Total Network Security Suite, Dynamic Virtual Private Networks* (1999)	
	C1204	Microsoft Corporation, Microsoft Proxy Server 2.0 (1997) (Proxy Server 2.0, Microsoft Prior Art VPN Technology)	
	C1205	David Johnson et. al., *A Guide To Microsoft Proxy Server 2.0* (1999) (Johnson, Microsoft Prior Art VPN Technology)	
	C1206	Microsoft Corporation, *Setting Server Parameters* (1997 (copied from Proxy Server 2.0 CD labeled MSFTVX00157288) (Setting Server Parameters, Microsoft Prior Art VPN Technology)	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 17 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AW	C1207	Kevin Schuler, *Microsoft Proxy Server 2* (1998) (Schuler, Microsoft Prior Art VPN Technology)	
	C1208	Erik Rozell et. al., *MCSE Proxy Server 2 Study Guide* (1998) (Rozell, Microsoft Prior 15 Art VPN Technology)	
	C1209	M. Shane Stigler & Mark A Linsenbardt, *IIS 4 and Proxy Server 2* (1999) (Stigler, Microsoft Prior Art VPN Technology)	
	C1210	David G. Schaer, *MCSE Test Success: Proxy Server 2* (1998) (Schaer, Microsoft Prior Art VPN Technology)	
	C1211	John Savill, *The Windows NT and Windows 2000 Answer Book* (1999) (Savill, Microsoft Prior Art VPN Technology)	
	C1212	Network Associates *Gauntlet Firewall Global Virtual Private Network User's Guide for Windows NT Version 5.0* (1999) (Gauntlet NT GVPN, GVPN)	
	C1213	Network Associates *Gauntlet Firewall For UNIX Global Virtual Private Network User's Guide Version 5.0* (1999) (Gauntlet Unix GVPN, GVPN)	
	C1214	File History for U.S. Application Serial No. 09/653,201, Applicant(s): Whittle Bryan, et al., Filing Date 08/31/2000.	
	C1215	*AutoSOCKS v2.1*, Datasheet, http://web.archive.org/web/19970212013409/www.aventail.com/prod/autoskds.html	
	C1216	Ran Atkinson, *Use of DNS to Distribute Keys*, 7 Sept. 1993, http://ops.ietf.org/lists/namedroppers/namedroppers.199x/msg00945.html	
	C1217	FirstVPN Enterprise Networks, Overview	
	C1218	Chapter 1: Introduction to Firewall Technology, Administration Guide; 12/19/07, http://www.books24x7.com/book/id_762/viewer_r.asp?bookid=762&chunked=41065062	
	C1219	The TLS Protocol Version 1.0; January 1999; page 65 of 71.	
	C1220	Elizabeth D. Zwicky, et al., Building Internet Firewalls, 2nd Ed.	
	C1221	Virtual Private Networks – Assured Digital Incorporated – ADI 4500; http://web.archive.org/web/19990224050035/www.assured-digital.com/products/prodvpn/adia4500.htm	
	C1222	Accessware – The Third Wave in Network Security, Conclave from Internet Dynamics; http://web.archive.org/web/11980210013830/interdyn.com/Accessware.html	
	C1223	Extended System Press Release, Sept. 2, 1997; *Extended VPN Uses The Internet to Create Virtual Private Networks*, www.extendedsystems.com	
	C1224	Socks Version 5; Executive Summary; http://web.archive.org/web/199970620031945/www.aventail.com/educate/whitepaper/sockswp.html	
	C1225	Internet Dynamics First to Ship Integrated Security Solutions for Enterprise Intranets and Extranets; Sept. 15, 1997; http://web.archive.org/web/19980210014150/interdyn.com	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 18 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AW	C1226	Emails from various individuals to Linux IPsec re: DNS-LDAP Splicing	
	C1227	Microsoft Corporation's Fifth Amended Invalidity Contentions dated September 18, 2009, VirnetX Inc. and Science Applications International Corp. v. Microsoft Corporation and invalidity claim charts for U.S. Patent Nos. 7,188,180 and 6,839,759	
	C1228	The IPSEC Protocol as described in Atkinson, et al., "Security Architecture for the Internet Protocol," Network Working Group, RFC 2401 (November 1998) ("RFC 2401"); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1229	S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1230	C. Madson and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1231	C. Madson and R. Glenn, "The Use HMAC-SHA-1-96 within ESP and AH," RFC 2404 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1232	C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1233	S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1234	Derrell Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1235	Douglas Maughan, et al, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1236	D. Harkins and D. Carrell, "The Internet Key Exchange (IKE)," RFC 2409 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1237	R. Glenn and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec." RFC 2410 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1238	R. Thayer, et al., "IP Security Document Roadmap," RFC 2411 (November 1998); http://web.archive.org/web/19991007070353/http://www.imib.med.tu-dresden.de/imib/Internet/Literatur/ipsec-docu_eng.html	
	C1239	Hilarie K. Orman, "The OAKLEY Key Determination Protocol," RFC 2412 (November 1998) in combination with J.M. Galvin, "Public Key Distribution with Secure DNS," Proceedings of the Sixth USENIX UNIX Security Symposium, San Jose California (July 1996) ("Galvin")	

EXAMINER	DATE CONSIDERED
	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.
1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

Subst. for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(Use as many sheets as necessary)*	Control No.	**95/001,270**
	Patent No.	**7,188,180**
	Issued Date	**March 6, 2007**
	First Named Inventor	**Victor Larson**
	Docket Number	**077580-0090**
Sheet 19 of 19		

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

EXAMINER'S INITIALS	CITE NO.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
AL	C1240	David Kosiur, "Building and Managing Virtual Private Networks" (1998)	
	C1241	P. Mockapetris, "Domain Names – Implementation and Specification," Network Working Group, RFC 1035 (November 1987)	
	C1242	Request for Inter Partes Reexamination of Patent No. 6,502,135, dated Nov. 25, 2009.	

EXAMINER	DATE CONSIDERED
AL	6/8/10

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

BST99 1643905-1.077580.0090

EXHIBIT C

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VirnetX Inc.	§	
	§	
Plaintiff,	§	
	§	
vs.	§	Case No. 6:10-cv-417
	§	
Cisco Systems, Inc., *et al.*,	§	
	§	JURY TRIAL DEMANDED
Defendants.	§	

DEFENDANT APPLE INC.'S ORIGINAL ANSWER, AFFIRMATIVE DEFENSES, AND COUNTERCLAIMS TO PLAINTIFF'S ORIGINAL COMPLAINT

Defendant Apple Inc. ("Apple") files this Original Answer, Affirmative Defenses and Counterclaims to Plaintiff's Original Complaint for Patent Infringement (the "Complaint") filed by VirnetX Inc. ("VirnetX").

I. ANSWER

THE PARTIES

1. - 2. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraphs 1 and 2 and therefore denies the same.

3. Apple admits that it is a California corporation organized and existing under the laws of California, with its principal place of business at One Infinite Loop, Cupertino, California 95014. Apple admits that it has conducted business in this district. Apple denies all other allegations contained in paragraph 3 of VirnetX's complaint.

4. - 5. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraphs 4 and 5 and therefore denies the same.

JURISDICTION AND VENUE

6. Apple admits that VirnetX alleges a civil action for patent infringement under the laws of the United States, Title 35 United States Code §§ 101, *et seq.* Apple admits that this Court has subject matter jurisdiction over VirnetX's claims for patent infringement. Apple denies all other allegations contained in paragraph 6 of VirnetX's complaint.

7. To the extent the allegations in paragraph 7 relate to Apple, Apple admits that venue is proper in this Court, but Apple denies that this judicial district is the most convenient forum for this case. Apple denies all other allegations in this paragraph to the extent such allegations relate to Apple. To the extent the allegations in paragraph 7 relate to the other Defendants in this case, Apple is without sufficient information or knowledge to either admit or deny the allegations and therefore denies the same.

8. To the extent the allegations in paragraph 8 relate to Apple, Apple admits that this Court has personal jurisdiction over Apple. Apple admits that it has conducted business in the State of Texas. Apple admits that it has and does sell products and provide services to persons within the State of Texas and this District, but it denies that it has committed any acts of infringement within this District or the State of Texas, and specifically denies any wrongdoing, infringement, inducement of infringement, or contribution to infringement. Apple denies all other allegations in this paragraph to the extent such allegations relate to Apple. To the extent the allegations in paragraph 8 relate to the other Defendants in this case, Apple is without sufficient information or knowledge to either admit or deny the allegations and therefore denies the same.

ASSERTED PATENTS

Petitioner Apple Inc. - Exhibit 1026, p. 1198

9. Apple admits that, according to the face of the patent, United States Patent No. 6,502,135 ("the '135 patent") is entitled "Agile Network Protocol for Secure Communications with Assured System Availability" and reflects an issue date of December 31, 2002. Apple admits that Edmund Colby Munger, Douglas Charles Schmidt, Robert Dunham Short, III, Victor Larson, and Michael Williamson are listed as inventors on the face of the patent. Apple admits that what appears to be a copy of the '135 patent is attached as Exhibit A to VirnetX's Complaint. Apple denies all other allegations contained in paragraph 9 of VirnetX's complaint.

10. Apple admits that, according to the face of the patent, United States Patent No. 6,839,759 ("the '759 patent") is entitled "Method for Establishing Secure Communication Link Between Computers of Virtual Private Network Without User Entering Any Cryptographic Information" and reflects an issue date of January 4, 2005. Apple admits that Victor Larson, Robert Dunham Short, III, Edmund Colby Munger, and Michael Williamson are listed as inventors on the face of the patent. Apple admits that what appears to be a copy of the '759 patent is attached as Exhibit B to VirnetX's Complaint. Apple denies all other allegations contained in paragraph 10 of VirnetX's complaint.

11. Apple admits that, according to the face of the patent, United States Patent No. 7,188,180 ("the '180 patent") is entitled "Method for Establishing Secure Communication Link Between Computers of Virtual Private Network" and reflects an issue date of March 6, 2007. Apple admits that Victor Larson, Robert Dunham Short, III, Edmund Colby Munger, and Michael Williamson are listed as inventors on the face of the patent. Apple admits that what appears to be a copy of the '180 patent is attached as Exhibit C to VirnetX's Complaint. Apple denies all other allegations contained in paragraph 11 of VirnetX's complaint.

Petitioner Apple Inc. - Exhibit 1026, p. 1199

12. Apple admits that, according to the face of the patent, United States Patent No. 7,418,504 ("the '504 patent") is entitled "Agile Network Protocol for Secure Communications Using Secure Domain Names" and reflects an issue date of August 26, 2008. Apple admits that Victor Larson, Robert Dunham Short, III, Edmund Colby Munger, and Michael Williamson are listed as inventors on the face of the patent. Apple admits that what appears to be a copy of the '504 patent is attached as Exhibit D to VirnetX's Complaint. Apple denies all other allegations contained in paragraph 12 of VirnetX's complaint.

13. Apple admits that, according to the face of the patent, United States Patent No. 7,490,151 ("the '151 patent") is entitled "Establishment of a Secure Communication Link Based on a Domain Name Service (DNS) Request" and reflects an issue date of February 10, 2009. Apple admits that Edmund Colby Munger, Robert Dunham Short, III, Victor Larson, and Michael Williamson are listed as inventors on the face of the patent. Apple admits that what appears to be a copy of the '151 patent is attached as Exhibit E to VirnetX's Complaint. Apple denies all other allegations contained in paragraph 13 of VirnetX's complaint.

COUNT ONE

ALLEGED PATENT INFRINGEMENT BY AASTRA

14. Apple incorporates by reference paragraphs 1-13 above as if fully set forth herein. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraph 14 regarding Aastra and the '135 patent and therefore denies the same.

15. – 22. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraphs 15-22 and therefore denies the same.

COUNT TWO

ALLEGED PATENT INFRINGEMENT BY APPLE

Petitioner Apple Inc. - Exhibit 1026, p. 1200

23. Apple incorporates by reference paragraphs 1-22 above as if fully set forth herein. Apple denies that it has infringed or continues to infringe the '135 and '151 patents.

24. Denied.

25. Denied.

26. Apple admits that it provides or has provided the iPhone, iPhone 3G, iPhone 3GS, iPhone 4, iPod Touch, and iPad to others in the United States. Apple denies that these or any other Apple products infringe any asserted claims of the '135 patent. Apple further denies all other allegations contained in paragraph 26 of VirnetX's Complaint.

27. Denied.

28. Denied.

29. Apple admits that it makes, uses, sells, offers for sale, imports, exports, supplies, and/or distributes within and from the United States the iPhone, iPhone 3G, iPhone 3GS, iPhone 4, iPod Touch, and iPad, but it denies that these or any other Apple products infringe any asserted claims of the '151 patent. Apple further denies all other allegations contained in paragraph 29 of VirnetX's Complaint.

30. Apple admits that it makes, uses, sells, offers for sale, imports, exports, supplies, and/or distributes within and from the United States the iPhone, iPhone 3G, iPhone 3GS, iPhone 4, iPod Touch, and iPad, but it denies that these or any other Apple products infringe any asserted claims of the '151 patent. It is not clear what is referenced by "Apple's servers, master discs, and other media that store, cache, or distribute iPhone OS." As such, Apple denies the same. Apple further denies all other allegations contained in paragraph 30 of VirnetX's Complaint.

Petitioner Apple Inc. - Exhibit 1026, p. 1201

31. Apple admits that it provides or has provided the iPhone, iPhone 3G, iPhone 3GS, iPhone 4, iPod Touch, and iPad to others in the United States. Apple denies that these or any other Apple products infringe any asserted claims of the '151 patent. It is not clear what is referenced by "Apple's servers, master discs, and other media that store, cache, or distribute iPhone OS." As such, Apple denies the same. Apple further denies all other allegations contained in paragraph 31 of VirnetX's Complaint.

32. Denied.

33. Denied.

34. Denied.

35. Denied.

36. Apple admits that it received notice of infringement after the filing of this lawsuit but denies that any Apple products infringe the '135 or '151 patents. Apple further denies all other allegations contained in paragraph 36 of VirnetX's Complaint.

COUNT THREE

ALLEGED PATENT INFRINGEMENT BY CISCO

37. Apple incorporates by reference paragraphs 1-36 above as if fully set forth herein. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraph 37 regarding Cisco and the '135, '759, '180, and '504 patents and therefore denies the same.

38. – 63. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraphs 38-63 and therefore denies the same.

COUNT THREE

ALLEGED PATENT INFRINGEMENT BY NEC

Petitioner Apple Inc. - Exhibit 1026, p. 1202

64. Apple incorporates by reference paragraphs 1-63 above as if fully set forth herein. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraph 64 regarding NEC and the '135 and '504 patents and therefore denies the same.

65. - 77. Apple is without sufficient information or knowledge to either admit or deny the allegations in paragraphs 65-77 and therefore denies the same.

DEMAND FOR JURY TRIAL

Apple also demands a trial by jury.

PRAYER FOR RELIEF

Apple opposes VirnetX's requested relief against Apple or any other relief VirnetX requests against Apple, including those specified in paragraphs 1-17 of this Section of VirnetX's Complaint.

DENIAL OF ANY REMAINING ALLEGATIONS

Except as specifically admitted herein, Apple denies any remaining allegations in VirnetX's Complaint that are directed at Apple.

II. AFFIRMATIVE DEFENSES

Apple asserts the following Affirmative Defenses.

FIRST AFFIRMATIVE DEFENSE
(No Infringement)

78. Apple does not infringe and has not infringed any valid and enforceable claim of the '135 and '151 patents.

Petitioner Apple Inc. - Exhibit 1026, p. 1203

SECOND AFFIRMATIVE DEFENSE
(Invalidity)

79. Claims of the '135 and '151 patents are invalid for failure to satisfy the conditions for patentability set forth in Title 35 of the United States Code, including without limitation §§ 101, 102, 103 and 112.

THIRD AFFIRMATIVE DEFENSE
(Failure to State a Claim)

80. VirnetX's claims for relief and each and every one of its allegations fail to state a claim upon which relief can be granted.

FOURTH AFFIRMATIVE DEFENSE
(Laches)

81. VirnetX's claims are barred in whole or in part by laches.

FIFTH AFFIRMATIVE DEFENSE
(Waiver)

82. VirnetX's claims are barred in whole or in part by waiver.

SIXTH AFFIRMATIVE DEFENSE
(Estoppel)

83. VirnetX's claims are barred in whole or in part by estoppel.

SEVENTH AFFIRMATIVE DEFENSE
(Notice, Damages, and Costs)

84. VirnetX's claims for damages, if any, against Apple are statutorily limited by 35 U.S.C. § 286 and/or § 287.

85. VirnetX is barred from recovering costs in connection with this action under 35 U.S.C. § 288.

EIGHT AFFIRMATIVE DEFENSE
(Lack of Standing)

Petitioner Apple Inc. - Exhibit 1026, p. 1204

86. VirnetX lacks standing to enforce one or more of the patents-in-suit, including because it does not have all substantial rights in the patents. Upon information and belief, Science Application International Corp. ("SAIC") retains substantial rights in one or more of the patents-in-suit and is a necessary party to this litigation.

NINTH AFFIRMATIVE DEFENSE
(Sales to Government)

87. VirnetX's claims are limited by 28 U.S.C. § 1498.

TENTH AFFIRMATIVE DEFENSE
(Unclean Hands and Inequitable Conduct)

88. As more fully outlined in Apple's Count III, specifically paragraphs 9-34 in Apple's Counterclaims, which are hereby incorporated by reference, the claims of the '135 and '151 patents are unenforceable due to inequitable conduct, infectious unenforceability, and/or unclean hands committed by the inventors, their counsel, SAIC, VirnetX, and/or others substantively involved in the prosecution of the '135 or '151 patents.

RESERVATION OF AFFIRMATIVE DEFENSES

89. Apple hereby reserves the right to supplement additional affirmative defenses as discovery proceeds in this case.

III. COUNTERCLAIMS

Apple asserts the following counterclaims against VirnetX.

PARTIES

1. Counterclaim plaintiff is a California Corporation with its principal place of business at One Infinite Loop, Cupertino, California 95014.

Petitioner Apple Inc. - Exhibit 1026, p. 1205

2. On information and belief based on Plaintiff's Complaint, Counterclaim Defendant VirnetX Inc. ("VirnetX") is a Delaware corporation, having a place of business located at 5615 Scotts Valley Drive, Suite 110, Scotts Valley, California.

JURISDICTION AND VENUE

3. These counterclaims arise under the patent laws of the United States as enacted under Title 35 of the United States Code and the provisions of the Federal Declaratory Judgment Act. The jurisdiction of this Court is proper under 28 U.S.C. §§ 1331, 1338, 2201 and 2202.

4. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391 and 1400.

COUNT I – DECLARATION OF NON-INFRINGEMENT

5. Based on VirnetX's filing of this action and Apple's Affirmative Defenses, an actual controversy has arisen and now exists between VirnetX and Apple as to whether Apple has infringed or is infringing one or more claims of U.S. Patent Numbers 6,502,135 ("the '135 patent") and 7,490,151 ("the '151 patent").

6. Pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, Apple requests the declaration of the Court that Apple does not infringe and has not infringed any valid and enforceable claim of the '135 and '151 patents.

COUNT II – DECLARATION OF PATENT INVALIDITY

7. Based on VirnetX's filing of this action and Apple's Affirmative Defenses, an actual controversy has arisen and now exists between VirnetX and Apple as to the validity of the claims of the '135 and '151 patents.

8. Pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, Apple requests the declaration of the Court that the '135 and '151 patents are invalid.

COUNT III – DECLARATION OF UNENFORCEABILITY

Petitioner Apple Inc. - Exhibit 1026, p. 1206

9. Based on VirnetX's filing of this action and Apple's Affirmative Defenses, an actual controversy has arisen and now exists between VirnetX and Apple as to the enforceability of the '135 and '151 patents.

10. The '135 patent, which issued on December 31, 2002, was filed with the United States Patent and Trademark Office ("Patent Office") on February 15, 2000 as U.S. Patent Application No. 09/504,783 ("the '783 application").

11. The '151 patent, which issued on February 10, 2009, was filed with the United States Patent and Trademark Office ("Patent Office") on September 30, 2002 as U.S. Patent Application No. 10/259,494 ("the '494 application").

12. On information and belief, the applications that matured into the '135 and '151 patents were assigned to Science Application International Corporation ("SAIC"). On information and belief, SAIC assigned to VirnetX certain rights in the '135 patent after issuance and certain rights in the application that matured into the '151 patent.

A. The '135 Patent

13. The '135 patent is unenforceable due to inequitable conduct. Based on a review of the file history and based on Apple's understanding of the allegations by VirnetX, one or more of the people substantively involved in the prosecution of the application leading to the '135 patent, including a reexamination, were aware of information material to the patentability of the claims of the '135 patent, but withheld that information from the Patent Office with the intent to deceive.

14. The withheld information includes U.S. Patent Application No. 09/399,753 ("the Miller Application"), which was pending during the prosecution of the '135 patent. The pendency of the Miller Application was information material to patentability of the '135 patent

Petitioner Apple Inc. - Exhibit 1026, p. 1207

based on Apple's understanding of the allegations by VirnetX. The withheld information also includes RFC 2401-Security Architecture for the Internet Protocol ("RFC 2401") and information concerning the publication date of the Aventail Administrator's Guide ("Aventail"), which are material to patentability based upon Apple's understanding of the allegations by VirnetX. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

15. The Miller Application, RFC 2401, and the Aventail reference are not cumulative to the prior art made of record during prosecution of the '135 patent. On information and belief, there is a substantial likelihood that a reasonable examiner would have considered this art in determining whether to allow the '135 patent to issue.

16. During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution (including Ross Dannenburg) were aware of the Miller Application. Mr. Dannenburg was involved in the prosecution of the Miller Application at least as early as June 14, 2002, when he signed an Amendment / Response in the prosecution history of the Miller Application. Mr. Dannenburg was involved in the prosecution of the '135 patent at least as early as January 28, 2002, when he signed a Transmittal Form for an Amendment / Response in the prosecution file history of the '135 patent. Therefore, Mr. Dannenburg was involved in the prosecution of the Miller Application while he was prosecuting the '135 patent. Based on Apple's understanding of the allegations by VirnetX, the pendency of the Miller Application is information material to patentability. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to disclose this material information to the Patent Office at any time during the prosecution of the '135 patent with intent to deceive. Moreover, the materiality of the Miller Application leads to an inference of intent to

Petitioner Apple Inc. - Exhibit 1026, p. 1208

deceive. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

17. During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution were aware of RFC 2401, including Mr. Dannenburg, because it is mentioned in the specification of the '135 patent. Based on Apple's understanding of the allegations by VirnetX, RFC 2401 is material prior art. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to submit this material prior art reference to the Patent Office as required by 37 C.F.R. 1.56 and 37 C.F.R. 1.97, with intent to deceive. Moreover, in mentioning RFC 2401 in the application, those substantively involved in the prosecution of the application described RFC 2401 in a way that concealed its materiality, with intent to deceive. Moreover, the materiality of RFC 2401 leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

18. On or about February 15, 2007, VirnetX filed a lawsuit against Microsoft Corporation ("Microsoft") in the Eastern District of Texas, Tyler Division, C.A. No. 6:07-CV-80 (the "Microsoft Case"), alleging that Microsoft infringed certain VirnetX patents, including the '135 patent.

19. In December 2009, Microsoft filed a reexamination request with the Patent Office requesting reexamination of claims 1-10 and 12 of the '135 patent, citing, among other references, the Aventail reference as prior art under 35 U.S.C. § 102(a). Microsoft asserted that the Aventail reference anticipated claims 1-10 and 12 of the '135 patent.

Petitioner Apple Inc. - Exhibit 1026, p. 1209

20. On or about December 31, 2009, the Patent Office ordered reexamination of claims 1-10 and 12 of the '135 patent, finding, in part, that the Aventail reference raised a substantial new question of patentability of all of the requested claims of the '135 patent.

21. On or about January 15, 2010, the Patent Office issued a non-final action rejecting claims 1, 3, 4, 6-10, and 12 of the '135 patent as being anticipated by the Aventail reference.

22. On or about February 22, 2010, VirnetX filed a petition to extend its deadline for responding to the office action, pointing out, in part, that it needed additional time to investigate whether the Aventail reference was proper prior art, including investigating the dates of conception and reduction to practice of the inventions claimed in the '135 patent as well as diligence there between. The petition also cited as a basis for extension that the Microsoft Case was causing a "significant drain" on VirnetX's resources. Moreover, the petition stated that the extension "would likely also permit consideration of any court conclusions regarding the claims presently under reexamination." The petition was filed by Toby Kusmer of McDermott Will & Emery, the same firm that represented VirnetX in the Microsoft Case until 2009. The Patent Office responded on or about February 24, 2010, granting an extension, setting the deadline for response as April 15, 2010.

23. On or about March 8, 2010, trial of the Microsoft Case ("Microsoft Trial") commenced. During the Microsoft Trial, one or more witnesses for VirnetX, including inventor Edward Munger, testified that the claims of the '135 patent were conceived no earlier than three months after September 23, 1999, placing the date of conception for claims 1-10 and 12 on or about December 23, 1999. During the Microsoft Trial, Microsoft alleged, in part, that claims 1-10 and 12 of the '135 patent were anticipated by the Aventail reference, which on information and belief bears a copyright date 1996 – 1999. Microsoft presented evidence indicating that the

Petitioner Apple Inc. - Exhibit 1026, p. 1210

Aventail reference may have been published as early as June 1999. Based on a review of the trial record, VirnetX did not dispute the publication date of the Aventail reference. The Microsoft Trial concluded on or about March 16, 2010. Therefore, at least as of March 16, 2010, VirnetX was aware that the Aventail reference may have been published at least as early as June 1999, which is prior to the February 15, 2000, filing date of the application that matured into the '135 patent and prior to the earliest conception date of December 1999 claimed by the inventor of the '135 patent.

24. On or about March 25, VirnetX gave notice to the Patent Office of the outcome of the case and submitted the jury verdict form from the case. On or about March 29, 2010, VirnetX filed a petition requesting that the reexamination proceeding be suspended. The Patent Office did not respond to the request until after the date set for VirnetX's response to the non-final office action rejection.

25. On or about April 15, 2010, VirnetX responded to the office action rejection, in part, by asserting that the Aventail reference should not be considered prior art because no evidence had been submitted by Microsoft that established the actual publication date of the Aventail reference. Moreover, VirnetX did not provide the result of any investigation it may have made with respect to the publication date of the Aventail reference or the dates of conception or reduction to practice of the '135 patent that it indicated it would make in its petition for an extension of time, nor did VirnetX provide any information that it learned from the Microsoft Trial that related to the publication date of the Aventail reference. Based on a review of the prosecution history, VirnetX did not disclose that its conception date for the claims of the '135 patent was no earlier than December 1999, nor did VirnetX disclose that the Aventail

Petitioner Apple Inc. - Exhibit 1026, p. 1211

reference may have been published as early as June 1999, as it was made aware of during the Microsoft Trial.

26. On June 16, 2010, the Patent Office issued an Action Closing Prosecution. In the action, the examiner recites that he made an attempt to determine the publication date of the Aventail reference, but was unsuccessful. Based on the lack of evidence of the publication date, the examiner withdrew all of the rejections that had been based on the Aventail reference.

27. VirnetX and/or its representatives, agents, and attorneys who were substantively involved in the prosecution of the reexamination knew or should have known of the Microsoft trial and the evidence presented regarding the publication date of the Aventail reference. For example, Mr. Kusmer specifically referenced the Microsoft Trial and the potential for additional material information to come to light during that trial when seeking an extension to respond to an office action, as set forth in paragraph 24 above. VirnetX and/or its representatives, agents, and attorneys withheld this information with the intent to deceive, either willfully or with such gross negligence or recklessness as constituting an act of willfulness amounting to inequitable conduct. Moreover, the materiality of the Aventail publication and the aforementioned evidence presented at the Microsoft Trial leads to an inference of intent to deceive. Among other things, the information withheld was material to the reexamination of the '135 patent, in violation of the duty of candor the representatives and/or the attorneys owed to the Patent Office.

The '151 Patent

28. The application that issued as the '151 patent was a divisional of the application that issued as the '135 patent.

Petitioner Apple Inc. - Exhibit 1026, p. 1212

29. The '151 patent is unenforceable due to unclean hands and/or infectious unenforceability resulting from inequitable conduct committed during the prosecution of the '135 patent, including its reexamination, as set forth above in paragraphs 13-29.

30. The '151 patent is also unenforceable due to inequitable conduct. Based on Apple's understanding of the allegations by VirnetX, one or more of the people substantively involved in the prosecution of the application leading to the '151 patent were aware of information material to the patentability of the claims of the '151 patent, but withheld that information from the Patent Office with the intent to deceive.

31. The withheld information includes the Aventail reference and "Building a Microsoft VPN: A comprehensive collection of Microsoft resources," pages 1-216 ("the Microsoft VPN reference"). These references were material to patentability based upon Apple's understanding of the allegations by VirnetX. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

32. The Aventail and Microsoft VPN references are not cumulative to the prior art made of record during prosecution of the '151 patent. On information and belief, there is a substantial likelihood that a reasonable examiner would have considered this art in determining whether to allow the '151 patent to issue.

33. During the prosecution of the application leading to the '151 patent, one or more of the people substantively involved in its prosecution were aware of the Aventail reference, including Mr. Kusmer of the McDermott law firm. Mr. Kusmer filed the application that led to the issuance of the '151 patent, which was filed on September 20, 2002. The McDermott law firm was aware of the Aventail reference at least as early as February 13, 2008, when Microsoft disclosed the reference in its invalidity contentions. The '151 patent did not issue until February

Petitioner Apple Inc. - Exhibit 1026, p. 1213

10, 2009. Based on Apple's understanding of the allegations by VirnetX, the Aventail reference is material prior art. Moreover, in the reexamination of the '135 patent, the Patent Office found a substantial new question of patentability based on the Aventail reference, and the claims of the '135 patent relate to the same subject matter as the claims of the '151 patent. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to disclose this material prior art reference to the Patent Office with intent to deceive. Moreover, the materiality of the Aventail reference leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

34. During the prosecution of the application leading to the '151 patent, one or more of the people substantively involved in its prosecution, including Mr. Kusmer, were aware of the Microsoft VPN reference. The McDermott law firm was aware of the Aventail reference at least as early as February 13, 2008, when Microsoft disclosed the reference in its invalidity contentions. The '151 patent did not issue until February 10, 2009. Based on Apple's understanding of the allegations by VirnetX, the Microsoft VPN reference is material prior art. Moreover, in the reexamination of the '135 patent, the Patent Office found a substantial new question of patentability based on the Microsoft VPN reference, and the claims of the '135 patent relate to the same subject matter as the claims of the '151 patent. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to disclose this material prior art reference to the Patent Office with intent to deceive. Moreover, the materiality of the Microsoft VPN reference leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

JURY DEMAND

35. Apple demands a trial by jury.

Petitioner Apple Inc. - Exhibit 1026, p. 1214

EXCEPTIONAL CASE

36. To the extent this is an exceptional case under 35 U.S.C. 285, Apple is entitled to recover from VirnetX for Apples' attorneys' fees and costs incurred in connection with this action.

PRAYER FOR RELIEF

Apple respectfully requests a judgment against VirnetX as follows:

A. A declaration that Apple does not infringe and has not infringed any valid and enforceable claim of the '135 and '151 patents;

B. A declaration that the '135 and '151 patents are invalid;

C. A declaration that the '135 and '151 patents are unenforceable;

D. That VirnetX take nothing by its Complaint against Apple;

E. That the Court enter judgment against VirnetX and in favor of Apple and that VirnetX's Complaint be dismissed with prejudice;

F. That the Court enter a judgment that this is an exceptional case under 35 U.S.C. § 285 and enter a judgment awarding Apple its costs and reasonable attorneys' fees; and

G. That the Court grant Apple whatever further relief the Court may deem just and proper.

Respectfully submitted,

Date: October 29, 2010

/s/ Danny L. Williams
Danny L. Williams - LEAD ATTORNEY
State Bar No. 21518050
E-mail: danny@wmalaw.com
Ruben S. Bains

Petitioner Apple Inc. - Exhibit 1026, p. 1215

Texas Bar No. 24001678
E-mail: rbains@wmalaw.com
Drew Kim
Texas Bar No. 24007482
E-mail: dkim@wmalaw.com
Williams, Morgan & Amerson, P.C.
10333 Richmond, Suite 1100
Houston, Texas 77042
Telephone: (713) 934-7000
Facsimile: (713) 934-7011

ATTORNEYS FOR APPLE INC.

CERTIFICATE OF SERVICE

I hereby certify that the following counsel of record who are deemed to have consented to electronic service are being served this 29th day of October, 2010, with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3). Any other counsel of record will be served by, electronic mail, facsimile transmission and/or first class mail on this same date.

Dated: October 29, 2010

/s/ Mark Dunglinson
Mark Dunglinson

Petitioner Apple Inc. - Exhibit 1026, p. 1216

EXHIBIT D

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VirnetX Inc.,	§	
	§	
Plaintiff,	§	
	§	
v.	§	
	§	CIVIL ACTION NO. 6:10-CV-417 LED
Cisco Systems, Inc.	§	
Apple Inc.	§	Judge: Hon. Leonard Davis
Aastra USA Inc.	§	
Aastra Technologies Ltd.	§	
NEC Corporation, and	§	
NEC Corporation of America,	§	
	§	
Defendants.	§	
	§	

DEFENDANT AND COUNTERCLAIM-PLAINTIFF AASTRA TECHNOLOGIES LIMITED'S ANSWER, AFFIRMATIVE DEFENSES AND COUNTERCLAIMS TO VIRNETX INC.'S ORIGINAL COMPLAINT

Aastra Technologies Limited ("Aastra Technologies"), defendant and counterclaim-plaintiff in the above-entitled and numbered civil action, replies to the Original Complaint of VirnetX Inc. ("VirnetX") as follows.

THE PARTIES

1. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is "a corporation organized and existing under the laws of the State of Delaware, and maintains its principal place of business at 5615 Scotts Valley Drive, Suite 110 Scotts Valley, California," and, therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1218

2. Aastra Technologies admits that it is a Canadian corporation with its principal place of business at 155 Snow Blvd., Concord, Ontario Canada, L4K 4N9. Aastra Technologies admits that Aastra USA Inc. is a Delaware corporation with its principal place of business at 2811 Internet Blvd., Frisco, Texas 75034. Aastra Technologies denies that it regularly conducts and transacts business in Texas, throughout the United States, and within the Eastern District of Texas. Aastra Technologies admits that Aastra USA Inc. regularly conducts and transacts business in Texas, throughout the United States, and within the Eastern District of Texas. Aastra Technologies denies that either it or Aastra USA Inc. it has committed or continues to commit any acts that give rise to any cause of action asserted in VirnetX's complaint. Except as admitted above, Aastra Technologies denies the allegations of Paragraph 2.

3. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 3 and therefore, denies these allegations.

4. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 4 and therefore, denies these allegations.

5. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 5 and therefore, denies these allegations.

JURISDICTION AND VENUE

Petitioner Apple Inc. - Exhibit 1026, p. 1219

6. Aastra Technologies admits that VirnetX purports to bring this action under the patent laws of the United States, Title 35, United States Code, but Aastra Technologies denies any liability thereunder. Aastra Technologies does not contest that the Court has exclusive subject matter over this matter under 28 U.S.C. § 1338. Except as admitted above, Aastra Technologies denies the allegations of Paragraph 6.

7. Admitted.

8. Aastra Technologies admits that this Court has personal jurisdiction over Aastra Technologies. Except as admitted above, Aastra Technologies denies the allegations of Paragraph 8.

ASSERTED PATENTS

9. Aastra Technologies admits that United States Patent No. 6,502,135 ("the '135 patent"), entitled "Agile Network Protocol for Secure Communications with Assured System Availability" issued on December 31, 2002, but denies any further characterization of the '135 patent, its inventors, or its examination as alleged in Paragraph 9. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '135 patent and possesses all rights of recovery under the '135 patent" and, therefore, denies these allegations. Aastra Technologies admits that a purported copy of the '135 patent was attached to the complaint as Exhibit A. Except as expressly admitted above, Aastra Technologies denies the allegations in Paragraph 9.

10. Aastra Technologies admits that United States Patent No. 6,839,759 ("the '759 patent"), entitled "Method for Establishing Secure Communication Link

Petitioner Apple Inc. - Exhibit 1026, p. 1220

Between Computers of Virtual Private Network Without User Entering Any Cryptographic Information" issued on January 4, 2005, but denies any further characterization of the '759 patent, its inventors, or its examination as alleged in Paragraph 10. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '759 patent and possesses all rights of recovery under the '759 patent" and, therefore, denies these allegations. Aastra Technologies admits that a purported copy of the '759 patent was attached to the complaint as Exhibit B. Except as expressly admitted above, Aastra Technologies denies the allegations in Paragraph 10.

11. Aastra Technologies admits that United States Patent No. 7,188,180 ("the '180 patent"), entitled "Method for Establishing Secure Communications Link Between Computers of Virtual Private Network" issued on March 6, 2007, but denies any further characterization of the '180 patent, its inventors, or its examination as alleged in Paragraph 11. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '180 patent and possesses all rights of recovery under the '180 patent" and, therefore, denies these allegations. Aastra Technologies admits that a purported copy of the '180 patent was attached to the complaint as Exhibit C. Except as expressly admitted above, Aastra Technologies denies the allegations in Paragraph 11.

12. Aastra Technologies admits that United States Patent No. 7,418,504 ("the '504 patent"), entitled "Agile Network Protocol for Secure Communications Using

Petitioner Apple Inc. - Exhibit 1026, p. 1221

Secure Domain Names" issued on August 26, 2008, but denies any further characterization of the '504 patent, its inventors, or its examination as alleged in Paragraph 12. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '504 patent and possesses all rights of recovery under the '504 patent" and, therefore, denies these allegations. Aastra Technologies admits that a purported copy of the '504 patent was attached to the complaint as Exhibit D. Except as expressly admitted above, Aastra Technologies denies the allegations in Paragraph 12.

13. Aastra Technologies admits that United States Patent No. 7,490,151 ("the '151 patent"), entitled "Establishment of a Secure Communication Link Based on a Domain Name Service (DNS) Request" issued on February 10, 2009, but denies any further characterization of the '151 patent, its inventors, or its examination as alleged in Paragraph 13. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '151 patent and possesses all rights of recovery under the '151 patent" and, therefore, denies these allegations. Aastra Technologies admits that a purported copy of the '151 patent was attached to the complaint as exhibit E. Except as expressly admitted above, Aastra Technologies denies the allegations in Paragraph 13.

COUNT ONE

PATENT INFRINGEMENT BY AASTRA TECHNOLOGIES

Petitioner Apple Inc. - Exhibit 1026, p. 1222

14. Aastra Technologies incorporates by reference paragraphs 1-13 as if fully set forth herein. Aastra Technologies denies that it has infringed and/or continues to infringe the '135 patent.

15. Denied.

16. Denied.

17. Denied.

18. Denied.

19. Denied.

20. Denied.

21. Denied.

22. Aastra Technologies admits that it has received actual notice of infringement by virtue of the filing of this lawsuit. Aastra Technologies denies that it has received constructive notice. Aastra Technologies denies that VirnetX has complied with the requirements of 35 U.S.C. § 287. Except as expressly admitted above, Aastra Technologies denies the allegations in Paragraph 22.

COUNT TWO

PATENT INFRINGEMENT BY APPLE

23. Aastra Technologies incorporates by reference paragraphs 1-22 as if fully set forth herein. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 23 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1223

24. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 24 and therefore, denies these allegations.

25. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 25 and therefore, denies these allegations.

26. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 26 and therefore, denies these allegations.

27. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 27 and therefore, denies these allegations.

28. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 28 and therefore, denies these allegations.

29. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 29 and therefore, denies these allegations.

30. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 30 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1224

31. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 31 and therefore, denies these allegations.

32. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 32 and therefore, denies these allegations.

33. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 33 and therefore, denies these allegations.

34. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 34 and therefore, denies these allegations.

35. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 35 and therefore, denies these allegations.

36. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 36 and therefore, denies these allegations.

COUNT THREE

PATENT INFRINGEMENT BY CISCO

37. Aastra Technologies incorporates by reference paragraphs 1-36 as if fully set forth herein. Aastra Technologies is without knowledge or information sufficient

Petitioner Apple Inc. - Exhibit 1026, p. 1225

to form a belief as to the truth of the allegations set forth in Paragraph 37 and therefore, denies these allegations.

38. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 38 and therefore, denies these allegations.

39. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 39 and therefore, denies these allegations.

40. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 40 and therefore, denies these allegations.

41. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 41 and therefore, denies these allegations.

42. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 42 and therefore, denies these allegations.

43. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 43 and therefore, denies these allegations.

44. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 44 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1226

45. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 45 and therefore, denies these allegations.

46. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 46 and therefore, denies these allegations.

47. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 47 and therefore, denies these allegations.

48. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 48 and therefore, denies these allegations.

49. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 49 and therefore, denies these allegations.

50. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 50 and therefore, denies these allegations.

51. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 51 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1227

52. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 52 and therefore, denies these allegations.

53. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 53 and therefore, denies these allegations.

54. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 54 and therefore, denies these allegations.

55. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 55 and therefore, denies these allegations.

56. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 56 and therefore, denies these allegations.

57. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 57 and therefore, denies these allegations.

58. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 58 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1228

59. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 59 and therefore, denies these allegations.

60. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 60 and therefore, denies these allegations.

61. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 61 and therefore, denies these allegations.

62. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 62 and therefore, denies these allegations.

63. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 63 and therefore, denies these allegations.

COUNT FOUR

PATENT INFRINGEMENT BY NEC

64. Aastra Technologies incorporates by reference paragraphs 1-63 as if fully set forth herein. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 64 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1229

65. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 65 and therefore, denies these allegations.

66. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 66 and therefore, denies these allegations.

67. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 67 and therefore, denies these allegations.

68. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 68 and therefore, denies these allegations.

69. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 69 and therefore, denies these allegations.

70. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 70 and therefore, denies these allegations.

71. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 71 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1230

72. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 72 and therefore, denies these allegations.

73. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 73 and therefore, denies these allegations.

74. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 74 and therefore, denies these allegations.

75. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 75 and therefore, denies these allegations.

76. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 76 and therefore, denies these allegations.

77. Aastra Technologies is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 77 and therefore, denies these allegations.

AASTRA TECHNOLOGIES' AFFIRMATIVE DEFENSES

78. Aastra Technologies has not and does not literally, directly, contributorily, by way of inducement, and/or under the doctrine of equivalents, infringe any valid and/or enforceable claim of the '135 patent.

Petitioner Apple Inc. - Exhibit 1026, p. 1231

79. Each of the claims of the '135 patent are invalid for failing to comply with one of more of the requirements for patentability specified by Part II of Title 35 of the United States Code §101 *et seq.*, including without limitation 35 U.S.C. §§ 102, 103 and/or 112.

80. VirnetX is estopped from construing the claims of the '135 patent to cover or include, either literally or by application of the doctrine of equivalents, methods used, devices manufactured, used, imported, sold or offered for sale by Aastra Technologies because of admissions and statements to the PTO during prosecution of the applications leading to the issuance of the patent, disclosure or language in the specification of the patent and/or limitations in the claims of the patent.

81. The relief sought by VirnetX is barred in whole or in part by the doctrine of laches.

82. To the extent that products accused of infringement were or are used or manufactured by or for the United States , the relief sought by VirnetX is limited by 28 U.S.C. § 1498(a).

83. The relief sought by VirnetX is barred in whole or in part by 35 U.S.C. § 287.

84. VirnetX is not entitled to an injunction against Aastra Technologies because VirnetX has an adequate remedy at law.

85. VirnetX lacks standing to bring suit to enforce the '135 patent because it does not possess all substantial rights in the '135 patent.

86. The '135 patent is unenforceable due to inequitable conduct. Based on the contents of the prosecution history and based on Aastra Technologies' understanding

Petitioner Apple Inc. - Exhibit 1026, p. 1232

of the allegations by VirnetX, one or more of the people substantively involved in the prosecution of the application leading to the '135 patent, and the subsequent reexamination of the '135 patent, were aware of information material to the patentability of the claims of the '135 patent, but withheld that information from the Patent Office with the intent to deceive.

The existence of US. Patent Application No. 09/399,753 ("the Miller Application"), was withheld during the prosecution of the '135 patent. The pendency of the Miller Application was information material to patentability of the '135 patent based on Aastra Technologies' understanding of the allegations by VirnetX. The withheld information also includes RFC 2401-Security Architecture for the Internet Protocol ("RFC 2401") and the Aventail Administrator's Guide ("Aventail"), which are material to patentability based upon Aastra Technologies' understanding of the allegations by VirnetX. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

The Miller Application, RFC 2401, and the Aventail reference are not cumulative to the prior art made of record during prosecution of the '135 patent. There is a substantial likelihood that a reasonable examiner would have considered this art in determining whether to allow the '135 patent to issue.

During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution (including Ross Dannenburg) were aware of the Miller Application. Mr. Dannenburg was involved in the prosecution of the Miller Application during the prosecution of the '135 patent at least as early as June 14, 2002, when he signed an Amendment / Response in the

Petitioner Apple Inc. - Exhibit 1026, p. 1233

prosecution history of the Miller Application. Mr. Dannenburg was involved in the prosecution of the '135 patent at least as early as January 28, 2002, when he signed a Transmittal Form for an Amendment / Response in the prosecution file history of the '135 patent. Therefore, Mr. Dannenburg was involved in the prosecution of the Miller Application while he was prosecuting the '135 patent. Based on Aastra Technologies' understanding of the allegations by VirnetX, the pendency of the Miller Application is information material to patentability. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to disclose this material information to the Patent Office at any time during the prosecution of the '135 patent with intent to deceive. Moreover, the materiality of the Miller Application leads to an inference of intent to deceive. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution were aware of RFC 2401, including Mr. Dannenburg, because it is mentioned in the specification of the '135 patent. Based on Aastra Technologies' understanding of the allegations by VirnetX, RFC 2401 is material prior art. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to submit this material prior art reference to the Patent Office as required by 37 C.F.R. 1.56 and 37 C.F.R. 1.97, with intent to deceive. Moreover, in mentioning RFC 2401 in the application, those substantively involved in the prosecution of the application described RFC 2401 in a way that concealed its materiality, with intent to deceive. Moreover, the materiality of

Petitioner Apple Inc. - Exhibit 1026, p. 1234

RFC 2401 leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

VirnetX also committed inequitable conduct during the reexamination of the '135 patent. On or about February 15, 2007, VirnetX filed a lawsuit against Microsoft Corporation ("Microsoft") in the Eastern District of Texas, Tyler Division, C.A. No. 6:07-CV-80 (the "Microsoft trial"), alleging that Microsoft infringed certain VirnetX patents, including the '135 patent.

During the Microsoft trial, one or more witnesses for VirnetX, including inventor Edward Munger, testified that the claims of the '135 patent were conceived no earlier than three months after September 23, 1999, placing the date of conception for claims 1-10 and 12 on or after December 23, 1999.

During the Microsoft trial, Microsoft alleged, in part, that claims 1-10 and 12 of the '135 patent were anticipated by the Aventail reference, which on information and belief bears a copyright date between 1996 – 1999.

In December 2009, Microsoft filed a re-examination request with the Patent Office requesting re-examination of claims 1-10 and 12 of the '135 patent, citing, among other references, the Aventail reference as prior art under 35 U.S.C. § 102(a). Microsoft asserted that the Aventail reference anticipated claims 1-10 and 12 of the '135 patent.

On or about December 31, 2009, the Patent Office ordered re-examination of claims 1-10 and 12 of the '135 patent, finding, in part, that the Aventail reference raised a substantial new question of patentability of all of the requested claims of the '135 patent.

Petitioner Apple Inc. - Exhibit 1026, p. 1235

On or about January 15, 2010, the Patent Office issued a non-final action rejecting claims 1, 3, 4, 6-10, and 12 as being anticipated by the Aventail reference.

On or about February 22, 2010, VirnetX filed a petition to extend its deadline for responding to the office action, pointing out, in part, that it needed additional time to investigate whether the Aventail reference was proper prior art, including investigating the dates of conception and reduction to practice of the inventions claimed in the '135 patent as well as diligence there between. The petition also cited as a basis for extension that the Microsoft case was causing a "significant drain" on VirnetX's resources. Moreover, the petition stated that the extension "would likely also permit consideration of any court conclusions regarding the claims presently under reexamination." The petition was filed by Toby Kusmer of McDermott Will & Emery, the same firm that represented VirnetX in the Microsoft case until 2009. The Patent Office responded on or about February 24, 2010, granting an extension, and setting the deadline for response as April 15, 2010.

On or about March 8, 2010, the Microsoft trial commenced. During trial, Microsoft argued that the Aventail reference invalidated claims 1-10 and 12 of the '135 patent. Microsoft presented evidence indicating that the Aventail reference may have been published as early as June 1999. Based on a review of the trial record, VirnetX did not dispute the publication date of the Aventail reference. The Microsoft trial concluded on or about March 16, 2010. Therefore, at least as of March 16, 2010VirnetX was aware that the Aventail reference may have been published at least as early as June 1999, which is prior to the February 15, 2000, filing date of the application that matured into the '135 patent and prior to the earliest conception date

Petitioner Apple Inc. - Exhibit 1026, p. 1236

of December 1999 claimed by the inventor of the '135 patent.

On or about March 25, 2010, VirnetX gave notice to the Patent Office of the outcome of the case and submitted the jury verdict form from the case. On or about March 29, 2010, VirnetX filed a petition requesting that the re-examination proceeding be suspended. The Patent Office did not respond to the request until after the date set for VirnetX's response to the non-final office action rejection.

On or about April 15, 2010, VirnetX responded to the office action rejection, in part, by asserting that the Aventail reference should not be considered prior art because no evidence had been submitted by Microsoft that established the actual publication date of the Aventail reference. Moreover, VirnetX did not provide the result of any investigation it may have made with respect to the publication date of the Aventail reference or the dates of conception or reduction to practice of the '135 patent that it indicated it would make in its petition for an extension of time, nor did VirnetX provide any information that it learned from the Microsoft trial that related to the publication date of the Aventail reference. Based on a review of the prosecution history, VirnetX did not disclose that its conception date for the claims of the '135 patent was no earlier than December 1999, nor did VirnetX disclose that the Aventail reference may have been published as early as June 1999, a fact to which VirnetX was made aware during the Microsoft trial.

On June 16, 2010, the Patent Office issued an Action Closing Prosecution. In the action, the examiner recites that he made an attempt to determine the publication date of the Aventail reference, but was unsuccessful. Based on the lack of evidence of the publication date, the examiner withdrew all of the rejections that had

Petitioner Apple Inc. - Exhibit 1026, p. 1237

been based on the Aventail reference.

VirnetX and/or its representatives, agents, and attorneys who were substantively involved in the prosecution of the re-examination knew or should have known of the Microsoft trial and the evidence presented regarding the publication date of the Aventail reference. For example, Mr. Kusmer specifically referenced the Microsoft trial and the potential for additional material information to come to light during that trial when seeking an extension to respond to an office action, as set forth above. VirnetX and/or its representatives, agents, and attorneys withheld this information with the intent to deceive, either willfully or with such gross negligence or recklessness as constituting an act of willfulness amounting to inequitable conduct. Moreover, the high degree of materiality of the Aventail publication and the aforementioned evidence presented at the Microsoft trial leads to an inference of intent to deceive. Among other things, the information withheld was material to the reexamination of the '135 patent, in violation of the duty of candor the representatives and/or the attorneys owed to the Patent Office.

AASTRA TECHNOLOGIES' COUNTERCLAIMS

87. Aastra Technologies Limited ("Aastra Technologies") is a Canadian corporation with its principal place of business at 155 Snow Blvd., Concord, Ontario Canada, L4K 4N9.

88. VirnetX, Inc. ("VirnetX"), as represented in Paragraph 1 of its Original Complaint, has claimed that it is a Delaware corporation with its principal place of business at 5615 Scotts Valley Drive, Suite 110 Scotts Valley, California.

Petitioner Apple Inc. - Exhibit 1026, p. 1238

89. This Court has subject matter jurisdiction over the Counterclaim pursuant to 28 U.S.C. §§ 1331, 1338, and 2201 as it arises under an Act of Congress relating to patents.

90. Venue is proper in this district under 28 U.S.C. §§ 1391(b), (c) and 1400.

91. By filing its complaint, VirnetX has consented to the personal jurisdiction of this Court.

DECLARATORY JUDGMENT FOR NON-INFRINGEMENT OF UNITED STATES PATENT NO. 6,502,135

92. Aastra Technologies hereby re-alleges and incorporates by reference Paragraphs 87-91 as though fully set forth herein.

93. United States Patent No. 6,502,135 ("the '135 patent"), entitled "Agile Network Protocol for Secure Communications with Assured System Availability" was issued on December 31, 2002. VirnetX claims to be the owner by assignment of the '135 patent.

94. Aastra Technologies has not directly infringed, contributed to infringement, or induced infringement of any valid claim of the '135 patent, nor is Aastra Technologies directly infringing, contributing to infringement, or inducing infringement of any valid claim of the '135 patent.

95. An actual controversy exists between Aastra Technologies and VirnetX regarding the alleged infringement '135 patent by virtue of VirnetX's allegation of infringement.

96. Aastra Technologies is entitled to judgment from this Court that the '135 patent is not infringed by Aastra Technologies.

Petitioner Apple Inc. - Exhibit 1026, p. 1239

DECLARATORY JUDGMENT FOR INVALIDITY OF UNITED STATES PATENT NO. 6,502,135

97. Aastra Technologies hereby re-alleges and incorporates by reference Paragraphs 87-96 as though fully set forth herein.

98. The '135 patent is invalid for failing to comply with one or more of the requirements for patentability set forth in Part II of Title 35 U.S.C. § 101 *et seq.*, including without limitation 35 U.S.C. §§102, 103 and/or 112.

99. An actual controversy exists between Aastra Technologies and VirnetX regarding the validity of the '135 patent by virtue of VirnetX's allegation of infringement.

100. Aastra Technologies is entitled to judgment from this Court that the '135 patent is invalid.

DECLARATORY JUDGMENT FOR UNENFORCEABILITY OF UNITED STATES PATENT NO. 6,502,135

101. Aastra Technologies hereby re-alleges and incorporates by reference Paragraphs 87-100 as though fully set forth herein.

102. The '135 patent is unenforceable due to inequitable conduct. Based on the contents of the prosecution history and based on Aastra Technologies' understanding of the allegations by VirnetX, one or more of the people substantively involved in the prosecution of the application leading to the '135 patent, and the subsequent reexamination of the '135 patent, were aware of information material to the patentability of the claims of the '135 patent, but withheld that information from the Patent Office with the intent to deceive.

Petitioner Apple Inc. - Exhibit 1026, p. 1240

103. The existence of US. Patent Application No. 09/399,753 ("the Miller Application"), was withheld during the prosecution of the '135 patent. The pendency of the Miller Application was information material to patentability of the '135 patent based on Aastra Technologies' understanding of the allegations by VirnetX. The withheld information also includes RFC 2401-Security Architecture for the Internet Protocol ("RFC 2401") and the Aventail Administrator's Guide ("Aventail"), which are material to patentability based upon Aastra Technologies' understanding of the allegations by VirnetX. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

104. The Miller Application, RFC 2401, and the Aventail reference are not cumulative to the prior art made of record during prosecution of the '135 patent. There is a substantial likelihood that a reasonable examiner would have considered this art in determining whether to allow the '135 patent to issue.

105. During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution (including Ross Dannenburg) were aware of the Miller Application. Mr. Dannenburg was involved in the prosecution of the Miller Application during the prosecution of the '135 patent at least as early as June 14, 2002, when he signed an Amendment / Response in the prosecution history of the Miller Application. Mr. Dannenburg was involved in the prosecution of the '135 patent at least as early as January 28, 2002, when he signed a Transmittal Form for an Amendment / Response in the prosecution file history of the '135 patent. Therefore, Mr. Dannenburg was involved in the prosecution of the Miller Application while he was prosecuting the '135 patent. Based on Aastra

Petitioner Apple Inc. - Exhibit 1026, p. 1241

Technologies' understanding of the allegations by VirnetX, the pendency of the Miller Application is information material to patentability. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to disclose this material information to the Patent Office at any time during the prosecution of the '135 patent with intent to deceive. Moreover, the materiality of the Miller Application leads to an inference of intent to deceive. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

106. During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution were aware of RFC 2401, including Mr. Dannenburg, because it is mentioned in the specification of the '135 patent. Based on Aastra Technologies' understanding of the allegations by VirnetX, RFC 2401 is material prior art. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to submit this material prior art reference to the Patent Office as required by 37 C.F.R. 1.56 and 37 C.F.R. 1.97, with intent to deceive. Moreover, in mentioning RFC 2401 in the application, those substantively involved in the prosecution of the application described RFC 2401 in a way that concealed its materiality, with intent to deceive. Moreover, the materiality of RFC 2401 leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

107. VirnetX also committed inequitable conduct during the reexamination of the '135 patent. On or about February 15, 2007, VirnetX filed a lawsuit against Microsoft Corporation ("Microsoft") in the Eastern District of Texas, Tyler Division,

Petitioner Apple Inc. - Exhibit 1026, p. 1242

C.A. No. 6:07-CV-80 (the "Microsoft trial"), alleging that Microsoft infringed certain VirnetX patents, including the '135 patent.

108. During the Microsoft trial, one or more witnesses for VirnetX, including inventor Edward Munger, testified that the claims of the '135 patent were conceived no earlier than three months after September 23, 1999, placing the date of conception for claims 1-10 and 12 on or after December 23, 1999.

109. During the Microsoft trial, Microsoft alleged, in part, that claims 1-10 and 12 of the '135 patent were anticipated by the Aventail reference, which on information and belief bears a copyright date between 1996 – 1999.

110. In December 2009, Microsoft filed a reexamination request with the Patent Office requesting re-examination of claims 1-10 and 12 of the '135 patent, citing, among other references, the Aventail reference as prior art under 35 U.S.C. § 102(a). Microsoft asserted that the Aventail reference anticipated claims 1-10 and 12 of the '135 patent.

111. On or about December 31, 2009, the Patent Office ordered re-examination of claims 1-10 and 12 of the '135 patent, finding, in part, that the Aventail reference raised a substantial new question of patentability of all of the requested claims of the '135 patent.

112. On or about January 15, 2010, the Patent Office issued a non-final action rejecting claims 1, 3, 4, 6-10, and 12 as being anticipated by the Aventail reference.

113. On or about February 22, 2010, VirnetX filed a petition to extend its deadline for responding to the office action, pointing out, in part, that it needed additional time to investigate whether the Aventail reference was proper prior art,

Petitioner Apple Inc. - Exhibit 1026, p. 1243

including investigating the dates of conception and reduction to practice of the inventions claimed in the '135 patent as well as diligence there between. The petition also cited as a basis for extension that the Microsoft case was causing a "significant drain" on VirnetX's resources. Moreover, the petition stated that the extension "would likely also permit consideration of any court conclusions regarding the claims presently under reexamination." The petition was filed by Toby Kusmer of McDermott Will & Emery, the same firm that represented VirnetX in the Microsoft case until 2009. The Patent Office responded on or about February 24, 2010, granting an extension, and setting the deadline for response as April 15, 2010.

114. On or about March 8, 2010, the Microsoft trial commenced. During trial, Microsoft argued that the Aventail reference invalidated claims 1-10 and 12 of the '135 patent. Microsoft presented evidence indicating that the Aventail reference may have been published as early as June 1999. Based on a review of the trial record, VirnetX did not dispute the publication date of the Aventail reference. The Microsoft trial concluded on or about March 16, 2010. Therefore, at least as of March 16, 2010, VirnetX was aware that the Aventail reference may have been published at least as early as June 1999, which is prior to the February 15, 2000, filing date of the application that matured into the '135 patent and prior to the earliest conception date of December 1999 claimed by the inventor of the '135 patent.

115. On or about March 25, 2010, VirnetX gave notice to the Patent Office of the outcome of the case and submitted the jury verdict form from the case. On or about March 29, 2010, VirnetX filed a petition requesting that the re-examination

Petitioner Apple Inc. - Exhibit 1026, p. 1244

proceeding be suspended. The Patent Office did not respond to the request until after the date set for VirnetX's response to the non-final office action rejection.

116. On or about April 15, 2010, VirnetX responded to the office action rejection, in part, by asserting that the Aventail reference should not be considered prior art because no evidence had been submitted by Microsoft that established the actual publication date of the Aventail reference. Moreover, VirnetX did not provide the result of any investigation it may have made with respect to the publication date of the Aventail reference or the dates of conception or reduction to practice of the '135 patent that it indicated it would make in its petition for an extension of time, nor did VirnetX provide any information that it learned from the Microsoft trial that related to the publication date of the Aventail reference. Based on a review of the prosecution history, VirnetX did not disclose that its conception date for the claims of the '135 patent was no earlier than December 1999, nor did VirnetX disclose that the Aventail reference may have been published as early as June 1999, a fact to which VirnetX was made aware during the Microsoft trial.

117. On June 16, 2010, the Patent Office issued an Action Closing Prosecution. In the action, the examiner recites that he made an attempt to determine the publication date of the Aventail reference, but was unsuccessful. Based on the lack of evidence of the publication date, the examiner withdrew all of the rejections that had been based on the Aventail reference.

118. VirnetX and/or its representatives, agents, and attorneys who were substantively involved in the prosecution of the re-examination knew or should have known of the Microsoft trial and the evidence presented regarding the publication

Petitioner Apple Inc. - Exhibit 1026, p. 1245

date of the Aventail reference. For example, Mr. Kusmer specifically referenced the Microsoft trial and the potential for additional material information to come to light during that trial when seeking an extension to respond to an office action, as set forth above. VirnetX and/or its representatives, agents, and attorneys withheld this information with the intent to deceive, either willfully or with such gross negligence or recklessness as constituting an act of willfulness amounting to inequitable conduct. Moreover, the high degree of materiality of the Aventail publication and the aforementioned evidence presented at the Microsoft trial leads to an inference of intent to deceive. Among other things, the information withheld was material to the reexamination of the '135 patent, in violation of the duty of candor the representatives and/or the attorneys owed to the Patent Office.

EXCEPTIONAL CASE

119. This is an exceptional case pursuant to 35 U.S.C. § 285 entitling Aastra Technologies to an award of attorneys' fees as a result of, *inter alia*, VirnetX's assertion of the '135 patent against Aastra Technologies with the knowledge that the '135 patent is unenforceable and for VirnetX's failure to perform a reasonable pre-suit investigation of its infringement contentions against Aastra Technologies.

DEMAND FOR JURY TRIAL

120. Aastra Technologies hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

121. WHEREFORE, Aastra Technologies prays for the following relief:

Petitioner Apple Inc. - Exhibit 1026, p. 1246

A. That the Court enter judgment that VirnetX is not entitled to any relief with respect to its allegations against Aastra Technologies and dismiss all of VirnetX's allegations with prejudice;

B. That the Court enter a judgment that Aastra has not infringed and is not directly infringing or indirectly infringing by contribution or inducement, whether willfully or otherwise, any claim of the '135 patent, as alleged by VirnetX;

C. That the Court enter a judgment that the claims of the '135 patent are invalid;

D. That the Court enter a judgment that the claims of the '135 patent are unenforceable;

E. That the Court enter a declaratory judgment that the claims of the '135 patent are not infringed;

F. That the Court enter a declaratory judgment that the claims of the '135 patent are invalid;

G. That the Court enter a declaratory judgment that the claims of the '135 patent are unenforceable;

H. That the Court declare this an exceptional case and award Aastra Technologies its costs, expenses, and reasonable attorneys' fees pursuant to 35 U.S.C. § 285 and all other applicable statutes, rules, and common law; and

Petitioner Apple Inc. - Exhibit 1026, p. 1247

l. That the Court award Aastra Technologies such other and further relief as the Court may deem just and proper.

Petitioner Apple Inc. - Exhibit 1026, p. 1248

DATED: October 29, 2010

Respectfully Submitted,

By: /s/ Phillip N. Cockrell

Phillip N. Cockrell
Lead Attorney
State Bar No. 04465500
pcockrell@pattonroberts.com
PATTON ROBERTS, PLLC
400 Century Plaza
2900 St. Michael Dr.
Texarkana, Texas 75503
Telephone: 903-334-7000
Facsimile: 903-334-7007

Jon B. Hyland
jhyland@pattonroberts.com
State Bar No. 24046131
Robert D. Katz
rkatz@pattonroberts.com
State Bar No. 24057936
PATTON ROBERTS, PLLC
901 Main St., Suite 3300
Dallas, Texas 75202
Telephone: 214-580-3826
Facsimile: 903-334-7007

Petitioner Apple Inc. - Exhibit 1026, p. 1249

CERTIFICATE OF SERVICE

This is to certify that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3) on this the 29th Day of October, 2010.

/s/ Phillip N. Cockrell

Petitioner Apple Inc. - Exhibit 1026, p. 1250

EXHIBIT E

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VirnetX Inc.,	§	
	§	
Plaintiff,	§	
	§	
v.	§	
	§	**CIVIL ACTION NO. 6:10-CV-417 LED**
Cisco Systems, Inc.	§	
Apple Inc.	§	**Judge: Hon. Leonard Davis**
Aastra USA Inc.	§	
Aastra Technologies Ltd.	§	
NEC Corporation, and	§	
NEC Corporation of America,	§	
	§	
Defendants.	§	
	§	

DEFENDANT AND COUNTERCLAIM-PLAINTIFF AASTRA USA INC.'S ANSWER, AFFIRMATIVE DEFENSES AND COUNTERCLAIMS TO VIRNETX INC.'S ORIGINAL COMPLAINT

Aastra USA Inc. ("Aastra USA"), defendant and counterclaim-plaintiff in the above-entitled and numbered civil action, replies to the Original Complaint of VirnetX Inc. ("VirnetX") as follows.

THE PARTIES

1. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is "a corporation organized and existing under the laws of the State of Delaware, and maintains its principal place of business at 5615 Scotts Valley Drive, Suite 110 Scotts Valley, California," and, therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1252

2. Aastra USA admits that Aastra Technologies Limited is a Canadian corporation with its principal place of business at 155 Snow Blvd., Concord, Ontario Canada, L4K 4N9. Aastra USA admits that it is a Delaware corporation with its principal place of business at 2811 Internet Blvd., Frisco, Texas 75034. Aastra USA denies that Aastra Technologies Limited regularly conducts and transacts business in Texas, throughout the United States, and within the Eastern District of Texas. Aastra USA admits that it regularly conducts and transacts business in Texas, throughout the United States, and within the Eastern District of Texas. Aastra USA denies that either it or Aastra Technologies Limited have committed or continues to commit any acts that give rise to any cause of action asserted in VirnetX's complaint. Except as admitted above, Aastra USA denies the allegations of Paragraph 2.

3. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 3 and therefore, denies these allegations.

4. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 4 and therefore, denies these allegations.

5. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 5 and therefore, denies these allegations.

JURISDICTION AND VENUE

6. Aastra USA admits that VirnetX purports to bring this action under the patent laws of the United States, Title 35, United States Code, but Aastra USA denies

Petitioner Apple Inc. - Exhibit 1026, p. 1253

any liability thereunder. Aastra USA does not contest that the Court has exclusive subject matter over this matter under 28 U.S.C. § 1338. Except as admitted above, Aastra USA denies the allegations of Paragraph 6.

7. Admitted.

8. Aastra USA admits that this Court has personal jurisdiction over Aastra USA. Except as admitted above, Aastra USA denies the allegations of Paragraph 8.

ASSERTED PATENTS

9. Aastra USA admits that United States Patent No. 6,502,135 ("the '135 patent"), entitled "Agile Network Protocol for Secure Communications with Assured System Availability" issued on December 31, 2002, but denies any further characterization of the '135 patent, its inventors, or its examination as alleged in Paragraph 9. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '135 patent and possesses all rights of recovery under the '135 patent" and, therefore, denies these allegations. Aastra USA admits that a purported copy of the '135 patent was attached to the complaint as Exhibit A. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 9.

10. Aastra USA admits that United States Patent No. 6,839,759 ("the '759 patent"), entitled "Method for Establishing Secure Communication Link Between Computers of Virtual Private Network Without User Entering Any Cryptographic Information" issued on January 4, 2005, but denies any further characterization of the '759 patent, its inventors, or its examination as alleged in Paragraph 10. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the

Petitioner Apple Inc. - Exhibit 1026, p. 1254

allegations that VirnetX is the "owner of all rights, title, and interest in and to the '759 patent and possesses all rights of recovery under the '759 patent" and, therefore, denies these allegations. Aastra USA admits that a purported copy of the '759 patent was attached to the complaint as Exhibit B. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 10.

11. Aastra USA admits that United States Patent No. 7,188,180 ("the '180 patent"), entitled "Method for Establishing Secure Communications Link Between Computers of Virtual Private Network" issued on March 6, 2007, but denies any further characterization of the '180 patent, its inventors, or its examination as alleged in Paragraph 11. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '180 patent and possesses all rights of recovery under the '180 patent" and, therefore, denies these allegations. Aastra USA admits that a purported copy of the '180 patent was attached to the complaint as Exhibit C. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 11.

12. Aastra USA admits that United States Patent No. 7,418,504 ("the '504 patent"), entitled "Agile Network Protocol for Secure Communications Using Secure Domain Names" issued on August 26, 2008, but denies any further characterization of the '504 patent, its inventors, or its examination as alleged in Paragraph 12. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '504 patent and possesses all rights of recovery under the '504 patent" and, therefore, denies these allegations. Aastra USA admits that a purported copy of the '504 patent

Petitioner Apple Inc. - Exhibit 1026, p. 1255

was attached to the complaint as Exhibit D. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 12.

13. Aastra USA admits that United States Patent No. 7,490,151 ("the '151 patent"), entitled "Establishment of a Secure Communication Link Based on a Domain Name Service (DNS) Request" issued on February 10, 2009, but denies any further characterization of the '151 patent, its inventors, or its examination as alleged in Paragraph 13. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations that VirnetX is the "owner of all rights, title, and interest in and to the '151 patent and possesses all rights of recovery under the '151 patent" and, therefore, denies these allegations. Aastra USA admits that a purported copy of the '151 patent was attached to the complaint as exhibit E. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 13.

COUNT ONE

PATENT INFRINGEMENT BY AASTRA USA

14. Aastra USA incorporates by reference paragraphs 1-13 as if fully set forth herein. Aastra USA denies that it has infringed and/or continues to infringe the '135 patent.

15. Aastra USA admits that it makes, sells, offers for sale, exports, imports, supplies, and/or distributes within and from the United States the Clearspan platform, Pointspan platform, 6725ip telephone, 6721ip telephone, 6739i telephone, 6730i telephone, 6731i telephone, 6753i (53i) telephone, 6755i (55i) telephone, 6757i (57i) telephone, 6757i CT (57i CT) telephone, M670i (536M) Expansion Module, M675i (560M) Expansion Module, 9143i telephone, 9480i telephone, and 9480i CT

Petitioner Apple Inc. - Exhibit 1026, p. 1256

telephone. Aastra USA denies that any of these products infringe any valid claim of the '135 patent. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 15.

16. Aastra USA admits that it uses the products listed in Paragraph 15, but denies that such use infringes any valid claim of the '135 patent. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 16.

17. Aastra USA admits that it sells the products listed in Paragraph 15 to parties who use said products, but denies that such use infringes any valid claim of the '135 patent. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 17.

18. Denied.

19. Denied.

20. Denied.

21. Denied.

22. Aastra USA admits that it has received actual notice of infringement by virtue of the filing of this lawsuit. Aastra USA denies that it has received constructive notice. Aastra USA denies that VirnetX has complied with the requirements of 35 U.S.C. § 287. Except as expressly admitted above, Aastra USA denies the allegations in Paragraph 22.

COUNT TWO

PATENT INFRINGEMENT BY APPLE

23. Aastra USA incorporates by reference paragraphs 1-22 as if fully set forth herein. Aastra USA is without knowledge or information sufficient to form a belief as

Petitioner Apple Inc. - Exhibit 1026, p. 1257

to the truth of the allegations set forth in Paragraph 23 and therefore, denies these allegations.

24. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 24 and therefore, denies these allegations.

25. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 25 and therefore, denies these allegations.

26. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 26 and therefore, denies these allegations.

27. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 27 and therefore, denies these allegations.

28. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 28 and therefore, denies these allegations.

29. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 29 and therefore, denies these allegations.

30. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 30 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1258

31. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 31 and therefore, denies these allegations.

32. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 32 and therefore, denies these allegations.

33. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 33 and therefore, denies these allegations.

34. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 34 and therefore, denies these allegations.

35. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 35 and therefore, denies these allegations.

36. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 36 and therefore, denies these allegations.

COUNT THREE

PATENT INFRINGEMENT BY CISCO

37. Aastra USA incorporates by reference paragraphs 1-36 as if fully set forth herein. Aastra USA is without knowledge or information sufficient to form a belief as

Petitioner Apple Inc. - Exhibit 1026, p. 1259

to the truth of the allegations set forth in Paragraph 37 and therefore, denies these allegations.

38. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 38 and therefore, denies these allegations.

39. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 39 and therefore, denies these allegations.

40. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 40 and therefore, denies these allegations.

41. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 41 and therefore, denies these allegations.

42. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 42 and therefore, denies these allegations.

43. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 43 and therefore, denies these allegations.

44. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 44 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1260

45. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 45 and therefore, denies these allegations.

46. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 46 and therefore, denies these allegations.

47. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 47 and therefore, denies these allegations.

48. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 48 and therefore, denies these allegations.

49. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 49 and therefore, denies these allegations.

50. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 50 and therefore, denies these allegations.

51. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 51 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1261

52. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 52 and therefore, denies these allegations.

53. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 53 and therefore, denies these allegations.

54. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 54 and therefore, denies these allegations.

55. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 55 and therefore, denies these allegations.

56. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 56 and therefore, denies these allegations.

57. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 57 and therefore, denies these allegations.

58. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 58 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1262

59. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 59 and therefore, denies these allegations.

60. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 60 and therefore, denies these allegations.

61. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 61 and therefore, denies these allegations.

62. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 62 and therefore, denies these allegations.

63. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 63 and therefore, denies these allegations.

COUNT FOUR

PATENT INFRINGEMENT BY NEC

64. Aastra USA incorporates by reference paragraphs 1-63 as if fully set forth herein. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 64 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1263

65. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 65 and therefore, denies these allegations.

66. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 66 and therefore, denies these allegations.

67. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 67 and therefore, denies these allegations.

68. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 68 and therefore, denies these allegations.

69. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 69 and therefore, denies these allegations.

70. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 70 and therefore, denies these allegations.

71. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 71 and therefore, denies these allegations.

Petitioner Apple Inc. - Exhibit 1026, p. 1264

72. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 72 and therefore, denies these allegations.

73. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 73 and therefore, denies these allegations.

74. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 74 and therefore, denies these allegations.

75. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 75 and therefore, denies these allegations.

76. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 76 and therefore, denies these allegations.

77. Aastra USA is without knowledge or information sufficient to form a belief as to the truth of the allegations set forth in Paragraph 77 and therefore, denies these allegations.

AASTRA USA'S AFFIRMATIVE DEFENSES

78. Aastra USA has not and does not literally, directly, contributorily, by way of inducement, and/or under the doctrine of equivalents, infringe any valid and/or enforceable claim of the '135 patent.

Petitioner Apple Inc. - Exhibit 1026, p. 1265

79. Each of the claims of the '135 patent are invalid for failing to comply with one of more of the requirements for patentability specified by Part II of Title 35 of the United States Code §101 *et seq.*, including without limitation 35 U.S.C. §§ 102, 103 and/or 112.

80. VirnetX is estopped from construing the claims of the '135 patent to cover or include, either literally or by application of the doctrine of equivalents, methods used, devices manufactured, used, imported, sold or offered for sale by Aastra USA because of admissions and statements to the PTO during prosecution of the applications leading to the issuance of the patent, disclosure or language in the specification of the patent and/or limitations in the claims of the patent.

81. The relief sought by VirnetX is barred in whole or in part by the doctrine of laches.

82. To the extent that products accused of infringement were or are used or manufactured by or for the United States , the relief sought by VirnetX is limited by 28 U.S.C. § 1498(a).

83. The relief sought by VirnetX is barred in whole or in part by 35 U.S.C. § 287.

84. VirnetX is not entitled to an injunction against Aastra USA because VirnetX has an adequate remedy at law.

85. VirnetX lacks standing to bring suit to enforce the '135 patent because it does not possess all substantial rights in the '135 patent.

86. The '135 patent is unenforceable due to inequitable conduct. Based on the contents of the prosecution history and based on Aastra USA's understanding of the

Petitioner Apple Inc. - Exhibit 1026, p. 1266

allegations by VirnetX, one or more of the people substantively involved in the prosecution of the application leading to the '135 patent, and the subsequent reexamination of the '135 patent, were aware of information material to the patentability of the claims of the '135 patent, but withheld that information from the Patent Office with the intent to deceive.

Existence of US. Patent Application No. 09/399,753 ("the Miller Application"), was withheld during the prosecution of the '135 patent. The pendency of the Miller Application was information material to patentability of the '135 patent based on Aastra USA's understanding of the allegations by VirnetX. The withheld information also includes RFC 2401-Security Architecture for the Internet Protocol ("RFC 2401") and the Aventail Administrator's Guide ("Aventail"), which are material to patentability based upon Aastra USA's understanding of the allegations by VirnetX. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

The Miller Application, RFC 2401, and the Aventail reference are not cumulative to the prior art made of record during prosecution of the '135 patent. There is a substantial likelihood that a reasonable examiner would have considered this art in determining whether to allow the '135 patent to issue.

During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution (including Ross Dannenburg) were aware of the Miller Application. Mr. Dannenburg was involved in the prosecution of the Miller Application during the prosecution of the '135 patent at least as early as June 14, 2002, when he signed an Amendment / Response in the

Petitioner Apple Inc. - Exhibit 1026, p. 1267

prosecution history of the Miller Application. Mr. Dannenburg was involved in the prosecution of the '135 patent at least as early as January 28, 2002, when he signed a Transmittal Form for an Amendment / Response in the prosecution file history of the '135 patent. Therefore, Mr. Dannenburg was involved in the prosecution of the Miller Application while he was prosecuting the '135 patent. Based on Aastra USA's understanding of the allegations by VirnetX, the pendency of the Miller Application is information material to patentability. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to disclose this material information to the Patent Office at any time during the prosecution of the '135 patent with intent to deceive. Moreover, the materiality of the Miller Application leads to an inference of intent to deceive. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution were aware of RFC 2401, including Mr. Dannenburg, because it is mentioned in the specification of the '135 patent. Based on Aastra USA's understanding of the allegations by VirnetX, RFC 2401 is material prior art. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to submit this material prior art reference to the Patent Office as required by 37 C.F.R. 1.56 and 37 C.F.R. 1.97, with intent to deceive. Moreover, in mentioning RFC 2401 in the application, those substantively involved in the prosecution of the application described RFC 2401 in a way that concealed its materiality, with intent to deceive. Moreover, the materiality of

Petitioner Apple Inc. - Exhibit 1026, p. 1268

RFC 2401 leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

VirnetX also committed inequitable conduct during the reexamination of the '135 patent. On or about February 15, 2007, VirnetX filed a lawsuit against Microsoft Corporation ("Microsoft") in the Eastern District of Texas, Tyler Division, C.A. No. 6:07-CV-80 (the "Microsoft trial"), alleging that Microsoft infringed certain VirnetX patents, including the '135 patent.

During the Microsoft trial, one or more witnesses for VirnetX, including inventor Edward Munger, testified that the claims of the '135 patent were conceived no earlier than three months after September 23, 1999, placing the date of conception for claims 1-10 and 12 on or after December 23, 1999.

During the Microsoft trial, Microsoft alleged, in part, that claims 1-10 and 12 of the '135 patent were anticipated by the Aventail reference, which on information and belief bears a copyright date between 1996 – 1999.

In December 2009, Microsoft filed a reexamination request with the Patent Office requesting re-examination of claims 1-10 and 12 of the '135 patent, citing, among other references, the Aventail reference as prior art under 35 U.S.C. § 102(a). Microsoft asserted that the Aventail reference anticipated claims 1-10 and 12 of the '135 patent.

On or about December 31, 2009, the Patent Office ordered re-examination of claims 1-10 and 12 of the '135 patent, finding, in part, that the Aventail reference raised a substantial new question of patentability of all of the requested claims of the '135 patent.

Petitioner Apple Inc. - Exhibit 1026, p. 1269

On or about January 15, 2010, the Patent Office issued a non-final action rejecting claims 1, 3, 4, 6-10, and 12 as being anticipated by the Aventail reference.

On or about February 22, 2010, VirnetX filed a petition to extend its deadline for responding to the office action, pointing out, in part, that it needed additional time to investigate whether the Aventail reference was proper prior art, including investigating the dates of conception and reduction to practice of the inventions claimed in the '135 patent as well as diligence there between. The petition also cited as a basis for extension that the Microsoft case was causing a "significant drain" on VirnetX's resources. Moreover, the petition stated that the extension "would likely also permit consideration of any court conclusions regarding the claims presently under reexamination." The petition was filed by Toby Kusmer of McDermott Will & Emery, the same firm that represented VirnetX in the Microsoft case until 2009. The Patent Office responded on or about February 24, 2010, granting an extension, and setting the deadline for response as April 15, 2010.

On or about March 8, 2010, the Microsoft trial commenced. During trial, Microsoft argued that the Aventail reference invalidated claims 1-10 and 12 of the '135 patent. Microsoft presented evidence indicating that the Aventail reference may have been published as early as June 1999. Based on a review of the trial record, VirnetX did not dispute the publication date of the Aventail reference. The Microsoft trial concluded on or about March 16, 2010. Therefore, at least as of March 16, VirnetX was aware that the Aventail reference may have been published at least as early as June 1999, which is prior to the February 15, 2000, filing date of the application that matured into the '135 patent and prior to the earliest conception date

Petitioner Apple Inc. - Exhibit 1026, p. 1270

of December 1999 claimed by the inventor of the '135 patent.

On or about March 25, 2010 VirnetX gave notice to the Patent Office of the outcome of the case and submitted the jury verdict form from the case. On or about March 29, 2010, VirnetX filed a petition requesting that the re-examination proceeding be suspended. The Patent Office did not respond to the request until after the date set for VirnetX's response to the non-final office action rejection.

On or about April 15, 2010, VirnetX responded to the office action rejection, in part, by asserting that the Aventail reference should not be considered prior art because no evidence had been submitted by Microsoft that established the actual publication date of the Aventail reference. Moreover, VirnetX did not provide the result of any investigation it may have made with respect to the publication date of the Aventail reference or the dates of conception or reduction to practice of the '135 patent that it indicated it would make in its petition for an extension of time, nor did VirnetX provide any information that it learned from the Microsoft trial that related to the publication date of the Aventail reference. Based on a review of the prosecution history, VirnetX did not disclose that its conception date for the claims of the '135 patent was no earlier than December 1999, nor did VirnetX disclose that the Aventail reference may have been published as early as June 1999, a fact to which VirnetX was made aware during the Microsoft trial.

On June 16, 2010, the Patent Office issued an Action Closing Prosecution. In the action, the examiner recites that he made an attempt to determine the publication date of the Aventail reference, but was unsuccessful. Based on the lack of evidence of the publication date, the examiner withdrew all of the rejections that had

Petitioner Apple Inc. - Exhibit 1026, p. 1271

been based on the Aventail reference.

VirnetX and/or its representatives, agents, and attorneys who were substantively involved in the prosecution of the re-examination knew or should have known of the Microsoft trial and the evidence presented regarding the publication date of the Aventail reference. For example, Mr. Kusmer specifically referenced the Microsoft trial and the potential for additional material information to come to light during that trial when seeking an extension to respond to an office action, as set forth above. VirnetX and/or its representatives, agents, and attorneys withheld this information with the intent to deceive, either willfully or with such gross negligence or recklessness as constituting an act of willfulness amounting to inequitable conduct. Moreover, the high degree of materiality of the Aventail publication and the aforementioned evidence presented at the Microsoft trial leads to an inference of intent to deceive. Among other things, the information withheld was material to the reexamination of the '135 patent, in violation of the duty of candor the representatives and/or the attorneys owed to the Patent Office.

AASTRA USA'S COUNTERCLAIMS

87. Aastra USA Inc. ("Aastra USA") is a Delaware corporation with its principal place of business at 2811 Internet Blvd., Frisco, Texas 75034.

88. VirnetX, Inc. ("VirnetX"), as represented in Paragraph 1 of its Original Complaint, has claimed that it is a Delaware corporation with its principal place of business at 5615 Scotts Valley Drive, Suite 110 Scotts Valley, California.

Petitioner Apple Inc. - Exhibit 1026, p. 1272

89. This Court has subject matter jurisdiction over the Counterclaim pursuant to 28 U.S.C. §§ 1331, 1338, and 2201 as it arises under an Act of Congress relating to patents.

90. Venue is proper in this district under 28 U.S.C. §§ 1391(b), (c) and 1400.

91. By filing its complaint, VirnetX has consented to the personal jurisdiction of this Court.

DECLARATORY JUDGMENT FOR NON-INFRINGEMENT OF UNITED STATES PATENT NO. 6,502,135

92. Aastra USA hereby re-alleges and incorporates by reference Paragraphs 87-91 as though fully set forth herein.

93. United States Patent No. 6,502,135 ("the '135 patent"), entitled "Agile Network Protocol for Secure Communications with Assured System Availability" was issued on December 31, 2002. VirnetX claims to be the owner by assignment of the '135 patent.

94. Aastra USA has not directly infringed, contributed to infringement, or induced infringement of any valid claim of the '135 patent, nor is Aastra USA directly infringing, contributing to infringement, or inducing infringement of any valid claim of the '135 patent.

95. An actual controversy exists between Aastra USA and VirnetX regarding the alleged infringement '135 patent by virtue of VirnetX's allegation of infringement.

96. Aastra USA is entitled to judgment from this Court that the '135 patent is not infringed by Aastra USA.

Petitioner Apple Inc. - Exhibit 1026, p. 1273

DECLARATORY JUDGMENT FOR INVALIDITY OF UNITED STATES PATENT NO. 6,502,135

97. Aastra USA hereby re-alleges and incorporates by reference Paragraphs 87-96 as though fully set forth herein.

98. The '135 patent is invalid for failing to comply with one or more of the requirements for patentability set forth in Part II of Title 35 U.S.C. § 101 *et seq.*, including without limitation 35 U.S.C. §§102, 103 and/or 112.

99. An actual controversy exists between Aastra USA and VirnetX regarding the validity of the '135 patent by virtue of VirnetX's allegation of infringement.

100. Aastra USA is entitled to judgment from this Court that the '135 patent is invalid.

DECLARATORY JUDGMENT FOR UNENFORCEABILITY OF UNITED STATES PATENT NO. 6,502,135

101. Aastra USA hereby re-alleges and incorporates by reference Paragraphs 87-100 as though fully set forth herein.

102. The '135 patent is unenforceable due to inequitable conduct. Based on the contents of the prosecution history and based on Aastra USA's understanding of the allegations by VirnetX, one or more of the people substantively involved in the prosecution of the application leading to the '135 patent, and the subsequent reexamination of the '135 patent, were aware of information material to the patentability of the claims of the '135 patent, but withheld that information from the Patent Office with the intent to deceive.

103. The existence of US. Patent Application No. 09/399,753 ("the Miller Application"), was withheld during the prosecution of the '135 patent. The pendency

Petitioner Apple Inc. - Exhibit 1026, p. 1274

of the Miller Application was information material to patentability of the '135 patent based on Aastra USA's understanding of the allegations by VirnetX. The withheld information also includes RFC 2401-Security Architecture for the Internet Protocol ("RFC 2401") and the Aventail Administrator's Guide ("Aventail"), which are material to patentability based upon Aastra USA's understanding of the allegations by VirnetX. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

104. The Miller Application, RFC 2401, and the Aventail reference are not cumulative to the prior art made of record during prosecution of the '135 patent. There is a substantial likelihood that a reasonable examiner would have considered this art in determining whether to allow the '135 patent to issue.

105. During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution (including Ross Dannenburg) were aware of the Miller Application. Mr. Dannenburg was involved in the prosecution of the Miller Application during the prosecution of the '135 patent at least as early as June 14, 2002, when he signed an Amendment / Response in the prosecution history of the Miller Application. Mr. Dannenburg was involved in the prosecution of the '135 patent at least as early as January 28, 2002, when he signed a Transmittal Form for an Amendment / Response in the prosecution file history of the '135 patent. Therefore, Mr. Dannenburg was involved in the prosecution of the Miller Application while he was prosecuting the '135 patent. Based on Aastra USA's understanding of the allegations by VirnetX, the pendency of the Miller Application is information material to patentability. Nonetheless, those substantively involved in

Petitioner Apple Inc. - Exhibit 1026, p. 1275

the prosecution of the application intentionally failed to disclose this material information to the Patent Office at any time during the prosecution of the '135 patent with intent to deceive. Moreover, the materiality of the Miller Application leads to an inference of intent to deceive. This withholding of information material to patentability with the intent to deceive the Patent Office constitutes inequitable conduct.

106. During the prosecution of the application leading to the '135 patent, one or more of the people substantively involved in its prosecution were aware of RFC 2401, including Mr. Dannenburg, because it is mentioned in the specification of the '135 patent. Based on Aastra USA's understanding of the allegations by VirnetX, RFC 2401 is material prior art. Nonetheless, those substantively involved in the prosecution of the application intentionally failed to submit this material prior art reference to the Patent Office as required by 37 C.F.R. 1.56 and 37 C.F.R. 1.97, with intent to deceive. Moreover, in mentioning RFC 2401 in the application, those substantively involved in the prosecution of the application described RFC 2401 in a way that concealed its materiality, with intent to deceive. Moreover, the materiality of RFC 2401 leads to an inference of intent to deceive. This conduct, undertaken with the intent to deceive the Patent Office, constitutes inequitable conduct.

107. VirnetX also committed inequitable conduct during the reexamination of the '135 patent. On or about February 15, 2007, VirnetX filed a lawsuit against Microsoft Corporation ("Microsoft") in the Eastern District of Texas, Tyler Division, C.A. No. 6:07-CV-80 (the "Microsoft trial"), alleging that Microsoft infringed certain VirnetX patents, including the '135 patent.

Petitioner Apple Inc. - Exhibit 1026, p. 1276

108. During the Microsoft trial, one or more witnesses for VirnetX, including inventor Edward Munger, testified that the claims of the '135 patent were conceived no earlier than three months after September 23, 1999, placing the date of conception for claims 1-10 and 12 on or after December 23, 1999.

109. During the Microsoft trial, Microsoft alleged, in part, that claims 1-10 and 12 of the '135 patent were anticipated by the Aventail reference, which on information and belief bears a copyright date between 1996 – 1999.

110. In December 2009, Microsoft filed a reexamination request with the Patent Office requesting re-examination of claims 1-10 and 12 of the '135 patent, citing, among other references, the Aventail reference as prior art under 35 U.S.C. § 102(a). Microsoft asserted that the Aventail reference anticipated claims 1-10 and 12 of the '135 patent.

111. On or about December 31, 2009, the Patent Office ordered re-examination of claims 1-10 and 12 of the '135 patent, finding, in part, that the Aventail reference raised a substantial new question of patentability of all of the requested claims of the '135 patent.

112. On or about January 15, 2010, the Patent Office issued a non-final action rejecting claims 1, 3, 4, 6-10, and 12 as being anticipated by the Aventail reference.

113. On or about February 22, 2010, VirnetX filed a petition to extend its deadline for responding to the office action, pointing out, in part, that it needed additional time to investigate whether the Aventail reference was proper prior art, including investigating the dates of conception and reduction to practice of the inventions claimed in the '135 patent as well as diligence there between. The petition

Petitioner Apple Inc. - Exhibit 1026, p. 1277

also cited as a basis for extension that the Microsoft case was causing a "significant drain" on VirnetX's resources. Moreover, the petition stated that the extension "would likely also permit consideration of any court conclusions regarding the claims presently under reexamination." The petition was filed by Toby Kusmer of McDermott Will & Emery, the same firm that represented VirnetX in the Microsoft case until 2009. The Patent Office responded on or about February 24, 2010, granting an extension, and setting the deadline for response as April 15, 2010.

114. On or about March 8, 2010, the Microsoft trial commenced. During trial, Microsoft argued that the Aventail reference invalidated claims 1-10 and 12 of the '135 patent. Microsoft presented evidence indicating that the Aventail reference may have been published as early as June 1999. Based on a review of the trial record, VirnetX did not dispute the publication date of the Aventail reference. The Microsoft trial concluded on or about March 16, 2010. Therefore, at least as of March 16, 2010, VirnetX was aware that the Aventail reference may have been published at least as early as June 1999, which is prior to the February 15, 2000, filing date of the application that matured into the '135 patent and prior to the earliest conception date of December 1999 claimed by the inventor of the '135 patent.

115. On or about March 25, 2010, VirnetX gave notice to the Patent Office of the outcome of the case and submitted the jury verdict form from the case. On or about March 29, 2010, VirnetX filed a petition requesting that the re-examination proceeding be suspended. The Patent Office did not respond to the request until after the date set for VirnetX's response to the non-final office action rejection.

Petitioner Apple Inc. - Exhibit 1026, p. 1278

116. On or about April 15, 2010, VirnetX responded to the office action rejection, in part, by asserting that the Aventail reference should not be considered prior art because no evidence had been submitted by Microsoft that established the actual publication date of the Aventail reference. Moreover, VirnetX did not provide the result of any investigation it may have made with respect to the publication date of the Aventail reference or the dates of conception or reduction to practice of the '135 patent that it indicated it would make in its petition for an extension of time, nor did VirnetX provide any information that it learned from the Microsoft trial that related to the publication date of the Aventail reference. Based on a review of the prosecution history, VirnetX did not disclose that its conception date for the claims of the '135 patent was no earlier than December 1999, nor did VirnetX disclose that the Aventail reference may have been published as early as June 1999, a fact to which VirnetX was made aware during the Microsoft trial.

117. On June 16, 2010, the Patent Office issued an Action Closing Prosecution. In the action, the examiner recites that he made an attempt to determine the publication date of the Aventail reference, but was unsuccessful. Based on the lack of evidence of the publication date, the examiner withdrew all of the rejections that had been based on the Aventail reference.

118. VirnetX and/or its representatives, agents, and attorneys who were substantively involved in the prosecution of the re-examination knew or should have known of the Microsoft trial and the evidence presented regarding the publication date of the Aventail reference. For example, Mr. Kusmer specifically referenced the Microsoft trial and the potential for additional material information to come to light

Petitioner Apple Inc. - Exhibit 1026, p. 1279

during that trial when seeking an extension to respond to an office action, as set forth above. VirnetX and/or its representatives, agents, and attorneys withheld this information with the intent to deceive, either willfully or with such gross negligence or recklessness as constituting an act of willfulness amounting to inequitable conduct. Moreover, the high degree of materiality of the Aventail publication and the aforementioned evidence presented at the Microsoft trial leads to an inference of intent to deceive. Among other things, the information withheld was material to the reexamination of the '135 patent, in violation of the duty of candor the representatives and/or the attorneys owed to the Patent Office.

EXCEPTIONAL CASE

119. This is an exceptional case pursuant to 35 U.S.C. § 285 entitling Aastra USA to an award of attorneys' fees as a result of, *inter alia*, VirnetX's assertion of the '135 patent against Aastra USA with the knowledge that the '135 patent is unenforceable and for VirnetX's failure to perform a reasonable pre-suit investigation of its infringement contentions against Aastra USA.

DEMAND FOR JURY TRIAL

120. Aastra USA hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

121. WHEREFORE, Aastra USA prays for the following relief:

A. That the Court enter judgment that VirnetX is not entitled to any relief with respect to its allegations against Aastra USA and dismiss all of VirnetX's allegations with prejudice;

Petitioner Apple Inc. - Exhibit 1026, p. 1280

B. That the Court enter a judgment that Aastra USA has not infringed and is not directly infringing or indirectly infringing by contribution or inducement, whether willfully or otherwise, any claim of the '135 patent, as alleged by VirnetX;

C. That the Court enter a judgment that the claims of the '135 patent are invalid;

D. That the Court enter a judgment that the claims of the '135 patent are unenforceable;

E. That the Court enter a declaratory judgment that the claims of the '135 patent are not infringed;

F. That the Court enter a declaratory judgment that the claims of the '135 patent are invalid;

G. That the Court enter a declaratory judgment that the claims of the '135 patent are unenforceable;

H. That the Court declare this an exceptional case and award Aastra USA its costs, expenses, and reasonable attorneys' fees pursuant to 35 U.S.C. § 285 and all other applicable statutes, rules, and common law; and

I. That the Court award Aastra USA such other and further relief as the Court may deem just and proper.

Petitioner Apple Inc. - Exhibit 1026, p. 1281

DATED: October 29, 2010

Respectfully Submitted,

By: /s/ Phillip N. Cockrell ____

Phillip N. Cockrell
Lead Attorney
State Bar No. 04465500
pcockrell@pattonroberts.com
PATTON ROBERTS, PLLC
400 Century Plaza
2900 St. Michael Dr.
Texarkana, Texas 75503
Telephone: 903-334-7000
Facsimile: 903-334-7007

Jon B. Hyland
jhyland@pattonroberts.com
State Bar No. 24046131
Robert D. Katz
rkatz@pattonroberts.com
State Bar No. 24057936
PATTON ROBERTS, PLLC
901 Main St., Suite 3300
Dallas, Texas 75202
Telephone: 214-580-3826
Facsimile: 903-334-7007

Petitioner Apple Inc. - Exhibit 1026, p. 1282

CERTIFICATE OF SERVICE

This is to certify that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3) on this the 29th. Day of October, 2010.

__/s/ Phillip N. Cockrell_____

Petitioner Apple Inc. - Exhibit 1026, p. 1283

EXHIBIT F1

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX	*	Civil Docket No.
	*	6:07-CV-80
VS.	*	Tyler, Texas
	*	
	*	March 8, 2010
MICROSOFT CORPORATION	*	8:45 A.M.

TRANSCRIPT OF JURY TRIAL
BEFORE THE HONORABLE JUDGE LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPEARANCES:

FOR THE PLAINTIFFS:
MR. DOUGLAS CAWLEY
MR. BRADLEY CALDWELL
MR. JASON D. CASSADY
MR. LUKE MCLEROY
McKool-Smith
300 Crescent Court
Suite 1500
Dallas, TX 75201

MR. ROBERT M. PARKER
Parker, Bunt & Ainsworth
100 East Ferguson
Suite 1114
Tyler, TX 75702

APPEARANCES CONTINUED ON NEXT PAGE:

COURT REPORTERS:
MS. SUSAN SIMMONS, CSR
Ms. Judith Werlinger, CSR
Official Court Reporters
100 East Houston, Suite 125
Marshall, TX 75670
903/935-3868

(Proceedings recorded by mechanical stenography, transcript produced on CAT system.)

APPEARANCES CONTINUED:

FOR THE DEFENDANT:
MR. MATTHEW POWERS
MR. JARED BOBROW
MR. PAUL EHRLICH
MR. THOMAS KING
MR. ROBERT GERRITY
Weil Gotshal & Manges
201 Redwood Shores Parkway
5th Floor
Redwood City, CA 94065

MS. ELIZABETH WEISWASSER
MR. TIM DeMASI
Weil Gotshal & Manges
767 Fifth Avenue
New York, NY 10153

MR. DANIEL BOOTH
Weil Gotshal & Manges
700 Louisiana
Suite 1600
Houston, TX 77002

MR. RICHARD SAYLES
MR. MARK STRACHAN
Sayles Werbner
1201 Elm Street
4400 Renaissance Tower
Dallas, TX 75270

MR. ERIC FINDLAY
Findlay Craft
6760 Old Jacksonville Highway
Suite 101
Tyler, TX 75703

* * * * * *

P R O C E E D I N G S

(Jury out.)

COURT SECURITY OFFICER: All rise.

THE COURT: Please be seated. All right Ms. Ferguson, if you'll call the case.

COURTROOM DEPUTY: Case No. 6:07-cv-80, VirnetX versus Microsoft.

THE COURT: All right. Announcements?

MR. CAWLEY: Good morning, Your Honor. The Plaintiff VirnetX is ready.

THE COURT: Okay.

MR. POWERS: Good morning, Your Honor. Microsoft is ready as well.

THE COURT: Very well.

My goodness, we have a big audience today.

All right. Do we have some matters to take up with the Court before we bring the jury in?

MR. POWERS: Yes, Your Honor, just a few.

The first relates to the claims at issue which VirnetX has dropped at pretrial. There's three of them, and we just wanted it to be on the record that those are dropped with prejudice. And I understand VirnetX has no objection to that.

The three are, first, Claim 7 of the '135 patent; second, the allegations of contributory infringement as to the '180 patent; and, third, the allegations with regard to the '135 patent against the PeerNet APIs.

THE COURT: Is that correct, that VirnetX

dismisses those with prejudice?

MR. McLEROY: Yes, Your Honor.

THE COURT: Okay. Very well.

What else?

MR. POWERS: The second, Your Honor, is the stipulation which was filed by the parties last night regarding objections to certain exhibits. I have a copy for you, if it's not immediately available.

The parties just thought that would be an easier way of handling that issue outside the presence of the jury.

THE COURT: I want to look at that, and I want to hear some just discussion as to what that is. Lots of times on those, I like a final bite at the apple in the context of hearing the testimony, if it's something that you're really serious about wanting to put in, and you think it's important to the case. But maybe y'all can explain it to me such that we don't need to do that. But let's -- I don't want to keep the jury waiting, so we'll take that up later.

MR. POWERS: With that, I think there's only one more issue that probably needs to be discussed today before the jury, and that's a question about how Your Honor wishes to handle the admission of exhibits. The parties are agreed in all respects with respect to

how we would enforce your order with one exception. The exception is this: That VirnetX has given us a list last night of 260-some-odd exhibits that they wish to have admitted en masse this morning. And as to those exhibits where -- where there's no objection, we have no objection with one exception.

And that is as to exhibits where there's no intended use with a witness, that is inconsistent, as we understand it, with Your Honor's pretrial order, which said, for example, you can use an exhibit in opening where there's no objection as long as you have a good-faith intent to use it with a witness or that it will be used with a witness.

Our concern is that the proposal advanced by VirnetX would unduly burden the jury and the Court with perhaps hundreds of exhibits that no witness would ever explain or discuss.

And our view of Your Honor's past practice and appropriate practice is that, of course, we could admit exhibits en masse before the jury gets here as to which there is no objection. That's the procedure we followed in i4i, and we certainly agree with that.

But not just dumping into the record hundreds of exhibits that no witness is ever going to discuss, and that's the dispute before Your Honor at

this point.

MR. McLEROY: Yes, Your Honor, there's a long list of unobjected to exhibits, and we're aware of Your Honor's concern about the length of trial. And we don't want to burden the testimony, particularly the testimony of our infringement expert, by having him handle a number of exhibits that we believe we need in the record for appeal that are only going to slow down Your Honor's trial.

THE COURT: Well, what my goal is, is to speed the trial up. If -- I mean, an exhibit can be admitted without a witness referring to it. I mean, if it's otherwise admissible and is -- so my ruling would be that they can preadmit everything that is -- that there's no objection to, and that -- and if there is no objection and it's admissible.

Now, if you want to object to some of them and put them through the paces of proving them up, I mean, that's your right to do so.

MR. POWERS: No, that wasn't our concern. We have no objection -- we have no desire to force them to go through the issue of proving them up. That's not the point. We have no objection to any of these exhibits.

Our concern is that if the record has

literally hundreds of exhibits that no witness has ever discussed, that that is something that is not fair to the jury or Your Honor, because when those exhibits are then used, and, presumably, they're being put into the record to be used either on appeal or in argument to the jury or in argument to Your Honor, the jury and Your Honor don't have the benefit of testimony about what that exhibit means and doesn't mean.

And often, an exhibit will say something and be subject to differing interpretations, and without the benefit of testimony from someone who knows something about that exhibit, then you've got the jury and the Court struggling with what that exhibit means, and I argue that that's not the better procedure.

MR. McLEROY: Your Honor, the expert witness and technical expert witness are summarizing and basing their opinions on these exhibits. And as far as we're concerned, they would all be fair game for cross-examination by their expert.

THE COURT: Well, the -- I'll -- any exhibits that one side wishes to offer or the other side wishes to offer that are not objected to will be offered en masse, regardless of whether they're referred to by a witness or not, so -- unless someone objects on that basis. And I don't interpret your -- your request to be

an objection to that.

MR. POWERS: We -- we do object to the introduction of large masses of exhibits that no witness would ever discuss. We don't object to the individual exhibits.

THE COURT: Well, if you don't object to the individual object -- individual exhibits, then your objection to the manner of admission of the unobjected to exhibits is overruled.

MR. POWERS: Understood. Thank you, Your Honor.

THE COURT: All right. What's next?

MR. CALDWELL: Your Honor, VirnetX has one other issue.

At the pretrial conference, I raised with Your Honor that Microsoft has identified the defense of -- that the scope of the Doctrine of Equivalents that VirnetX intends to apply is limited by legal defenses of disclosure, dedication, and all elements rule. And Your Honor invited us to file a motion.

THE COURT: Right. I have that.
Is that going to be necessary this morning?

MR. CALDWELL: I don't think it is. I just wanted -- I didn't want to --

THE COURT: Right.

MR. CALDWELL: -- speak now or forever hold my peace.

THE COURT: That's not going to be referred to during opening statements?

MR. POWERS: It will not.

THE COURT: Okay. Very well. I'll take that up probably over the noon hour today.

Anything further?

MR. McLEROY: No, Your Honor.

MR. POWERS: Nothing further, Your Honor.

THE COURT: All right. Bring the jury in, please.

COURT SECURITY OFFICER: All rise for the jury.

(Jury in.)

THE COURT: Please be seated.

All right. Good morning, Ladies of the Jury. Hope that you've had a good weekend and restful and ready for a long week of sitting and listening and learning.

So we're going to get started fairly promptly on time this morning. I have some preliminary instructions to give you regarding the law in this case and what you should follow.

I will tell you that while you need to

listen to these -- and you're going to be provided with notepads in a little bit, and you're invited to take notes if you wish -- it's not entirely necessary that you do so, because all of these instructions will be given to you in much greater detail at the end of the case.

But my purpose is to help give you some framework, understanding of the -- of the terminology that's used, of the legal -- the law relating to the various matters that are at trial.

And then after I finish those instructions, the attorneys will give you their opening statements. And that's again where they will present for you at that point the evidence that they believe is going to be presented. And they will fit that within the framework of the law I've given you, and they will present to you what they expect the evidence is going to show you during the course of the trial.

So that's to give -- this is -- my instructions are to give you an overview of the law and the instructions you're to follow. And their opening statements will give you an overview of what they expect the evidence to be. And then after we finish the opening statements, we'll go straight into the evidence, okay?

All right. Well, let me start with the instructions. These will probably take, hopefully, no more than 30, 40 minutes at the most. And I'll have to pause occasionally to wet my whistle, because they are rather lengthy.

All right. Ladies of the Jury: You have now been sworn in as the jury to try this case. As the jury, you will decide the disputed questions of fact. As the Judge, I will decide all questions of law and procedure.

From time to time during the trial and at the end of the trial, I will instruct you on the rules of law that you must follow in making your decision. Very soon, the lawyers for each side will make what is called an opening statement. Opening statements are intended to assist you in understanding the evidence. However, what the lawyers say during their opening statements is not evidence. The only evidence that you will hear and that you will rely upon in making your decision is what you hear from this witness stand over here or by way of deposition or by way of exhibits that are introduced into evidence.

Now, the party who brings the lawsuit is the Plaintiff. In this action, the Plaintiff is VirnetX, Inc., who will be referred to as either the

Plaintiff or VirnetX during this trial.

The party against whom this suit is brought is called the Defendant. In this action, the Defendant is Microsoft Corporation, who will be referred to as Microsoft or the Defendant during these proceedings.

This is a case of alleged patent infringement.

After the opening statements, VirnetX will call witnesses and present evidence. Then Microsoft will have an opportunity to call witnesses and present evidence. Then, after all -- you've heard all of the evidence, I will then instruct you on the applicable law. I'll give you detailed instructions both orally as I'm doing now, and at end of the case, you will have those written instructions to take with you to the jury room.

After I've given you your final instructions, after all the evidence is in, you've heard the final instructions, then you'll hear the closing argument of the attorneys. After you've heard their closing arguments, then and only then will you retire to the jury room to -- for the first time, start to discuss the case, deliberate and reach a verdict.

Now that's a broad overview of what's

going to be happening over the next week.

During this case, I want you to keep an open mind. Do not decide any fact until you've heard all of the evidence, the closing arguments, and my instructions. Pay close attention to the evidence.

If you would like to take notes during the trial, you may do so. The court security officer will now pass out to you notebooks for you to take instructions -- or take notes, if you wish.

Inside the notebook, you should find a blank pad. The first thing that I would encourage you to do is to write your name on the first page of the blank pad.

Open that notebook and see if there's not a stenographer's pad in there. Is there?

Okay. Well, on the first page of that stenographer's pad, when you get it -- or actually on the outside cover, write your name. That will be your notebook for the -- for the course of the trial.

There's some other things in that black notebook that I'll go over with you in a moment, but for now, just get your notepad, get your name written on the front cover, and then you can flip over to the second page, and you're welcome to take notes, if you wish.

Again, all of these instructions will be

repeated to you again later, and they will be provided to you in writing later. But feel free to take any notes you wish.

Let me give you some instructions about notes, if you do decide to take them. If you decide to take notes in this case, be careful that you don't get so involved in your note-taking that you become distracted and miss part of the testimony in the case.

Your notes are to be used only as aids to your memory. And if your memory should later be different from your notes, you should rely on your memory and not on your notes.

Also, don't be unduly influenced by the notes of other jurors. A juror's notes are not entitled to any greater weight than the recollection of each juror concerning the testimony. For example, all because someone has written something down doesn't necessarily mean that they heard it right or that they wrote it down correctly.

So just because it's written down doesn't mean that it's to be given any greater weight than just what your memory would be. But it is there to help you. Even though our court reporter here is making stenographic notes of everything that is said, a typewritten copy of the testimony will not -- I

repeat -- will not be available for your use during deliberations.

On the other hand, any exhibits that are introduced into evidence will be available to you during your deliberations.

Until the trial is over, do not discuss this case with anyone and do not permit anyone to discuss this case in your presence. This includes your family and friends.

Do not discuss the case even with the other jurors, with your fellow jurors, until all of the jurors are in the jury room at the end of the case, and you actually begin deliberating. So as I told you last week, when you go to lunch or take a break, talk about anything you wish, but don't talk about this case.

If anyone should attempt to discuss this case with you or to approach you concerning the case, you should inform me immediately or through my Court staff.

During this trial you should hold yourself completely apart from the people involved in the case: The parties, the witnesses, the attorneys, and the persons associated with them. As you can see, there are a lot of people in the courtroom and a lot of attorneys involved in the case.

You've got a juror badge on, and I'm instructing everyone in the audience and in the courtroom that they should avoid having any conversation with you or any contact with you. Realize when they don't visit with you and when you don't visit with them, neither one of you are being rude to the other.

Just you're a juror; you need to hold yourself apart. Not that you would say anything improper or they would, but not only do we need to be fair, we need to give the appearance of being fair. So be sure that you hold yourself apart.

Also, if you have any type of social-networking internet site or tool, like Facebook, MySpace, or Twitter, you should not discuss or even mention the case at all on any of those sites. So no postings on Twitter, no discussion on Facebook, or on any of those social-networking sites.

Do not post updates about what is going on in the case. Do not send or receive text messages about the case. That would be entirely improper. And if you were to do that, it can result in all of the time and expense that everybody has spent getting the case to this point, and trying the case can be put in jeopardy. So please follow those instructions very, very carefully.

Also, do not make any independent investigation of any fact or matter in this case. Do not learn anything about the case from any outside source. Do not watch TV or read the newspaper, if there's anything in it about this case. Do not use the internet or Google to try to find out more information about the case, the parties, or the attorneys in this case.

For example, if you have a computer at home during this case, don't go home and get on your home computer and start trying to figure things out or Google stuff. And the reason for that, again, is very, very important.

You are to be guided only by the evidence that you hear -- hear in this courtroom, and any type of independent investigation would be extremely improper and, again, could put these proceedings in jeopardy. So go only by what you see and hear in the courtroom and nothing else. Make no independent investigation.

During the trial, it may be necessary for me to confer with the lawyers out of your hearing or to conduct a part of the trial out of your presence. I will handle these matters as briefly and as conveniently for you as I can, but you should remember that they are a necessary part of the trial.

And if you have to wait in the jury room -- and, again, I'm going to try to keep that to a real minimum. I'm going to try to deal with anything I need to take up with the attorneys during a break or during the noon hour or after hours or before hours, because I want your time to be spent this week here in the jury box hearing evidence.

But those occasions will come up where you're going to be in the jury room, and you're going to be wondering, well, why are we sitting in here? What's going on? Just realize that's part of the case. Again, we will try to hold it to a minimum.

Now, let me visit with you about the parties and the nature of this case. As I said, this is a patent case. This case involves two patents identified by their numbers as follows, and this may be where you want to start making some notes, if you wish.

The first one is Patent No. 6,502,135, and for simplicity, that's just going to be referred to as the '135 patent. So if I were making notes, I might say, okay, this case involves the '135 patent, and then it also involves the '180 patent. That's Patent No. 7,188,180. Again, it's referred to by the last three digits of the patent number.

So the case involves two patents: The

'135 and the '180.

These patents -- these two patents may be referred to from time to time as the patents-in-suit. That means they're the patents that are involved in this lawsuit. These patents generally relate to virtual private networks, and you'll hear a lot more about what a virtual private network is, also sometimes referred to as VPN.

You heard some during voir dire examination, but you're going to hear a lot more during the opening statements of the attorneys and during the evidence in the case.

All right. In this case, VirnetX, the Plaintiff, contends that Microsoft, the Defendant, is infringing the patents-in-suit, those two patents, the '180 and the '135 patent.

And they contend that they are infringing by making, using, selling, offering for sell, or importing Microsoft's accused software products and by causing others to infringe.

VirnetX also contends that Microsoft's infringement is willful.

Finally, part -- finally, VirnetX contends that it is entitled to damages as a result of Microsoft's infringement.

Microsoft, on the other hand, denies that it is infringing, willfully or otherwise, and contends that the patents-in-suit are invalid as being either anticipated by or obvious in light of what is called prior art.

Microsoft further contends that the asserted claims of the '135 patent are invalid, because the '135 patent specification does not satisfy the statutory requirements of setting forth an adequate written description or disclosing the inventor's best mode.

Now, that may all sound like Greek to you right now. It's a lot of new words thrown at you. I'm going to define a lot of those words for you as I go through the instructions. The attorneys are going to discuss them in their opening statements. The witnesses are going to help you understand those -- those words. So don't feel overwhelmed at this stage. You're going to get a lot of -- lot of education this week and lot of help from the attorneys and from the witnesses for both sides.

So let me go back and discuss with you the patent system, generally, the U.S. patent system. You saw some of that on the video that you saw on the first day when you came here. I'm going to go back over

some of that with you.

Patents are issued by the United States Patent & Trademark Office, which is part of the United States government. The United States government is empowered by the United States Constitution to enact patent laws and issue patents to protect inventions. Inventions that are protected by patents may be of products, compositions, or of methods for doing things and for using or making a product or composition.

The purpose of the patent system is to help advance science and technology. The patent system achieves this purpose by granting to the owner of a patent the right, for the life of the patent, to exclude any other person from making, using, offering for sale, or selling anywhere in the United States the invention covered by the patent.

A patent has a life for a limited amount of time, which for the patent involved in this case has not yet ended. Once a patent expires, the patent owner may no longer exclude anyone from making use of the invention claimed in the patent.

The invention then becomes part of the public domain, which means that anyone is free to use it; that is, after the term of the patent has expired. But during the term of the patent, if another person,

without the patent owner's permission, makes, uses, sells, or offers to sell something that is covered by the claims of the patent, then that person is said to have infringed the patent.

The patent owner may enforce a patent against other persons or companies believed to be infringers in a lawsuit in federal court as in this case.

To be entitled to patent protection, an invention must be new, useful, and non-obvious. As I noted, a patent gives its owner the right to exclude other people from making, using, selling, or offering for sale what is covered by the claims of the patent.

Everyone, however, has the right to use existing knowledge and principles. A patent cannot remove from the public the ability of what was known or obvious before the invention was made or patent protection sought.

The granting of a patent by the United States Patent & Trademark Office, however, carries with it the presumption that the patent is valid. From the issuance of a patent, it is presumed that its subject matter is new, useful, and constitutes an advance that was not, at the time of the invention was made, obvious to one of ordinary skill in the art.

However, that presumption may be rebutted by -- at trial, and you, the finder of fact, may find the patent to be invalid.

Now, let's talk about the various parts of a patent.

A patent includes two basic parts: A written description of the invention and the patent claims.

The written description may include drawings, is often referred to as the specification of the patent.

Now, if you will look in the notebook, you will find a copy of the '180 patent. If you would, open your notebook and see if you can locate that. Everybody have it?

It should have a tab on it. And then you'll see a page, in the upper left-hand corner, it says United States patent. And then on the right-hand side it says Patent No. U.S. 7,188,180B2. That's the '180 patent.

That first page is the cover page of the '180 patent, and it provides identifying information, including the date the patent issued.

You see that in the upper right-hand corner -- well, it shows the date of the patent, March

6th, 2007. The patent number, along the top, as well at the inventors' names, the filing date.

You'll notice over on the left-hand column about halfway down, it says filed November 7th, 2003. That's the filing date.

The assignee up -- you'll see a little higher up on that left-hand column, there's a No. 73 out beside it. It says assignee, VirnetX, Inc. That's who the patent was assigned to, which is the Plaintiff in this case.

You will also see a list of what's called prior art publications considered in the Patent Office when deciding to issue the patent.

Now, the specification of the '180 patent begins with an abstract found on the cover page. That's in the lower right-hand corner of the patent on the front page.

The abstract is a brief statement about the subject matter of the patent. You'll see it starts with the first sentence: A technique is disclosed for establishing a secure communication link between a first computer and a second computer over a computer network. And then it goes on to give a summary or an abstract of what the inventor is claiming the invention is.

Next are drawings, which you will see

are -- appear beginning on Page 3. You will see Figure 1. And that continues for the next 37 pages -- or it's Figures 1 through 37 on the next 40 pages.

I'm not going to ask you to look at all of those, but if you will, flip all the way over to Figure 40, which -- or Figure 37, which is on Page 43 -- or Page -- Sheet 40 of 40 of the patent.

All right. If you've found Figure 37, turn one more page, and that is the beginning of the written description.

Now, the drawings, Figures 1 through 37, those depict various aspects or features of the invention. The drawings are described in words later in the patent description. Beginning on that page after the drawings, that is where the written description of the invention begins.

In this portion of the patent, each page is divided into two columns, which are numbered at the top.

Is everyone looking at the page that has a 1 over the first column and a 2 over the second column? Everybody have that page?

It's the first page following the drawings.

So you'll see that's Column 1 and 2. And

then you'll see down the middle of the page are some little numbers. There's a 5, a 10, a 15, a 20.

You follow those? Everybody see those?

Those are the line numbers. So what this allows you to do is, if someone wants to refer you to a particular part of the patent, they may refer you to Column 1, Line -- let me see what would be a good example -- let's say Line 25.

So if you look in Column 1 and then you look down in the middle little numbers down to 25, you would be at Column 1, Line 25. And that's where the section entitled, Background of the Invention, lies. And, likewise, you could refer to any column number or any line and follow right in the patent to where it goes.

Now, this written description includes a background section, which is on Column 1, Line 25. And then if you'll flip the page over to the next page on Column 3, Line 9, that begins the summary of the invention. And that goes on for several pages over to Column 8.

And on Column 8, there's a brief description of the drawings where it discusses what each one of the drawings say. Then over on Column 9 begins a detailed description of the invention down on Column 9,

Line 46.

Is everybody up with me?

Okay. We're making patent experts out of y'all real fast here.

In the -- through the detailed description of the invention, it goes through a very detailed description for many pages, and it includes some specific examples within that detailed description.

Now, that description goes on until -- near the end of the written description is what we call the claims of the patent. And if you'll flip all the way over to -- it's near the end, beginning on Column 56. So turn all the way over to Column 56 in the patent.

Everybody have Column 56?

Okay. Look down Column 56 to Line 48, and you'll see what it says is, What is Claimed is, colon, and then 1. And 1 begins a method for accessing a secure computer network address comprising steps of, and then it lists several steps.

And then you'll see a No. 2. And then on the next page, you'll see on over 3, 4, 5. And it goes on all the way to Column 60, Line 34 where it ends. And as you'll see, there are 41 claims over on Column 60 at the end of the patent. There are 41 claims.

Now, all of those claims are not being asserted, just certain ones, and that will be discussed with you in greater detail later. But for now, let's go back to Column 56, Claim 1, which is one of the asserted claims. And I'm going to give you some specific instructions about what a claim means.

The claims of a patent are the main focus of a patent case, because the claims are what define the patent owner's rights under the law. That is, the claims define what the patent owner may exclude other -- others from doing during the term of the patent.

The claims of a patent serve two purposes. First, they set the boundaries of the invention covered by the patent.

Second, they provide notice to the public of what those boundaries are. Thus, when a product or a method is accused of infringing a patent, the patent claims are compared to the accused product or method to determine whether there is infringement.

The claims of the patent are what are infringed when patent infringement occurs, because the claims define what the patent is.

The claims are also at issue when the validity of a patent is challenged. In reaching your determination with respect to infringement and validity,

you must consider each claim separately.

In your notebook, you are provided with this Court's construction of the meaning of certain terms in the asserted claims in this patent. You must use these meanings that I give to you when you decide the issues of infringement and invalidity.

If you'll turn over -- I think it's the next tab in your notebook. You should see a listing of terms that the Court has construed previously.

Everybody find that?

You don't need to be too concerned with it right now other than to just know it's there. There are certain words within these claims. For example, within Claim 1, there are certain words that at a pretrial proceeding, the attorneys had different arguments over what a particular word meant. And they asked me to construe it, and I have done that, and I've provided you with those definitions.

So it's kind of like if you're reading a book and there's a particular word there that maybe you don't quite understand, you would go to a dictionary to look it up. Well, you would go to my claim construction to look up the meaning of those words, and you'll be guided by those meanings.

Now, the attorneys will do a good job of

explaining all of that when they get into the evidence, but you just need to know for now that those constructions are there and that they relate to these claim terms.

So let's look at Claim 1. It goes through several steps there. I don't think I'll read the whole thing at this time -- well, let's read through it. It might be helpful to you.

Claim 1, Column 56 said -- says: A method for accessing a secure computer network address comprising steps of, receiving to secure domain name, sending a query message to a secure domain name service. The query message requesting from the secure domain service a secure computer network address corresponding to the secure domain name.

Then receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name and sending an access request message to the secure computer network address using a virtual private network communication link.

So those are the steps of the claim. Now you may not understand what all of those mean at this point, but, again, that will be explained to you during the course of opening statements and during the evidence

that you hear in the case.

But for now, just realize there's Claim 1; it's one of the asserted claims; and it comprises those various steps that I've mentioned to you or I just read to you.

Now, let me visit with you about how a patent such as this is obtained. We've gone over the patent, the various parts of it. Let's talk about how someone obtains a patent.

The United States Patent & Trademark Office is the agency of our government that examines patent applications and issues patents just like this one.

When an applicant for a patent files a patent application with the Patent & Trademark Office, the application is assigned to a Patent Examiner. And you'll remember that from the video you saw the first day.

The Patent Examiner in the Patent & Trademark Office then examines that patent application to determine whether the invention described in the patent application meets the requirements of the patent laws for a patentable invention.

In examining a patent application, the Patent Examiner makes a search in the Patent Office

records for prior art -- and you'll hear that referred to a lot -- for prior art pertinent to the claims of the patent application.

The Patent Office records may or may not contain all of the prior art pertinent to the claims of the patent application.

The prior art is defined by statute, and I will give specific instructions after the close of the evidence as to what constitutes prior art.

But, generally speaking, prior art is technical information and knowledge that was known to the public either before the invention by the applicant or more than a year before the effective date of the application.

The Patent Examiner advises the applicant of his or her findings in a communication called an office action. The Examiner may reject the claims, if he or she believes they do not meet the requirements for patentable inventions.

The applicant may respond to the rejection with arguments to support the claims and may sometimes make changes or amend the claims or submit new claims.

If the Examiner concludes that the legal requirements for a patent have been satisfied, he or she

allows the claims, and the application issues as a patent.

The process from the filing of the patent application to the issuance of the patent is called patent prosecution. And that's what I've just described to you that goes on between the applicant and the Patent Office.

The record of papers relating to that patent prosecution is referred to as the -- as the prosecution history for that patent, or the file history. In other words, it's documents that relate to what transpired between the applicant and the Patent & Trademark Office.

So that generally is how the patent process works.

Now, let me turn to the issues that you are going to be deciding as the jury in this case. I'm now going to give you some information about those issues that are going to be presented to you at the trial as well as a short overview of the applicable law relating to those.

At the close of the trial, you will be given much more specific instructions that you must follow in reaching your verdict. You will also be given a verdict form and questions that you must answer in

providing your verdict. That will all transpire at the end of the case.

But now let me instruct you on the various instructions that you will follow in deciding the case.

First, I want to visit with you about the burdens of proof.

In any legal action, facts must be proved by a required standard of evidence known as the burden of proof. You may have heard about this in a criminal case, proof beyond a reasonable doubt; or in a civil case, it's proof beyond -- or proof by a preponderance of the evidence.

In a case such as this, there are two different burdens of proof that are used. The first is what's called the preponderance of the evidence standard; and the second is called the clear and convincing evidence standard.

The standard beyond a reasonable doubt that's used in criminal cases, that doesn't apply in a civil case like this. We have two standards: Preponderance of the evidence and clear and convincing evidence.

In this case, VirnetX must prove its claim of patent infringement by a preponderance of the

evidence. When a party has the burden of proof by a preponderance of the evidence, it means that you must be persuaded that what the party seeks to prove is more probably true than not true.

To put it another way, if you were to put the evidence for and against the party who must prove the fact on the opposite sides of a scale, a preponderance of the evidence requires that the scale tip at least somewhat toward the party who has the burden of proof. That's the preponderance of the evidence standard.

Microsoft has the burden of proving its defense of invalidity by a heavier burden called the clear and convincing evidence standard.

When a party has to prove something by clear and convincing evidence, it means that the evidence must produce, in your minds, a firm belief or conviction as to the matter sought to be established. In other words, if you were to put the evidence for and against the party who must prove the fact on the opposite sides of a scale, the clear and convincing evidence standard requires that the scale tip more heavily toward the party who has the burden of proof.

Again, you may have heard of a burden of proof used in criminal cases called beyond a reasonable

doubt. That burden is the highest burden of proof and is used only in criminal cases. It does not apply to this case. You should, therefore, put that standard, beyond a reasonable doubt, out of your mind for purposes of this case.

Now let me visit with you about infringement.

As I told you, VirnetX contends that Microsoft infringes Claims 1, 10, and 12 of the '180 patent, and Claims 1, 4, 15, 17, 20, 31, 33, and 35 of the '180 patent by making, using, offering for sale, selling, and importing into the United States certain accused products and using certain accused methods. This is called direct infringement.

VirnetX also contends that Microsoft infringes indirectly by inducing or contributing to the direct infringement of others.

I will first tell you about direct infringement, and then I will tell you about indirect infringement.

First, direct infringement. VirnetX seeks to prove direct infringement of the '180 patent by literal infringement. To prove literal infringement of a particular claim, VirnetX must prove by a preponderance of the evidence that the accused products

or accused manner of use of the accused products contains each and every limitation of that particular claim.

VirnetX also seeks to prove direct infringement of both patents through the Doctrine of Equivalents. The Doctrine of Equivalents provides that patent protection is not limited to a claim's literal terms but also embraces its equivalents.

To prove infringement under the Doctrine of Equivalents, VirnetX must prove by a preponderance of the evidence that for each claim limitation not literally met, the limitation is met equivalently in the accused manner of use.

I will tell you much more about what is meant by equivalence at the end of the case, but just realize that those are the two ways of infringement: Direct infringement and Doctrine of Equivalents.

Now with regard to indirect infringement. VirnetX also alleges that Microsoft has indirectly infringed the asserted claims by inducing and/or contributing to another's direct infringement.

To prove that Microsoft induced someone else to infringe, VirnetX must prove by a preponderance of the evidence that Microsoft encouraged or instructed another person to make or use the patented apparatuses

or use the patented methods in a manner that infringes, and that Microsoft knew of the patent and knew or should have known that the encouragement or instructions would result in the other person doing that which you find to be an infringement.

To prove that Microsoft contributed to another's direct infringement, VirnetX must prove by a preponderance of the evidence that Microsoft sold or supplied to another person a component that is a material part of the patented invention and is not suitable for other substantial non-infringing uses. VirnetX must also prove that the other person directly infringed the patent claims and that Microsoft knew that the component was especially made for use in an infringing manner.

Microsoft denies that it has either directly or indirectly infringed any of the claims of the patents-in-suit.

Now, with regard to willful infringement. VirnetX also claims that Microsoft willfully infringed the patent claims. To prove willful infringement, VirnetX must prove that Microsoft acted despite an objectively high likelihood that its actions constituted infringement of a valid patent and that Microsoft either knew or should have known of that risk.

VirnetX's willful infringement claim requires a higher burden of proof, the clear and convincing standard, than VirnetX's other claims, which require proof by a preponderance of the evidence.

I will explain in more detail at the end of the case how you decide whether infringement is willful.

Now with regard to invalidity.

Microsoft contends that the asserted claims of the patents-in-suit are invalid. Invalidity is a defense to a patent infringement. A person accused of infringement has the right to assert that the claimed invention in a patent did not meet the requirements of patentability and, therefore, that the patent claim is invalid.

However, the granting of a patent by the Patent & Trademark Office carries with it the presumption that the patent is valid. The presumption of patent validity imposes the burden on Microsoft to prove invalidity by the clear and convincing evidence standard.

I will now explain to you briefly the legal requirements for each of the grounds on which Microsoft relies in its contention that the asserted claims of the patents are invalid.

I will provide more details for each ground in my final instructions to you at the end of the case.

First is the defense of anticipation. Microsoft contends that the inventions covered by the asserted claims of the patents-in-suit are not new. An invention is not new -- an invention that is not new is said to have been anticipated by the prior art.

To prove that a claim is anticipated by the prior art, Microsoft must prove by clear and convincing evidence that each and every limitation of the claim was present in a single item of prior art.

Next is obviousness.

Microsoft also contends that a number of asserted claims of the patents-in-suit are invalid for obviousness.

To prove invalidity of a patent based on obviousness, Microsoft must prove by clear and convincing evidence that the invention defined by the claim would have been obvious to a hypothetical person of ordinary skill in the art at the time the invention was made.

It will be up to you to decide the level of ordinary skill in the art of the '135 and the '180 patents based on all the evidence introduced at trial,

including the level of education and experience of persons working in the field, the type of problems encountered in the field, and the sophistication of the technology.

So we've discussed two ways that a patent can be found invalid: Anticipation and/or obviousness.

Next is written description.

Microsoft also contends that the asserted claims of the '135 patent are invalid, because the description of the invention in the specification does not meet certain requirements.

A patent claim is invalid, if the specification of the patent does not contain an adequate written description of the claimed invention. That is referred to as the written description requirement.

To succeed, Microsoft must show by clear and convincing evidence that the specification fails to meet the law's requirements for a description of the written invention.

I will describe in more detail at the end of the case how you decide the issue of written description.

Next is what's called best mode.

Microsoft also contends that the asserted claims of the patent are invalid, because the patent

does not contain a description of the best way to make, use, and carry out the claimed invention. This is referred to as the best mode requirement.

In order to prove that the asserted claims of the patents-in-suit are invalid for failure to disclose the best mode of the invention, Microsoft must prove by clear and convincing evidence that, first, at the time the application was filed, the inventor knew of a best mode of performing the claimed invention; and, second, that the patents-in-suit do not disclose that best mode.

I will describe in mere detail at the end of the case how you decide the issue of best mode.

Now, that concludes the instructions regarding infringement and the instructions regarding invalidity.

Now, let me give you some instructions regarding damages.

VirnetX claims that as a result of Microsoft's infringement, it is entitled to damages in the form of a reasonable royalty on each of Microsoft's accused products.

Damages cannot be speculative. VirnetX must prove the damages it has suffered as a result of Microsoft's alleged infringement by a preponderance of

the evidence.

The fact that I am instructing you about damages now does not mean that VirnetX is or is not entitled to recover damages. I will explain to you further at the end of the trial how a reasonable royalty is determined.

And at the end of the trial, you will get a written charge that will have all of these instructions in it in much more detail than I am giving them to you now. And you will also have a verdict form that will ask you some very simple questions dealing with the issues of infringement, invalidity, and damages.

So that's what you're going to be deciding in this case, is infringement, invalidity, and damages.

Now, let me visit with you about the claims of the patent again, more specifically construction of the claims.

I will instruct you now and at the end of the case about the meaning of some of the claim language. You must use these meanings I give you when you decide the issues of infringement and invalidity.

In deciding whether or not an accused product infringes the patent, the first step is to

understand the meaning of the words used in the patent claims. It is my job as Judge to determine what the patent claims mean and to instruct you about that meaning.

You must accept the meanings I give you and use them when you decide whether or not a patent claim is infringed and whether or not a patent is invalid.

It may be helpful to refer back to the patents in the notebook as I discuss the claims at issue here. The claims are at the end of each patent.

In the '135 patent, the claims start with Column 47, Line 20. And in the '180 patent, the claims start with Column 56, Line 48.

The patent claims may exist in two forms referred to as independent claims and dependent claims. An independent claim does not refer to any other claim of the patent. It is not necessary to look at any other claim to determine what an independent claim covers.

For example, Claim 1 of the '180 patent is an independent claim.

And, if you will, turn to Claim 1 of the '180 patent. So find the '180 patent and turn over to Column No. 56. And you'll see down at Column 56, Line 48, it says, What is claimed is Claim 1, a method

for accessing a secure computer address comprising steps of, and then it gives the steps.

That's what's called an independent claim. It's not dependent on any other claim.

But a dependent claim is one that refers to at least one other claim in the patent. A dependent claim includes each of the limitations of the other claim or claims to which it refers as well as the additional limitations recited in the dependent claim.

Therefore, to determine what a dependent claim covers, it is necessary to look at both the dependent claim and the other claim or claims to which it refers.

For example, Claim 4 of the '180 patent -- if you'll turn over to the next page, Column 57, Line 7, you'll see the No. 4. That's Claim 4.

And Claim 4 says: The method, according to Claim 1. So right there, it's incorporated in Claim 1 and all of its elements into this, but then it has the additional element. It says: The method according to Claim 1 wherein the response message contains provision -- provisioning information for the virtual private network.

So Claim 4 is what we call a dependent

claim.

The claims of the patents-in-suit use the word -- use the words comprises and comprising. For example, back to Claim 1, you see at the beginning of Claim 1, it says a method for accessing a secure computer network address comprising steps of.

Now, a claim that uses the words comprising or comprises means including or containing. A claim that uses the word comprising or comprises is not limited to products or methods having only the elements that are recited in the claim, but also covers products or methods that add additional elements.

Take, for example, a claim that covers a table. If the claim recites a table comprising a table top, legs, and glue, the claim will cover any table that contains these structures -- structures, even if the table also contains other structures, such as a leaf or wheels on the legs. That's a very simple example of what using the word comprising means. In other words, it can have other features in addition to those that are covered by the patent.

I have now instructed you as to the types of claims at issue in this case. I am next going to define the meaning of words used in the patent claims at issue -- issues. You must use the definitions I provide

to you when you decide infringement and invalidity. If you'll now take a look at the chart at the back of your book, you will see the various instructions that I have given to you. There's not very many of them; it's all on one page.

You will see, for example, up at the top under the '135 network -- or '135 patent, virtual private network, or VPN.

Does everybody have that?

It should be the last tab in your notebook. It has a sheet that looks like this (indicates).

A JUROR: First page?

THE COURT: First page of your notebook. Okay. Sorry about that. First page OF your notebook. I don't believe it has a title on the page, but it has '135 patent and '180 patent in the middle.

Everybody have it?

Okay. You'll see at the first one, virtual private network. The Court has -- the parties came to me and said we need you to define what this means, and they presented various arguments. And this is the construction that I determined, and it's the construction that you will follow in trying this case.

A virtual private network, or VPN, is a

network of computers which privately communicate with communication paths between the computers.

So that's an example of a definition. I'm not going to go through all of these now. They're there for your reference, and you can -- you'll hear about them during the case, but you'll see the various words that have been defined and construed by the Court with regard to the claims.

All of this will become clear to you as the trial progresses, but this is a good starting place for you to help you understand some of the basic elements of a patent and some of the basic language and nomenclature.

Again, if you're feeling a little overwhelmed at this point, rest assured there's going to be lots of explanation and lots of time to digest. This is the first time you've heard a lot of these words, a lot of these concepts. You're going to be hearing a lot more about them during the opening statements, during the evidence.

We'll have experts from both sides that are going to help you understand this case. And at the end, you'll hear closing arguments. You'll have my Court instructions, and you'll -- you'll be well-equipped to decide this case by the time you get to

the end of it.

Now, finally, let me just discuss with you your duties as jurors.

You have two duties as jurors. Your first duty is to decide the facts from the evidence in the case. That is your job and yours alone.

Your second duty is to apply the law that I give you to the facts. You must follow these instructions, even if you disagree with them. Each of the instructions is important, and you must follow all of them.

You must perform your duties fairly and impartially.

Do not allow sympathy, prejudice, fear, or public opinion to influence you. Nothing I say now and nothing I say or do during the trial is meant to indicate any opinion on my part about what the facts are or about what your verdict should be.

You are the sole judges of the facts, and that is your job alone.

That concludes my opening instructions to you. It took just a little bit over an hour. We're going to hear opening statements by both sides in a moment.

I believe I've given y'all how long?

MR. CAWLEY: 45 minutes, Your Honor.

THE COURT: All right. Each side is going to have 45 minutes for opening statements. So before we begin, I think we'll take our morning break at this time, give you a chance to have a cup of coffee. We should have some refreshments in there for you. Use the restroom.

When we come back, you'll hear opening statements from both sides. That should take about an hour and a half. So if you'll be back here at 10:30, which is 20 minutes from now, we'll begin opening statements.

We should be through by noon. Then we'll let you go to lunch, and then we'll come back and start the evidence after lunch.

So be in recess until 10:30.

COURT SECURITY OFFICER: All rise.

THE COURT: Please remember my instructions. Don't discuss the case during your break.

(Recess.)

COURT SECURITY OFFICER: All rise.

(Jury in.)

THE COURT: Please be seated.

All right. Ladies of the Jury, we will now hear opening statements, first by counsel for the

Plaintiff.

MR. CAWLEY: Thank you, Your Honor. Ladies of the Jury, every lawsuit is a story, and this one is no exception.

The case that you'll hear this week is a story about a small team of people who invented a way to make it easy to communicate safely over the internet.

Now, people who actually use computers themselves certainly would be helped by that invention. But as you'll hear this week, the use of computers has become so widespread in our world today, that all of us, whether we actually put our hands on a computer or not, are helped by keeping communications over the internet safe and protected.

I'd like to introduce you, again, to the man who led that small team of people.

Would you stand up, please, Mr. Munger?

This is Mr. Edmund Colby Munger. He goes by the name of Gif, and since he led that team of inventors, I want to tell you a little bit about his story that you'll hear during this trial.

You'll hear that Mr. Munger -- if we could dim the lights a little bit -- chose and had an opportunity to attend the United States Naval Academy where he graduated in 1967. He was immediately assigned

to duty on a ship off the coast of Vietnam during the Vietnam War.

You'll hear that Mr. Munger became the commander of his own ship at the age of only 28 years old; that he spent the next 20 years -- actually, a total of 20 years as an officer in the United States Navy.

Now, the reason that that's important for this case and the story that you'll hear in this case is that if you don't know already, you'll learn a little bit about the fact that the United States Navy is heavily dependent on technology: Radar, computers, and things of that nature; and that Mr. Munger, while he was in the Navy, was typically responsible for high-tech matters relating to the ships that he served on.

After he retired from the Navy in his early 40s, Mr. Munger joined an unusual company that you'll hear a little bit about in this case. It's called Science Applications International Corporation. Now you may never have heard of that company. It's not well-known.

It's unusual, because it's a company that was founded by a nuclear scientist, and his idea for a business was to use private enterprise to provide scientific solutions for problems that the military and

other branches of the United States government might have.

You'll hear that Mr. Munger was excited to join this company, because he had a lot of respect for the scientists in this company, which is usually called SAIC, that he had worked for or worked with when he was still an officer in the United States Navy.

One of the first projects that Mr. Munger worked on at SAIC actually formed a pathway that would eventually lead to the invention in this case.

You may remember that during the first Iraq war -- that's the war that President -- the first President Bush invaded Iraq -- that during the first Iraq war, we heard a lot of news accounts about something called scud missiles. You may remember that.

Scud missiles were missiles mounted on trucks that the Iraqi army had, that they could put in hiding, under a bridge or elsewhere, then bring out and fire off with no more than a few minutes' notice.

You'll hear that the American military did not have an effective way to defend against scuds, and they turned to SAIC and to Mr. Munger to try and find a solution to that problem.

What they came up with was a system that came to be known as the Global Hawk. The Global Hawk is

an unmanned aircraft that flies very high above the Earth for long periods of time. It had the ability to sense or to see the scud missile launcher on the ground and to communicate actual pictures of that to a satellite orbiting over the Earth.

That satellite then had the ability to send those same pictures to a soldier on the ground who would see pictures of the scud, understand where it is, and communicate that information to either aircraft or troops that could attack the scud -- scud missile before it had an opportunity to launch.

You'll hear, though, that there was something very unusual about this project. Because time was short, the system had to use a satellite that was a public satellite. It wasn't owned by the military. It was a satellite that any company can rent time on to transmit television pictures or other things.

And that presented a grave problem of securing it, because it was possible that someone on the ground -- we'll call them a hacker -- could intercept the communication from the satellite back to the ground, and understand what the military was about to do.

Therefore, you will hear Mr. Munger explain that an important part of this Global Hawk program, which he headed, was to secure or find a way to

lock up those communications so that a hacker, if they attempted to intercept them, would be locked out and couldn't see the data that was being transmitted from the satellite.

This experience in Global Hawk caused Mr. Munger -- you will hear him testify -- to begin thinking about the future of military needs and the future of the need for communication security.

You will hear that he wrote a paper, which was read in Washington, D.C., called the Aladdin Paper, and the reason he named it Aladdin was he saw a future in which by rubbing something like a magic lamp, the military and other security agencies would be able to call out all kinds of resources, like satellite communication, like cell phone communication, and like communication over the internet.

Mr. Munger's thinking about this issue, and to some extent the Aladdin Paper that was read by people in the military and security agencies, caused a contract to come about between Mr. Munger's company that he worked for, SAIC, and an unusual company called N-Q-Tel.

N-Q-Tel was founded by Congress. It was a company set up by Congress. And its purpose was rather than to spend lots of money inside the government

developing solutions for the Central Intelligence Agency, that N-Q-Tel would invest relatively small amounts of money with private enterprise so they could come up with better solutions for the things the CIA needed.

In return for this, the company would get to keep any inventions that they made along the way. And, of course, the CIA would be able to use those inventions for whatever purpose they needed.

There was a particular need that the CIA had that related to this contract between N-Q-Tel and SAIC. And it was that CIA agents, I guess people like spies, but others, might be anywhere in the world and needed to be able to communicate securely back to the CIA. They needed to be able to use the internet to do that.

But as you'll learn in this case, the internet is not secure. Therefore, that wouldn't be good enough for the CIA.

And the CIA asked Mr. Munger and this company, SAIC, to come up with a solution of how they could communicate securely over the internet.

Mr. Munger worked with several other scientists who were on this team and who are also inventors on the patents. One of them is Dr. Bob Short.

Dr. Short, if you would stand up, please.

Dr. Short is also an inventor, along with his co-worker, Mr. Munger. They still work together to this very day. And you will hear him testify in this case.

Thank you, Dr. Short.

You will hear him testify how, when SAIC undertook this job for N-Q-Tel and the CIA, he and his team went out and researched different ways that already existed to make communications secure on the internet, because there were some ways that people were already doing it.

He and his team of experts were already aware of them, but they did a lot of research and bought a lot of projects -- products to see what was available at that time to see if it would be suitable for what the CIA needed.

One that was the most interesting and the one that you'll be hearing about in this case -- in fact, Judge Davis warned you that we'd be talking a lot about this, and now we're about to -- is called a virtual private network.

Now because you'll be hearing a lot about virtual private networks in this case, I'd like to interrupt the story of Mr. Munger and his team of

inventors working for the CIA for just a minute, so we can spend just a few minutes talking about what this thing called a virtual private network is and what it does.

First of all, as you probably already know this, rather than say the mouthful of virtual private network every time, it's frequently abbreviated, VPN. So if you see references or hear references in this to a VPN, you know we're talking about a virtual private network.

Now, we'll certainly attempt to keep abbreviations like this to a minimum, because I know it gets confusing very fast. But VPN is one that you're bound to hear.

To understand what this VPN, or virtual private network, is, let's talk first about a network. Now that's a word that we use occasionally. It sounds like a net, like a hair net or a fishing net.

Frequently, we talk about a network of co-workers, a network of friends, which, in that context, means many communications among people. But here, of course, we're talking about computers and computer networks.

If you have a number of computers, they can be connected either with wires or with radio

communication or in other ways. And the software on one computer can share information with software on another computer that it's connected to. That's a network.

The information could be words, like in an e-mail. The information could be a picture that's sent from one computer to another. The information can be a lot of different things. But the function of the computer network is to allow computers to share information.

We have huge computer networks in the world now. This just shows the United States, and it's very much an under-exaggeration of how many computers are on the network in the United States that's known as the internet. All the internet is, is a vast network of computers both in the United States and around the globe that are all linked together.

Because they are linked together in this example, someone from Company A who wants to send data or information to Company B can set up a link or a communication over the network. And one of the beauties of the network is that if for some reason that particular path doesn't work, then they can choose this one, a different path, or many other different paths depending on what's available and what's the most efficient.

So that's what the network word in a virtual private network is.

Private refers to a network that somebody owns and controls all of. They own the computers; they own the wires.

If you work in a small business and your business has a network and it owns the computers and it owns the wires that connect them, it's a private network. Nobody out in the public is allowed to use it. A virtual private network -- virtual is a word that we've been hearing a lot in the last few years, and I'm sure you recognize that in this context what it usually means is it's not real; it's not a real, concrete thing that you can touch, but it's something that behaves as if it were real.

So a virtual private network is a computer network that's not really private. It goes over publicly available stuff like the internet, but it behaves as though it is private.

Now, how would that work?

Here we see Company A again, and this time a remote user -- maybe that's an employee of Company A, who's traveling. Looks like he's in Florida or thereabouts, and he wants to communicate securely back to Company A.

His computer can set up this connection over the internet. And by using certain techniques that I will tell you a little bit more about in a minute, those connections can be secured.

Looks familiar. Looks a lot like the Global Hawk problem and the security between the satellite and the ground. But here it's the path along the internet that's being secured.

And once it's secured, a hacker, who attempts to intercept the information, is locked out. They can't see anything useful.

This is an example of a virtual private network. It's not actually private, because the remote user in Company A don't own the internet that they're talking over. But we call it a virtual private network, because it behaves as if it were private, and it is as secure as if someone actually owned all the computers and all the wires.

This kind of technology existed at the time when Dr. Bob Short and Gif Munger and their team of inventors was trying to find a way to help the CIA communicate securely over the internet.

But virtual private networks that you've seen here had a major drawback that made them unacceptable for what the CIA needed and unacceptable

for almost all people who needed to communicate securely over the internet.

Here's an article from a publication called Network World from 1998, about the time that Dr. Short and Gif Munger were working on this problem. And it says that remote access, which is what we're talking here, is a nightmare for support desks.

Staffers never know what combination of CPU modem, operating system, and software configuration they're going to have to support. Adding VPN software makes it worse.

Let me show you a document that you'll hear about in the case. This is Plaintiff's Exhibit 983.

This is basically an instruction manual for some Microsoft software that was available in the year 2000 that could be used to set up a virtual private network. Let me give you just a sense of what you had to do to set up that virtual private network.

First of all, you had to create something called an IPSEC policy, and there were seven -- excuse me -- five steps you had to go through described in the document to do that. But then you had to build a filter list from Net A to Net B, and there were nine steps you had to go through to do that.

Then you had to build a filter list from Net A -- Net B to Net A, and there were seven steps you had to do to do that.

Then you had to configure a rule for Net A to a Net B tunnel. There were ten steps that you had to follow to do that.

Then you had to configure a rule for Net B to Net A. That was seven more steps to do that. That process was so complicated that even experts who were setting this up were encouraged to print out a long list of descriptions of what they had done and get on the phone to try and figure out why their virtual private network wouldn't work.

You will hear from Dr. Short and others that the virtual private network software and hardware that was available in the late '90s was too complicated, too cumbersome, and took too long for most people to actually use.

You'll also hear that people who worked in the security field know that if security is too complicated for people to use, they just won't use it.

If you have a burglar alarm system and the keypad is so complicated that you can't really figure it out, then you're going to leave the house without setting it. That's the way -- that's the way we

all are.

And the people working on this knew that wasn't a solution for what the CIA needed for one of its agents to be able to quickly but securely communicate over the internet.

That then lays the foundation for the invention in this case. You will hear that Mr. Gif Munger, Dr. Short, and two of their colleagues worked on this problem for months. They consulted with other people; they did research. They had to find a solution. How can a VPN be set up quickly and easily?

Finally, you'll hear about a train ride that they took coming back from a meeting in New York back to near where they live, in Washington, D.C., in September of 2009.

On that train ride, Dr. Short, who you just met, had a breakthrough that would solve the problem of how people can set up VPNs easily.

Here at a high level is their invention. Now, of course, you'll hear a lot more about this later on, but in the time that I have right now, let me explain to you that, once again, we have a remote user traveling in Florida, who wants to communicate back to her company. Looks like they're in California.

By typing in what's called a domain name,

the remote user's computer will trigger something called a DNS request.

Now, let me stop there. Those of you who actually used the internet, or have seen it at all, have used a domain name, although you may not have called it that.

A domain name simply means the name of something you're trying to reach out to on the internet, such as Amazon.com; that's a domain name; eBay.com; that's a domain name.

So a remote user types in the domain name and does one click on her computer. That DNS request then goes to some VPN software that's part of the invention, which sends back information to her computer necessary to set up a connection, not yet a secure connection.

There's also software involved in the invention on the far end of the network, this time at Company A. And that software between the two computers automatically negotiates the secure VPN connection between them.

And just like we saw before, once that VPN is set up, a hacker is locked out from being able to hack in to information that's traveling on that network. The important thing to remember here is this remote user

in Florida didn't have to go through all these steps that I described to you to set up a secure VPN.

What she had to do was one click on her computer.

Now, Ladies and Gentlemen, you'll hear evidence that this invention solved the problem of VPNs and made them practical solutions to secure communications over the internet.

Now, it may be important for you to understand when these events occurred, so let me stop the story again, and let's look at this timeline a moment.

We go from 1998 to 2007. It was in 1998 that Gif Munger and Bob Short and their co-inventors were working on the Global Hawk program and first encountered this problem of the need to secure communications that were going over public things, like satellites, or later, the internet.

It was in 1999 that they thought of the invention in this case which provided a way to make setting up VPNs on the internet easy and practical.

In the year 2000, they filed two patent applications for their invention. The first was filed early in the year. And after two years of consideration -- that application was in the United

States Patent Office for two years, and after those two years, the Patent Office issued this patent for the invention, agreeing that it was something new and useful and important.

The second application that they had filed stayed in the Patent Office for almost seven years, the Patent Office considering it all that time. But at the end of those seven years, the Patent Office issued the second patent in this case; again, finding, as a result of their work, that this invention was something new, something valuable, and something important.

Now, we've been talking so far about the VirnetX side of the story. VirnetX is a company that Mr. Munger will explain to you was formed in order to try and make a business out of this invention, and to enforce the patent so that they could receive fair value from anyone who wanted to use the invention.

I've been telling you about Mr. Munger, about his team, and about VirnetX, but now let's change the subject a little bit, and I want to talk to you for a few minutes about Microsoft, the Defendant in this case.

Microsoft, as you know, is the largest computer software company in the world. Let's take a

look at what Microsoft was doing and thinking at the time Mr. Munger and his team had their invention in 1999, about the subject of security, and particularly about virtual private networks.

Fortunately, we don't have to guess or speculate about what Microsoft was doing, because there have been a lot of documents produced in this case, so we'll have an opportunity to show you some documents that will actually reveal to you what Microsoft was doing.

You'll see that in that year, when the inventors had their idea in 1999, Microsoft had this confidential business plan talking about their strategy of how they would win in the marketplace. And they decided that what they needed was to have the best integrated, transparent, which means automatic, policy-based VPN. They recognized they needed an automatic VPN.

And that this would help establish Microsoft as a valued leader in security products. In that same document, you'll see that Microsoft recognized that what they needed was transparent end-to-end security, an automatic VPN, just like you heard that the inventors were thinking about and found a way to do.

But you'll see that Microsoft, at this time at least, didn't see that way to do it. Other Microsoft documents tell us in this confidential document on the subject of transparent connectivity, which, as you saw in the earlier document, is just a way of saying how can we get all this set up without having to go through all these steps.

They said a hard problem is automatic access and configuration. Microsoft recognized that the same problem that Mr. Munger and his co-inventors were working on wasn't something easy to solve. It wasn't something that was obvious. It was a hard problem.

But as the next couple of years went by, Microsoft came under increasing pressure to increase the quality of the security products that it was offering to the public.

You are probably all familiar with Mr. Bill Gates, who, at the time, was the Chairman of Microsoft, and now the former Chairman.

In 2002, he wrote that, we, Microsoft, are now making security improvements an even higher priority than adding features. In other words, instead of coming up with new things the computer could do, Microsoft had now made it an even higher priority to make security improvements.

In the next year, Mr. Gates wrote: As we increasingly rely on the internet to communicate and conduct business, a secure computing platform has never been more important. Along with the vast benefits of increased connectivity, new security risks have emerged on the scale that few in our industry fully anticipated. As a leader in the computing industry, Microsoft has a responsibility to help its customers address these concerns so they no longer have to choose between security and usability.

Exactly the issue we talked about a minute ago. The keypad on the burglar alarm is too complicated to use. Here Mr. Gates is telling us, in 2003, that Microsoft is struggling to find a way so that its customers have something simple enough to use that they don't have to make that choice.

In the next year, 2004, Mr. Gates is still very much concerned with security, as is Microsoft. He says that security advancements outlined today, as well as industry collaboration and innovations in security technology for the future, will play a key role in providing users with a safer and more seamless computing experience.

In a 19 -- excuse me -- 2004, again, he says, if you look at our resources -- that's Microsoft

he's referring to -- and what's the biggest part of that research and development in investment at Microsoft right now, it's focused on security.

As a result of this intense focus, Microsoft also recognized one of the key issues they had to solve was security for remote access, just like we saw with the woman in Florida who needed a VPN.

In this document in 2004, Microsoft said that enhancing the security of corporate assets worldwide is a top priority for the Microsoft information technology organization.

A major concern is remote access -- just what we saw before -- the services and connections that allow approved employees to connect to a corporation's network from a remote location.

As a result of these concerns, Microsoft released some products that allowed its customers to connect to virtual private networks very easily. And one that we'll talk about in this case was called Live Communications Server 2005 that was introduced to the market, as you might guess, in 2005.

In the literature describing that Microsoft Live Communication Server 2005, Microsoft said that with Live Communication, your team can connect with co-workers, partners, suppliers, and customers in

real-time, share critical and time-sensitive information, and collaborate with other organizations as easily as they do today with co-workers, while taking advantage of built-in security measures to help safeguard your proprietary business information.

And in another Microsoft document, this time in 2007, in talking about their communications software, Microsoft says: Not only are we able to launch new business communications with just one click, but user set-up and administration is extremely simple. Does that sound familiar?

It should, because what you will hear from the testimony in this case by experts highly qualified in this field is that just one click that Microsoft refers to starts the invention that is the same as what was patented by Mr. Munger and Dr. Short and their co-inventors.

You'll also see Microsoft documents that establish that this kind of business, this communication software business, was enormously promising for Microsoft financially. You will see that at this time in 2007, they projected that this market was worth an estimated $45 billion.

When Mr. Munger testifies later today, you will hear him explain that during the course of

trying to make something of his invention, trying to get people interested in it, trying to make it usable, he was asked to do some research on this Microsoft Live Communication 2005 product, where he began to suspect for the first time that Microsoft was infringing his patents.

He told the people at his employer at that time, SAIC, and some other people, and they sent a letter to Microsoft, and that letter said we'd like to contact you in the next week or so to discuss the possibility of offering a license to our '135 patent.

We believe the '135 patent would be of interest to your company in connection with this Live Communication Server 2005 product and in connection with Microsoft Office Communicator 2005 product.

And the parties exchange some letters back and forth about that possibility. So what you will hear in this case, Ladies and Gentlemen, is that at the end of the day, Microsoft has refused to pay fair value for their use of the patents and the inventions in this case.

As a result, Mr. Munger, Mr. Short, and their new company, VirnetX, have been required to file this lawsuit to ask you to award them a reasonable royalty for Microsoft's use of their invention.

Now, how much would be a reasonable royalty?

Well, you saw that document in which Microsoft projected that the market might be $45 billion. In fact, they were a little pessimistic. You will hear that from its sale of products that use the inventions in this case, Microsoft has made $48 billion. You will also hear something else interesting. You will hear that back in 2002, SAIC, Mr. Munger's company, entered into a license agreement with a company called SafeNet to use the invention. And you'll hear that at that time SafeNet agreed to pay 20 percent of its revenues from the invention as a reasonable royalty.

Now, you'll also hear that SafeNet, under this agreement, was going to be required to spend money to develop the invention so that it would be ready for sale. And a few months after entering this agreement, they decided that they didn't want to spend the money to develop the invention. Therefore, they terminated this agreement.

But I believe you'll find, when you hear the evidence, that this agreement entered into my SafeNet and their agreement, at least in the initial negotiation, to pay 20 percent of the revenues is a powerful indicator to you of how valuable this invention

really is to people like Microsoft.

But VirnetX and Mr. Munger and Mr. Short are not going to ask you to award them anything like 20 percent of Microsoft's revenues from the sale of these products.

We're going to introduce you later on in the trial, probably on Wednesday, to a man named Brett Reed.

If you'd stand up, Mr. Reed.

Mr. Reed has been in the business for many, many years of valuating the value of things like patents and the amount of a reasonable royalty.

Thank you, Mr. Reed.

He'll take you through a lengthy analysis of how professionals in the field do that. Judge Davis will give you some instructions later on in the trial that you'll hear that Mr. Reed followed in doing that. And you'll hear what he concluded is that the $48 billion in Microsoft's revenue from sale of these products should actually be reduced to no more than $30 billion. And he'll explain to you that he's concluded that a lot of that royalty base doesn't have anything to do with the invention and, therefore, he excluded it.

Out of what's left of the 30 billion, he has concluded that not the SafeNet's 20 percent is fair,

but a fair royalty in this case is less than 1 percent of Microsoft's revenues for the '135 patent and less than 1 percent for the '180 patent.

In short, he will tell you that if you take the dollar that Microsoft made from using the invention that a reasonable royalty is one-third of a penny to two-thirds of a penny for each patent.

Now, I did refer to pennies, but, of course, we're not talking about pennies here. We're talking about billions. Mr. Reed will show you his calculations and will tell you that applying this approach means that the total reasonable royalty he concludes would be paid by Microsoft to VirnetX is $242 million.

That's a lot of money; $242 million is a lot of money in any context. But, remember, Microsoft, you will hear evidence show you, made an enormous amount of money from the use of this invention.

VirnetX asks you only to award them what you find is a reasonable royalty.

Now, that's almost the end of my remarks to you this morning before you hear the evidence. But you will also, of course, hear from Microsoft in this case, as you should.

But I think that once you've heard all

the evidence, you will find that there is a clear path in the evidence which suggests to you that VirnetX should be awarded a reasonable royalty. And I'm afraid that you'll hear that Microsoft in this case will consistently try to distract you and misdirect you from that path.

I think that they will argue to you, well, we don't really use the patent. We don't infringe.

Well, Ladies and Gentlemen, I would like to introduce you to Dr. Mark Jones. Mark Jones is a professor of computer science at Virginia Tech University.

You will hear that in order to really find out whether or not Microsoft infringes, you have to be able to look at Microsoft's secret computer code. And they won't show that to just anybody and show it to the public. Ordinarily, people can't see Microsoft's secret computer code.

But you will hear that in this case, Judge Davis has allowed Professor Jones to study that Microsoft code, and he will explain to you after many, many hours of study, his conclusion that Microsoft uses the inventions and infringes the patents.

I'll warn you, he'll tell you that

conclusion, but then we're going to have to let him spend about two hours, probably on Wednesday, dotting all the Is and crossing all the Ts so that it's entirely clear to you that Microsoft, in fact, does infringe.

I think, though, that if Microsoft is not able to distract you by arguing that they don't infringe, the next thing they may say is, well, if we do infringe, it's not willful.

Well, remember, Microsoft got that letter in 2006 telling them about the patent. I think you'll hear that they didn't do anything to avoid infringing; that they didn't have any good excuse for believing that they didn't infringe; and that they basically just adopted a head-in-the-sand policy of being indifferent about the patents.

Microsoft will then tell you, I believe, well, if you don't buy that we don't infringe and you don't buy that our infringement wasn't willful, how about this: The patent is invalid. Maybe you'll buy that.

Ladies and Gentlemen, Microsoft has already started trying to lead you off the path. You'll remember in jury selection a week ago when the Microsoft lawyer and I had a chance to ask everybody on the potential jury panel a few questions, do you

remember Microsoft saying to you, well, would everybody agree that during this trial, you won't just assume that the patent is valid? Everybody agree you're just not going to assume that?

Ladies and Gentlemen, here's what Judge Davis told you about just this morning. Judge Davis told you, the granting of a patent by the Patent & Trademark Office carries with it the presumption that the patent is valid. The presumption of patent validity imposes the burden on Microsoft to prove invalidity by the clear and convincing evidence standard.

Judge Davis told you about that presumption not once, not twice, but three times this morning.

And at the very end of the trial, we anticipate that we'll put Professor Jones back on the stand very briefly to explain to you how Microsoft is wrong in its attempt to distract you from the path of fair compensation by claiming that the patents are no good.

But if you don't believe that they don't infringe and you don't believe that their infringement was willful and if you don't buy that the patent was invalid, how about this?

Microsoft will say the patents really

aren't valuable. Nobody wants them.

Now, Ladies and Gentlemen, you will hear -- you'll hear it directly from Mr. Munger that he had a difficult time trying to make something out of his invention.

Unfortunately, he started off trying to raise money for it, and in the recession of 2000/2001, the last bad recession we had before this one, when technology companies were particularly hard hit, a few years later, he discovers that the largest software company in the world is already using his invention. And from that point forward, you'll hear him explain it was basically hopeless; that this small group of inventors, this small team would be able to compete against a company like Microsoft, that Microsoft wasn't made to respect their patent rights.

But that, Ladies and Gentlemen, I'll suggest to you will be the most compelling evidence of how valuable the invention is, because you will hear that the largest software company in the world, Microsoft, uses the invention and has made an enormous amount of money doing so.

Now, Ladies of the Jury, I think you've heard about enough from me this morning, and I'm sure you're anxious now to hear this story told by the people

who actually lived through it. Mr. Munger will be our very first witness in the trial?

And we look forward to introducing him to you shortly.

THE COURT: Thank you, Mr. Cawley.

All right. Counsel for Microsoft.

MR. POWERS: Thank you, Your Honor.

THE COURT: Mr. Powers.

MR. POWERS: Well, good morning. I appreciate this opportunity from Judge Davis to tell you Microsoft's side of the story.

And the interesting thing about it is, we can agree with almost everything that VirnetX's lawyer tells you up until about the last five minutes, the signs-in-the-woods part of the opening statement.

Because there really isn't a disagreement in this case about whether security is a good thing, whether patents are a good thing, whether people should pay fair value for their patents. That's -- there's no disagreement about that issue at all.

But what I do want to talk to you about is the areas that he called distractions. Remember that the end of the signs? That's the issue that I want to talk about.

Because Microsoft believes very, very

strongly -- and I'll say it straight out -- that Microsoft does not infringe these patents; that these patents are not valid; and that VirnetX is entitled to no compensation from Microsoft; that is the issue in this case.

And we will present the evidence on those issues in this case. But I want to start with explaining, from our point of view, who the key entities, the key companies are in this case.

We already heard about all of them -- a little bit about them from Mr. Cawley. He referred to this company, SAIC. Now, SAIC is a very large company. Over 40,000 employees, about $8 billion in sales. They're a very, very big company.

And they primarily sell, as Mr. Cawley said, to the U.S. Government. So they're very relevant to this case, not only because of that, because the technology at issue, which was called NetEraser and then later VernetX by Mr. Munger, that technology was developed at SAIC. So you're going to be hearing a lot about it for that reason.

Mr. Munger and Mr. Short were both employees at SAIC at that time, and SAIC filed patent applications that relate to the patents that we're talking about here in this case.

But you'll also hear that SAIC attempted very hard to try to get many, many companies interested in that technology. The very same technology you just heard about, Mr. Munger and Mr. Short developed. They worked very hard to try to get people interested in it, and that didn't work.

And I want to pause there for a minute, because that shouldn't be a surprise. There's no shame in developing technology that people don't want to buy, because it doesn't really solve a problem, it doesn't work very well or whatever. It happens all the time. Coke developed new Coke. That didn't work very well. Ford developed the Edsel. That didn't work very well. Microsoft developed a lot of those products that just didn't sell very well at all. It happens routinely in this business when you're trying to develop something new, particularly in the technology space.

But what you're supposed to do is step back, pick yourself up, and try again. Make something people do want.

And Microsoft has been successful. No doubt about it. It's Microsoft's position that it's successful because of its own engineers, it's own hard work.

And that success is nothing to be ashamed

of. That's a good thing. That's part of what makes this country great, is people making things that keep people employed, that people want to help. That's what it's supposed to be, how it's supposed to work.

So there's no shame in the fact that the technology that Mr. Munger and Mr. Short developed wasn't successful commercially. No shame in that. But it is a fact, and I'll show you some evidence that relates to that, because it's important in this case.

Finally, SAIC, the very company that employed Mr. Munger and Mr. Short, the very company that filed these patent applications, it decided this technology was not worth further developing, and that decision is supported in this case as well.

Here's a list of the companies that SAIC tried to sell to. You see some of the biggest names in the industry: Morgan Stanley, Amazon, eBay, Yahoo, people who were building the internet space, and they took the technology to them, and Mr. Munger was often the person going to give a demonstration and explaining the technology.

And these companies, for one reason or another, said: No, no thanks. We're not interested. And that was their decision. And in fact, no company, no company bought the technology that Mr. Munger and Mr.

Short developed at that point.

Well, they didn't stop there. To their credit, they were persistent, and because SAIC primarily sells to the government, they thought, well, maybe government agencies.

You recall the discussion in Mr. Cawley's opening statement that the whole idea of this was to be used for spies and the CIA, so let's try to sell it to the CIA, Homeland Security, the FBI, and many others. And here they had two advantages. One advantage was that SAIC had very good relationships with those agencies. Most of SAIC's business is to sell it to them.

But, second, the government already had a free license to these patents because of the N-Q-Tel funding that Mr. Cawley told you about.

So you'd think that some of these agencies, if it really solved the problem of security and they could have the license for free, they would have said: Yes, let's use it. Well, they said no, and they said: No. Thank you.

Now, that -- again, there's no shame in that. A lot of people, including Microsoft, make the products that people just say no thank you to, but that's a fact.

So when you hear VirnetX say that they solved the problem of security, the question would be why did none of these companies, all of which were interested in security, why did they say no thanks?

Well, let's talk about N-Q-Tel for a minute, because Mr. Cawley raised it, and that is the place where the initial funding for this work came. You heard that from Mr. Cawley in his opening statement. And you heard about the relationship between N-Q-Tel and the CIA.

Well, what you didn't hear was that N-Q-Tel decided to stop the funding, because they gave some initial money before the developmental work started, so before they saw any technology, and then VirnetX, SAIC, delivered that technology to the CIA and said: Here, try it out, and we'd like some more money, please, to finish the development.

N-Q-Tel said no. And in language that's fairly clear but harsh, but not my language, N-Q-Tel said: This NetEraser project -- that's the name that -- one of the names Mr. Munger had given it -- should be placed in the living dead category -- he put it, not my words -- with little or no attention paid to it.

So the very same company that started the funding that was the source of it said, after they saw

the technology: No, we're not interested.

Well, to their credit, SAIC didn't give up, but then they decided to stop funding as well. And this is a memo from Mr. Munger's boss, Mr. Jobien. This is in June of 2001. And he tells them: Well, the company has pretty much thrown in the towel on NetEraser, now VirnetX.

So in 2001, June, they said: Well, we're just not going to fund it anymore.

And also in June, this is, again, an internal SAIC document: We're going to pull the plug on VirnetX, which is another name they were using internally for that technology that Mr. Munger and Mr. Short developed.

So you have technology that they worked hard to develop. They had a good idea, trying to make things newer, all good so far. They developed it, but it didn't work as well as they wanted it to. It didn't solve the problem that people wanted it to.

And, therefore, the original funders said: We're not interested anymore. Their own company said: We're throwing in the towel.

But interestingly, there's -- part of the reason was why. So in this memo from Mr. Hendrix, who's a SAIC executive, he says why they're pulling the plug.

He says: The straw that broke the camel's back was the loss of the ANX beta site as they decided to go with an Aventail solution.

Now, ANX was a company that SAIC had a relationship with, and ANX chose a different technology over Mr. Munger's and Mr. Short's. They chose something called Aventail.

And you're going to hear more about that, because that's one of the pieces of prior art that's at issue in this case. It's another technology by another company that solved that VPN security problem.

And SAIC, Mr. Munger and Mr. Short's own employers, chose it instead of the Munger/Short technology. And they went beyond that. SAIC actually invested in Aventail. Where SAIC stopped funding the VernetX's technology, they decided to fund Aventail instead.

Remember that when we get to the discussion about prior art and validity, because Aventail is very, very important to that.

Now, you heard about SafeNet in the opening statement from VirnetX's lawyer. And you heard about a license that SafeNet had with SAIC. And that's all true.

But what you didn't hear is that once

SAI -- once SafeNet got the technology, the Munger-Short technology, and looked at it and evaluated it, they said: Does it really solve the problem? Does it really work? No, it doesn't actually accomplish any real simplicity. And as they put it: It just moved the complexity around.

So all that discussion you heard about trying to make everything simpler, the company that actually had the chance to sell that technology, wanted to sell that technology, because it really worked, after evaluating the technology, said it doesn't really work. And what did they do? They paid VirnetX, under that license agreement that you heard about in opening statement? No. They terminated it before they had to pay them a dime under that 20 percent. No payments under that 20 percent, because the technology didn't work.

Now, you heard about the letters that SAIC sent to Microsoft, but there's one part of that story you didn't hear. It is true that after deciding to stop funding their own technology and after being rejected in other attempts to find the funding and customers for it, at that point, they did send a letter to Microsoft saying: We think you infringe.

And here's that letter in May of 2006.

And it says: We think this patent covers any internet-based communications implementing a particular RFC.

RFC is a type of standard in this business, and you'll hear more about that.

Well, you'll find out that that statement proved not to be true, the one they said in the first letter accusing us of infringement. We wrote back very, very promptly, just two or three days later, saying: Well, we disagree, but we'd like to meet.

We wrote again in September of the same year. We still disagree then and now, but we'd like to meet. But even more than that, we want some information that backs up your claim. Give us something that backs up your position, the claim you made that we infringe.

Now, we think that a company that's going to come here and ask for $42 million would at least send us something saying why they thought we infringed or at least meet with us.

They gave us no information. They had no meeting. What they did was sue us, VirnetX. VernitX, Inc., was a company started in 2004 by this man named Kendall Larsen. He owns about 20 percent of the company or a little bit more, and he received the patents from SAIC to go sue Microsoft.

So after having the -- SAIC trying to make the company work, not being able to succeed, this is where they went next. VernetX has never sold a product, never.

Now Microsoft. Microsoft, I think we all know a lot about. They've been around for a long time now. They employ a lot of people and they have a great, great history of innovation in this space. They have over 26,000 engineers working very, very hard to create the products that we all use every day.

They're proud of that; we're proud of that. Now, the problem with that -- their success is often -- one of the people we're going to meet that you already met in jury selection is Gurdeep Pall. Gurdeep joined Microsoft in 1990.

Thank you, Gurdeep.

And he is one of the true pioneers in VPN technology. And VPN technology works, and people actually use it. He's a Vice President at Microsoft, and he coinvented something called Pointe2Pointe Tunneling Protocol.

And that was the first commercial VPN. Called PPTP. Unfortunately, you get a lot of acronyms in this case. I can't do anything about it. That's how these people speak.

But PPTP, which is hard to say five times fast, that was the first commercial successful VPN, virtual private network, and Mr. Pall coinvented that at Microsoft.

He also invented a technology called AutoDial, which is pretty much exactly what it sounds like, something which automatically makes a connection, very similar to what you're talking about, and that happened before Mr. Munger did his work. All of that happened before Mr. Munger did his work.

Mr. Pall has been recognized by many people, including Information Week, as being one of the premier technologists of our time working on this problem. He was called one of 15 innovators who will make a difference in 2008. Yet he's the one who stands here accused of being an infringer. He's a true innovator.

Let me back up some of what I just said. You heard from Mr. Cawley that in 2000, SAIC filed those patent applications. Now, when did Mr. Pall, Gurdeep Pall, do his PPTP VPN? Way back in 1996. Four years earlier. That's when he invented it and released it. And AutoDial came out later that year, four years earlier, a long time ago. He was working on that well before Mr. Munger even started, much less before they

had the invention.

Now, what was PPT -- PPTP -- can't even say it -- what is it and how did it work and why is it important? Well, it did really change how we work. It allowed easy access to a company network.

And you'll hear from Mr. Pall that one of the things he was thinking about when he was inventing this was how filled the Microsoft parking lot was at midnight. Everybody had to get their work done. They work very, very hard there, and they were working sitting in their cubicles working at midnight.

And he says: Wouldn't it be nice if we could work at home? That way we could go home, see our families, have dinner, and then work at home without having to stay here all night long. And that's one of the things he was trying to solve.

And sure enough, after he invented PPTP, that parking lot, never empty, was a lot, lot less filled at midnight. Because then people could work at home and do it easily, and they could do it securely.

Now, it's not just me saying that; the world recognized this advance. PC magazine, in December of 1996, gave Mr. Gurdeep Pall's Pointe2Pointe Tunneling Protocol the Networking Software Technical Excellence Award.

And what did they say about it? They said: It's a new protocol that enables secure remote access across the public internet, exactly what we're talking about here, exactly what VirnetX's lawyers say they saw in 2000, 1999. PC week is saying Mr. Pall did it in 1996.

But more than that, excellent security PPTP provides, and it's a virtual private network while locking out unauthorized users. All of that in 1996, four years before.

So what is this case about from Microsoft's perspective? Let me talk about first what we don't think it's about. It's not about whether patents are good. Microsoft agrees, patents are a good thing.

It's not about whether people who have patents should be paid fair value when someone uses those. We agree. And in fact, you'll hear in the evidence we do pay fair value when we use someone's technology. You'll hear about a lot of licenses that we took and said we're paying fair value.

It's not about whether -- it's not about whether security is a good thing. Security is a good thing and will be a problem. It has been forever, and it will be forever.

Every time you get an advance, there's still someone trying to make everything more secure. But the idea that the problem of security was solved in 1999 by Mr. Munger and Mr. Short's work, however hard they worked, it just isn't true. We're always working on better security. Always. But that's not the issue here.

It's also not about whether Mr. Munger should be saluted and thanked by everyone here for his war story. Everyone agrees with that. That's not the issue either.

The issues in this case, the ones that will be on the verdict form that Judge Davis mentioned to you, are really going to be three, and there are going to be a lot of issues that can be raised in the patent case, but I'm only going to talk about three, and these are the three core issues.

First, does Microsoft software, the ones they're saying infringe, does that software use the VirnetX's patent?

Second, was VirnetX first? You heard Judge Davis' instructions about anticipation. That's what this question is about. If somebody did what VernetX claimed but did it earlier, the patent's not valid.

And last, was VernetX's claimed invention obvious? But not just obvious to anyone; obvious to those skilled in this technology.

And that's an important distinction that I want to pause on for just a minute, because something that's obvious to somebody might not be obvious to others if they don't have the same training or experience.

We're coming up on tax season, and you could say whether something is deductible is not always obvious to me, but it would be obvious to an accountant who works in that space every day. You could say that a certain symptom that caused that symptom is not always obvious to me but would be obvious to a doctor or nurse who works in that field.

You could ask whether the reason for a teenager's behavior is obvious? Well, if you have five kids as I do, three of them teenagers, might be a little more obvious than to somebody who's never had a kid. And the whole point of that is, obviousness has to be viewed through the eyes of the person that's relevant. And here the person that's relevant is someone who has a lot of training in this exact space, a lot of education, and a lot of experience.

So much more is obvious to them than

would be obvious to almost anyone else in this courtroom.

Let's talk about the first issue first. Microsoft software does not use the VirnetX patent. Our first two witnesses are going to be Gurdeep Pall, who you've met, and Tyler Barton, another Microsoft employee who worked on these technologies.

Tyler, would you stand up, please?

And they will explain to you what they did, how it works. They'll tell you about that technology, and that will be from the people who actually invented it and made it work.

You'll also hear from Professor David Johnson, who's an expert in this space.

Mr. Johnson, could you stand up?

And he'll explain to you his analysis, after many, many hours, why Microsoft does not infringe. But I don't want to give you just conclusions; I want to show you the evidence and why Microsoft's products don't infringe. They don't use VernitX's patents. And there's two core reasons.

You heard from Judge Davis' instructions, and you'll hear later, that in order to show infringement, VirnetX has the burden to show every single aspect of those claims is contained in our

software. If it's missing only one, there's no infringement. And we're showing you two as to the '135 patent.

First question is whether they're VPNs. Now, Judge Davis has given you instructions on what a VPN means on that first sheet in the juror notebook, and this is a copy of it right here from your juror notebook. And the key point is, there has to be private communication.

So you might say, well, how do I know whether it's private? Well, you know whether it's private in two ways.

And the way it's important here is whether someone is eavesdropping on a communication, we'll know who's talking to whom. And for that, I have to spend just a little bit of time explaining some of what this technology is going to be about.

One of the products in question is Microsoft's Office Communicator, also called OC or OCS. In that context, this requirement that an eavesdropper can't tell who's talking to whom doesn't matter, and I'll show you why.

Now, in any communication on the internet, you see these numbers here on the left, 204.11.52.127 and the different numbers over on the

right? Those are called IP addresses.

And that's going to be one of the most important concepts in this case, an IP address. Because for a computer, an IP address is like a name.

So if these were two people talking, it might be Matt Powers talking to Gurdeep Pall. But in the case of computers, you use numbers because that's what computers work on.

And so the issue back when the computer on the left talks through that internet to the computer on the right, can an eavesdropper see who's talking to whom? And the answer here, as you see, is that eavesdropper can see exactly those numbers, and they're the same numbers.

What you'll hear from VirnetX is that their idea was, you prevent that eavesdropper from seeing the IP addresses.

So the big issue here is, can eavesdroppers see those numbers, the numbers corresponding to the real numbers of those computers?

If the answer is yes, there's no infringement, because it's not an -- it's not secret. It's not private. If the answer's no, then that limitation is met.

And you'll hear from VirnetX how they

tried all sorts of ways to prevent that eavesdropper from seeing those numbers, including using different numbers so that they could see maybe some numbers but not the right numbers.

But in our technology, because it's not being used with spies and CIA, but being used by normal folks sitting in our houses, those numbers are visible.

Now, there are many other things done for protection and security, but you can see those numbers, so there's no infringement.

Now, you might ask yourself, what does Microsoft say when it's trying to sell this Office Communicator Product? Do we say it's great because of the VPN, and therefore, it's secure?

Well, actually, we tell you the opposite. It doesn't require a VPN, and it needs only an internet connection. So it's the opposite.

So that VPN requirement of the claims just one of the things that VirnetX has to prove, it's just not there.

The second requirement that you'll see in the claims is that there be a website. Well, Microsoft products aren't websites. And, again, Judge Davis has given us a definition. That's in the front page of your book, and it says it's related web pages on the

worldwide web.

Well, we all know what web pages are. We use them often every day, whether it's Facebook, whether it's Google, whether it's Bing, any one of those, we use those every day, and that's a web page. You know what those are.

And the worldwide web, which is that www in the name, well, that's just a collection of all those web pages. They're all linked together, and the reason it's called a web is it sort of looks like a web like you would envision. That's why it was called web.

Now, this accused product, this OC/OCS, the Office Communicator, that's not a website. That's software that is running on a server.

Now, VernetX here has admitted it's not a website, even though that's a key requirement of the claim. So VirnetX has been forced to admit there's no literal infringement.

So what they're arguing is that OCS is equivalent to a website, and that will be an issue that you have to decide on this particular requirement. But it's important, from our point of view, that you understand that under their theory, almost everything is a website, even a phone. Even a phone can be a website under their definition or an equivalent to a website.

And I think that sort of argument tells you exactly what their position is.

So there are two requirements to that '135 patent that they have to prove, two requirements, and both of them are missing. If only one is missing, they cannot prove infringement.

So now let's talk about the '135 patent, again looking at the detail. Not the conclusion, but the actual facts.

Two requirements here, too. First, that same requirement of VPN. The second is something called a secure computer network address. You'll be hearing a lot about both of those.

Now, the VPN, same issue. The question is whether that -- these particular IP addresses can be seen by an eavesdropper.

Well, in Windows Meeting Space, which is a particular product -- the application that's at issue on this patent, '180, no dispute that that number and that number are both the -- you can't see them. And remember, if you can see those numbers, there's no infringement.

So VPN isn't satisfied for the '180 patent for the same reason it wasn't satisfied in the '135. It's not private. You can see the right numbers,

the right names of those computers.

But there's a second requirement, this secure computer network address. That requires authorization for access. That's Judge Davis' definition. And so the question is, on the products that they're talking about for the '180 patent, does the address require authorization for access?

Well -- and it's important to understand what that means, because in the context of a computer, you could have a computer, for example, at a big company, where you're behind what's called a firewall. And you cannot get to that computer unless you have access to get through that firewall. That's what protects that company's computers from outside people coming in. It's built up, it's protected, and it requires --

That's not what they're accusing here. What they're accusing here, it's saying that our computers at our homes are secure computer network addresses.

Well, I don't know about you, but my computer in my home gets a lot of e-mails that I didn't give anybody access to. Advertisements for things I didn't -- I don't want. A lot of what's called spam e-mail.

Now, that -- but that address is what they're calling a secure address. A lot of people get information to me on my home address that I don't give any authority to at all.

And so when you compare the difference between a secure address and an insecure address, I think a good example is 211 West Ferguson Street, which is the address of this courthouse that we're all in right now. That's a secure address.

It's locked at a lot of the time, and when it's not, there's a guard downstairs with a gun. You have to give your driver's license to get in, and then you have to go through a metal detector. That's a secure address. That's like the firewall that I told you about before.

My home computer, the one they're accusing here, where people can send spam without my authority, that's like the Wal-Mart. It's open 24 hours.

Now, 5050 Troup Highway is that address. Is that a secure address? No. Anybody can walk in. Just like my computer at home, anybody can send me an e-mail without me blocking it. That's the difference, and that's not a secure address.

So that's the second key requirement in

this case that VirnetX has to prove. And if they can't prove any one of them, they haven't made their case. They can't prove that one either.

So that's the first question. That's the first question you're going to be asked on the verdict form that Judge Davis gives you. Not a distraction. It's the actual issue in this case. Do we use their patents? The answer is no.

Second, was VirnetX first? Again, this is going to be the issue on the verdict form, anticipation. Well, they weren't. They were not first. And here the Patent Examiner did not have the best prior art.

And the three I'm going to focus on are Aventail -- you heard about that before -- Microsoft's PPTP with AutoDial -- you heard about that before; that's the one that Gurdeep Pall invented back in '96 -- and one you haven't heard about yet called Dynamic VPN, also known as DVPN, that was created by a company called Trusted Information Systems, TIS.

Now, I say the Patent Examiner didn't have this prior art. You might say, well, how do I know that? We know that for exactly the reason that Judge Davis you in the earlier instructions. The patents tell you exactly what prior art or what knowledge the

Examiner looked at, so we don't have any question about it. He lists it under references cited.

And the interesting thing is, it's the same Examiner for both patents, the '135 and the '180. The Examiner was the same person, Krisna Lim. And Aventail PPTP with AutoDial and DVPN, none of those is listed in those references cited.

So you are going to be the first group that can decide whether these patents are valid based on that prior art. The Patent Office didn't have a chance to, and under our system, if you remember from the jury video and from Judge Davis' instructions, you're the only group that can decide that. No one else has.

Now, you might say, how could that be? How could that be possible? The Patent Office is -- that's their job, is to look at all the prior art. Well, the answer to that lies partly in common sense and partly what you heard in the jury video, the jury video that you saw about a week ago. The common sense part is that Patent Examiners are human beings. None of us is perfect. People can make mistakes. That can happen. But you also heard in Judge Davis' instructions just this morning that the Patent Office may or may not have the best prior art. And that's the case here. Because we know the Patent Office didn't consider those three

references.

But you also saw in the jury video these pictures and saw that -- and heard this discussion, and you saw they had a lot of work to do.

Now, we're not saying they don't try their best, and we're not saying they make a mistake all the time. No. We're just saying, it's possible that in this context, they didn't have the best prior art to make the decision that you have to make. And that's exactly what happened in this case.

So the first piece of art I want to talk to you about is Aventail. I actually had to look it up. Their logo is a knight on a horse.

Aventail -- and the reason they named it that, and you'll hear about this from one of the witnesses -- it's a type of armor that each of the knights used when they were jousting. So it involves protection, and that's why they chose the name. I thought that was interesting.

You'll hear from Chris Hopen by videotape deposition. He's not a Microsoft employee. He's the one that founded Aventail, the company. And you'll hear from him about when -- what he did, when he did it, and how it works.

And you might ask yourself, who was

first? Was Aventail first, or was Mr. Munger or Dr. Short first? Well, here's their application in 2000.

Way back here in 1996, Mr. Hopen founded Aventail, four years earlier, and they actually had a product that people were selling and that many, many large companies, including many of the large companies that SAIC tried to sell to, who wouldn't buy it, they were using Aventail, and those sales started in late 1997.

But there's one other aspect about Aventail that's important in this case. It's not just that they were first and that they were selling actual products that people were using that worked; it's that SAIC in this case actually chose Aventail over its own technology.

Remember, the SAIC employees were Mr. Munger and Mr. Short, and they chose Aventail for the ANX beta site -- ANX did -- and SAIC chose to invest in Aventail rather than to further fund the work that Mr. Munger and Mr. Short were doing.

And that tells you a lot about whether Aventail was the earlier inventor because SAIC had the chance to pick either, and it chose Aventail.

You'll hear from Professor Wicker, an

expert witness in this case who's been very, very involved in the areas that matter. And it could be we'll talk about the DARPA, because that called the Defense Advanced Research Projects Agency.

It's affiliated with the Department of Defense, and their job is to do research and support research that relates -- that can support the Department of Defense. You're going to be hearing about that quite a bit.

Dr. Wicker was involved in that. Also involved in the National Science Foundation Cyber Security Center, which is called TRUST. And he's done a lot of work in this case.

Dr. Wicker, would you stand up? Thanks.

And you'll hear from him as to why, in his view, based on these specific references, it's invalid.

And I'm not going to -- I don't have the time to show you all that entails. He's certainly much better able to explain it than I am. But if you take the claim, and you divide it up into its various pieces, he will show you how each aspect of that claim is specifically found and executed in Aventail. He will show how every aspect of the claim works and how Aventail did it but did it before SAIC.

The second piece of prior art I want to talk about is Gurdeep's PPTP with AutoDial.

The first question, of course, is going to be, is it first? Because it's not prior art if it's not earlier. We have the same 2000 date where they filed their applications.

When did he do this work? We already know the answer to that. He did it back in 1996. But he didn't stop in '96. He kept improving it, and he got better and better, all before the patent application by SAIC.

NT5 was released in 1997. NT4, you're going to hear a lot about that. That's just the internal Microsoft name for that product. That was in '96. It's a real product. People were really buying it, using it, working. NT5, two years later, an improvement.

The Beta 3 released in 1999, yet all before, all before the work that we're talking about by Mr. Munger and Mr. Short.

So then the question is: We know it's earlier. What did it do?

Again, Dr. Wicker -- Professor Wicker will explain to you in detail how that prior art invalidates both patents-in-suit, because it did earlier

what they claim to have done later, which is really just the issue.

And, again, he'll do that comparing the claims, showing you, based on the figures of PPTP, how every aspect of that claim is found exactly in the reference PPTP and how PPTP works. But it was four years earlier.

So the four pieces of prior art that we're going to be talking about is this Trust & Information Systems Company's product called DVPN or Dynamic VPN. And you'll hear from three witnesses on this. None of them are a Microsoft witness, because it's not a Microsoft type of product.

The first is a man named Sami Sajdjari. Now, he works for DARPA, that company I just mentioned a little bit ago. And DARPA plays in this quite a bit. It's interesting. Mr. Sajdjari actually led a conference in February of 1998 that Mr. Munger attended that got him to really thinking about how to build a product here.

That was in February of 1998. Mr. Sajdjari was the one leading that meeting, and then Mr. Munger submitted a proposal to DARPA asking for funding.

Now, you'll also hear from Dan Sterne and Darrell Kindred, both who work for that Trust &

Information Systems Company, about what the product is and what it did.

And you'll also learn that it was well before. Same patents in 2000. Trust & Information Systems development started in '97 and actually showed that product at a DARPA conference in March of 1998, long before.

So it's clearly prior art.

And you'll also hear from both Mr. Sajdjari and Mr. Sterne that DARPA funded the TISC DVPN work; yet they rejected SAIC's request that DARPA fund Mr. Munger's work. They chose TISC's product and technology over Mr. Munger's and Mr. Short's. And you'll hear from Professor Wicker on that subject as well.

Now, the third and last issue is obviousness. And remember, obviousness is obvious to this person who's skilled in the area of the technology, not to really any of us. And you'll hear from experts on that issue.

So the first reason the patents are not valid, the biggest one first. That's a basic requirement of U.S. patent law, as Judge Davis has instructed you.

But we're also going to show you

obviousness, and obviousness goes to what people in this field were doing at that time.

And the interesting thing about this field is that it's not a couple of people in garages sort of working by themselves. You can imagine you wouldn't want that, if you're talking about how the system, the entire internet is going to work.

So there's an organization called the IP ITEF, Internet Engineering Task Force, and that is a very large organization made up of some of the best minds, from professors, companies, government, et cetera, who all come together and think about how the internet should work, which makes sense that you would want to all work together, so they need to follow all the same rules.

And you'll find out that the concepts in these SAIC patents were well, well known in already established standards at the time. Already established standards.

And those groups, the ITEF, got together and said -- they're trying for more security. Let's try these various efforts, and you'll hear about those different standards.

Damages. Short answer from Microsoft's perspective is there are none. We don't infringe, and

the patents are invalid.

When we talk about what this case is about, the first issue, does Microsoft's software use the VirnetX patent, the ones that they're saying we do and they're saying they infringe? Well, no.

That eavesdropper can see the address, the right address of those computers. And therefore, it's not anonymous and not private. It's not a VPN. It's certainly not a website and not a secure address. Not like this courthouse. It's more like the Wal-Mart, our computers at home.

Was VernetX first? They were four years behind other people and four years behind other people whose technology was working, being sold and bought and used out there in the world at a time when SAIC's technology people were saying: No thank you.

So does Microsoft software use the VirnetX patents? The answer to that is no.

Was VirnetX first? No. They were four years behind at least these three companies.

And was VirnetX's claimed invention obvious? The answer to that is yes.

So based on the evidence, based on the facts -- not distraction, but based on the actual issues you have to decide, we will ask you to render a verdict

for Microsoft.

I thank you very, very much for your attention.

THE COURT: Okay. Thank you, Mr. Powers.

All right. Ladies of the Jury, you've now heard the opening statements in the case, as well as the Court's preliminary instructions. We're going to recess for lunch at this time, and we'll come back after lunch and begin hearing the evidence in the case.

So I'm going to recess you until 1:30 today, give you a little extra time. Normally, we'll take about an hour, hour and 10 minutes. I'm going to give you about an hour and 25 minutes today, give you a chance to get familiar with downtown, find your restaurants you want to eat at, and get you some lunch.

And be back here ready to go at 1:30.

Please remember my instructions. Don't discuss the case among yourselves or with anyone else. Just keep your own countenance about the case until all the evidence comes in. So enjoy your lunch, and the jury is excused at this time.

COURT SECURITY OFFICER: All rise for the jury.

(Jury out.)

THE COURT: Please be seated.

All right. If you would, if you're in the audience, if you could just remain in the courtroom until we finish the hearing.

Ma'am, if you would just -- ma'am, if you would just remain in the courtroom until we finish the hearing. What I want to do is give the jury a chance to get out before everybody starts exiting, give them a head start on lunch ahead of all of you.

Let me just go over with the parties, when we come back after lunch, one of the first things I would like to do is have the exhibits introduced, and we'll go through that exercise first.

And then I'll have -- I'd like for you to have all of your witnesses in the room so that they can all be sworn in at one time. We won't have to do that piecemeal.

If they're not here today, then we'll swear them in as we deal with them, but everybody that's available today and here, please have them in the courtroom, and we'll swear them in.

Is either side going to invoke the Rule?

MR. POWERS: Yes, Your Honor.

THE COURT: Okay. Have y'all discussed and worked out an agreement as far as who is excused from the Rule?

MR. CAWLEY: Actually, we haven't. I assume expert witnesses.

MR. POWERS: Exactly.

MR. CAWLEY: Okay.

THE COURT: Expert witness, and we know who our company representatives are.

Anybody else in dispute?

MR. POWERS: There's no dispute, Your Honor.

THE COURT: Okay. All right. Well, just be sure y'all explain to your witness who's covered and who's not, and I won't try to go through that in front of the jury.

All right. Anything else before we break for lunch?

MR. CAWLEY: None from the Plaintiff.

MR. POWERS: None from Microsoft.

THE COURT: Okay. Very well. Well, let me ask you again about this motion to strike. When does that need to be taken up by?

MR. CALDWELL: Your Honor, I guess it depends on when Microsoft wants to -- if they're going to put on evidence in front of the jury. I mean, it's a legal defense, so I don't know that they're going to put on evidence in front of the jury, but I'm -- I'm not

sure I can answer.

MR. POWERS: As we said in the papers, Your Honor, we believe it's a legal defense. We're not putting on evidence in front of the jury about it. It's an issue for the Court.

THE COURT: Well, I'll continue to consider it then.

All right. Be in recess.

COURT SECURITY OFFICER: All rise.

(Lunch recess.)

* * * * *

CERTIFICATION

I HEREBY CERTIFY that the foregoing is a true and correct transcript from the stenographic notes of the proceedings in the above-entitled matter to the best of my ability.

/s/_____ _____
SUSAN SIMMONS, CSR Date
Official Court Reporter
State of Texas No.: 267
Expiration Date: 12/31/10

/s/_____ _____
JUDITH WERLINGER, CSR Date
Deputy Official Court Reporter
State of Texas No.: 731
Expiration Date: 12/31/10

EXHIBIT F2

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX	*	Civil Docket No.
	*	6:07-CV-80
VS.	*	Tyler, Texas
	*	
	*	March 8, 2010
MICROSOFT CORPORATION	*	1:30 P.M.

TRANSCRIPT OF JURY TRIAL
BEFORE THE HONORABLE JUDGE LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPEARANCES:

FOR THE PLAINTIFFS: MR. DOUGLAS CAWLEY
MR. BRADLEY CALDWELL
MR. JASON D. CASSADY
MR. LUKE MCLEROY
McKool-Smith
300 Crescent Court
Suite 1500
Dallas, TX 75201

MR. ROBERT M. PARKER
Parker, Bunt & Ainsworth
100 East Ferguson
Suite 1114
Tyler, TX 75702

APPEARANCES CONTINUED ON NEXT PAGE:

COURT REPORTERS: MS. SUSAN SIMMONS, CSR
Ms. Judith Werlinger, CSR
Official Court Reporters
100 East Houston, Suite 125
Marshall, TX 75670
903/935-3868

(Proceedings recorded by mechanical stenography, transcript produced on CAT system.)

APPEARANCES CONTINUED:

FOR THE DEFENDANT:
MR. MATTHEW POWERS
MR. JARED BOBROW
MR. PAUL EHRLICH
MR. THOMAS KING
MR. ROBERT GERRITY
Weil Gotshal & Manges
201 Redwood Shores Parkway
5th Floor
Redwood City, CA 94065

MS. ELIZABETH WEISWASSER
MR. TIM DeMASI
Weil Gotshal & Manges
767 Fifth Avenue
New York, NY 10153

MR. DANIEL BOOTH
Weil Gotshal & Manges
700 Louisiana
Suite 1600
Houston, TX 77002

MR. RICHARD SAYLES
MR. MARK STRACHAN
Sayles Werbner
1201 Elm Street
4400 Renaissance Tower
Dallas, TX 75270

MR. ERIC FINDLAY
Findlay Craft
6760 Old Jacksonville Highway
Suite 101
Tyler, TX 75703

* * * * * *

P R O C E E D I N G S

COURT SECURITY OFFICER: All rise.

(Jury in.)

THE COURT: Please be seated.

All right. Everybody ready to go?

Okay. All right. Let's see. First, we're going to have all the witnesses that are going to testify. So if you're a witness who's going to testify in this case, if you would please stand wherever you are.

All right. And if you would start here at the front and just state your name on around the room, so the court reporter can take it down.

A WITNESS: My name is Edmund Colby Munger.

A WITNESS: My name's Gurdeep Singh-Pall.

THE COURT: Would you spell that.

A WITNESS: Yes. G-U-R-D-E-E-P, S-I-N-G-H, and last name is P-A-L-L.

THE COURT: Thank you very much. Okay. Next?

A WITNESS: My name is Tyler Barton.

THE COURT: And how do you spell that last name.

A WITNESS: B-A-R-T-O-N.

THE COURT: Okay.

A WITNESS: My name is David Johnson.

A WITNESS: My name is Stephen Wicker.

A WITNESS: Mark Thomas Jones.

A WITNESS: Brett Reed.

A WITNESS: Robert Dunman Short.

THE COURT: Short?

A WITNESS: Short, yes.

THE COURT: If you would raise your right hand to be sworn.

(Witnesses sworn.)

THE COURT: Now each of you have been sworn as witnesses in this case. The Rule has been invoked, and that means if you're a witness and you're not a party representative and you're not an expert, then you cannot be present during the proceedings and would need to leave the courtroom.

Also, you cannot discuss the case with anyone else during the course of the case, other than one of the attorneys associated with the case.

So if you're one of the parties that is not -- or if you are a witness who is not an expert or who is not a representative of a party, you would need to leave the courtroom at this time; otherwise, you may be seated.

All right. At this time, does Plaintiff have some exhibits that it wishes to offer?

MR. McLEROY: Yes, Your Honor, we do. Should I read them into the record, Your Honor?

THE COURT: How long is it?

MR. McLEROY: It's a long list.

THE COURT: Long list? Let me see a copy of them, if you would.

All right. This is entitled, List of Plaintiff's Trial Exhibits to be Admitted.

Has Defendant Microsoft had an opportunity to review this list, which is 15 pages in length, and begins with No. 1 and ends at No. 983?

MR. POWERS: We've been exchanging lists of what's objected to, and I believe this list to be accurate, so there is no objection.

THE COURT: I am going to mark this as Plaintiff's Exhibit List No. 1 just for purposes of the court record.

Do you have any objections to any of the exhibits listed in this?

MR. POWERS: We do not, Your Honor.

THE COURT: So the exhibits listed in Plaintiff's Exhibit List No. 1 will be admitted, Ms. Ferguson.

Does the Defendant have any exhibits it wishes to offer?

MR. POWERS: Similarly, Your Honor.

THE COURT: All right.

All right. I have been handed what's

marked, List of Defendant Microsoft's Trial Exhibits to be Admitted. And this is some 21 pages in length, and begins with Exhibit No. 3001 and goes through 3576. And I will tell the Members of the Jury that these numbers aren't all consecutive, so there's not that many exhibits; it's just in -- just the numbering system for both parties.

All right. I will mark this as Defendant's Exhibit List No. 1.

Does Defendant offer all of these exhibits?

MR. POWERS: We do, Your Honor, and, similarly, I will represent that these are the exhibits that Plaintiff has said they have no objection to.

THE COURT: And does Plaintiff have any objection?

MR. McLEROY: Your Honor, excepting the representation, we have not had a chance to look at this list before, so we have not had a chance to double-check to make sure --

THE COURT: All right. Exchanging lists, and you have no reason to believe this is not the list?

MR. McLEROY: No, Your Honor. We have not exchanged this list before.

MR. POWERS: We have exchanged similar

list, but this is just a combined list of the lists that went back and forth. I will represent that.

THE COURT: Do you have any objections to the exhibits listed on Defendant's Exhibit List No. 1.

MR. McLEROY: No, Your Honor, we don't.

THE COURT: All right. Be admitted.

MR. POWERS: Your Honor --

THE COURT: And if -- if -- go over it and if as represented, there are any that aren't, bring it to my attention this afternoon, and I will reconsider those.

MR. McLEROY: Yes, Your Honor.

MR. POWERS: I will note for the record that our agreement that these are in evidence is subject to the stipulation that we earlier submitted to Your Honor that you haven't yet ruled, but it is subject to that issue.

THE COURT: I understand. All right. Okay. With that, Plaintiff may call their first witness.

MR. CAWLEY: Thank you, Your Honor. Plaintiff VirnetX would like to call to the stand Mr. Gif Munger.

THE COURT: All right. Mr. Munger.

MR. CAWLEY: Your Honor, may I approach

with a document?

THE COURT: You certainly may.

MR. CAWLEY: May I proceed, Your Honor?

THE COURT: Yes, you may.

EDMUND "GIF" MUNGER, PLAINTIFF'S WITNESS, PREVIOUSLY SWORN

DIRECT EXAMINATION

BY MR. CAWLEY:

Q. Would you please introduce yourself to the jury.

A. Yes, sir. I am Edmund Colby Munger, and I have a nickname Gif.

Q. Why are you here, Mr. Munger?

A. I'm one of the co-inventors on the two patents that are in question.

Q. What did you invent?

A. The invention makes it easier to communicate across the internet safely.

Q. Did you get patents for your invention?

A. Yes, sir.

Q. Is your invention important?

A. Yes, sir.

Q. Why do you say that?

A. All right. It's important that it's easy to set up VPN connections so we can protect -- protect

communications across the internet, whether they be pictures or files.

Q. What kind of people would use your invention?

A. Well, anybody could use the invention. Any individual, moms could move her pictures, but also small businesses could use it to communicate their sensitive data, large corporations, and even the government.

Q. Could it help even people who don't personally use computers?

A. Yes, sir.

Q. How is that?

A. Well, anytime you go into a store or use a credit card, the information that you provide is -- is -- is private, and that data is moved around by networks between banks to set up credit cards. And so businesses use it to order and transmit sensitive information.

Q. Now, Mr. Munger, did you invent this by yourself?

A. No, sir. It was a team.

Q. Tell us who -- who else was on the team.

A. There was Dr. Bob Short, Dr. Vic Larson, Dr. Doug Schmidt, and Michael Williamson.

Q. And are they all listed as inventors on the patent?

A. Yes, sir.
Q. Will we hear from any of them in this trial?
A. Yes. The jury will hear from Dr. Bob Short.
Q. All right. So, Mr. Munger, I would like for us to hear more about your invention and how the long process of your -- your managing to invent it with your team, but let's find out a little bit more about you first.

Where do you live?

A. I live in Crownsville, Maryland, which is just outside of Annapolis, Maryland.
Q. Are you married?
A. Yes, sir.
Q. Did you go to college?
A. Yes, sir.
Q. Where did you attend college?
A. I attended the United States Naval Academy and then later MIT.
Q. Why did you choose to attend the Naval Academy?
A. Well, my great-grand -- great-great grandfather was a fisherman out of Maine, and my dad commanded destroyers during World War II, so I guess it's pretty much in my blood.
Q. When did you graduate from the Naval Academy?

A. 1967.
Q. What did you do then?
A. I was commissioned as a -- an officer at the rank of ensign and went off to my first duty station, which was a destroyer off Vietnam.
Q. What were your duties on that destroyer off the coast of Vietnam?
A. I was a gunnery assistant.
Q. Would you say that your duties as a gunnery assistant were technical?
A. Yes, sir. I was responsible for the radar, the alignment of the guns, the computers that -- that operated the guns, yes, sir.
Q. Okay. And what -- what's the next duty you had after that ship?
A. I went to another destroyer where I was the weapons officer and became responsible for all of the weapon systems on the ship.
Q. And what about after them?
A. After that, I became the commanding officer of a mine sweeper, and then went to MIT.
Q. Okay. So you were the commanding officer of your own ship?
A. Yes, sir.
Q. At what age?

A. 28.
Q. Now, you said then you went to MIT.
Is that the Massachusetts Institute of Technology?
A. Yes, sir.
Q. Were you still in the Navy when you went to MIT?
A. Yes, sir.
Q. How did that come about?
A. Well, the Navy sends certain of its officers to engineering school so that they can work on the technology in the Navy and ships.
Q. What did you study during your time at MIT?
A. I studied naval architecture and marine engineering.
Q. Now, when you were studying those subjects -- and I guess we're talking about the mid-'70s; is that right?
A. Yes, sir.
Q. Did you use computers?
A. Yes, sir.
Q. What did you have reason to use computers for at MIT?
A. Well, for -- to get a master's, you needed to do research and write a thesis. And my -- my research

was the development of a -- of a program for ship design that if you modified the dimensions of the ship, it would tell you how it would change performance.

Q. So did you write that computer software?

A. Yes, sir.

Q. Now, just looking around the courtroom, I guess I could pick out a dozen computers very easily, but this is the mid-'70s we're talking about.

What were computers like then?

A. Well, it was -- it was early in the use of computers for engineering computations, and a computer was in a room that was this size. And if you wanted to write a program, you had to type it out on punch cards, put all the punch cards in a box, and take it to the room that had the big computer in it. They would run it. You would come back in a few hours, and they would give you a printout, and you'd go through this process over and over.

Q. Now, did you -- were you still on active duty in the Navy throughout your time at MIT?

A. I was.

Q. And you were at MIT for four years; is that right?

A. Three -- three years, sir.

Q. Three years.

And did you get a degree from MIT?

A. Yes, sir.

Q. What was that?

A. I got a master's in naval architecture, marine engineering, and an engineer's degree called naval architect.

Q. And after you got those graduate degrees from MIT, what did you do then?

A. I went back to sea with the Amphibious Forces, which are part of the Navy that work with the Marine Corps. And then I returned to the Naval Academy and taught engineering for two years.

And then I went back to a destroyer as second in command, and then I went to Washington to work on advanced ship concepts.

Q. What do you mean advanced ship concepts?

A. One of the projects I worked on was a stealth ship that was -- could resist attack by cruise missiles.

Q. All right. During this second half of your career as a naval officer after you left MIT, would you -- were you involved with technology in the Navy?

A. Yes, sir.

Q. And did you specifically work, as part of your duties in the Navy, with technology related to communications?

A. Yes, sir.

Q. Now, we've been talking about that a lot already today, security.

What is security?

A. Security is the protection of any -- any system, whether it's your home or a ship or aircraft or a communication system like the internet.

Q. And why is security important in communications?

A. Well, it's important that if we're going to communicate and we want to keep certain information private, that we use certain approaches. And also if we want to control critical systems, we want to keep -- we want to make sure that that's done safely.

Q. Now, Mr. Munger, did your work in the Navy help you later in your career when you were faced with some issues having to do with communication security?

A. Yes, sir.

Q. In fact, did your experience in the Navy help you invent the technology in this case?

A. Yes, sir.

Q. When did you retire from the service?

A. I retired in 1987.

Q. What was your rank?

A. Commander.

Q. So you retired from the Navy in 1987. By my arithmetic, you were 43 years old. You had spent your entire adult life in the United States Navy.

What did you decide to do then?

A. I went to a company called Science Applications International Corporation, or SAIC.

Q. Tell us a little bit about SAIC.

A. Well, it was founded in 1969 by a doctor in physics, and his concept was to bring scientists and engineers together to do research for the Department of Defense and the government.

Q. So what -- what was the -- what was the charge of SAIC?

A. SAIC was taking science and figuring out how to apply it to present-day problems.

Q. How many employees were there at SAIC when you joined?

A. When I joined, there were 6,000.

Q. 6,000?

Why did you make this decision to go to work at SAIC?

A. There were two reasons. One, I had met in the Navy some of the scientists and engineers that worked there, and I had a lot of respect for them, and I wanted to join and work with them.

The other one was it was an employee-owned company, meaning that each of the engineers or employees that worked at that company have ownership stake in the company.

Q. All right. You say that most of SAIC's work was for the governments in the realm of national security.

Can you give us some examples of the kind of things that SAIC has done for national security?

A. Well, a number of them are classified, but I think one that we may touch on every day is the -- they have developed sensors for airports to stop terrorists, and screening trucks and containers that come into port, that sort of thing.

And also, some of the projects that I worked on like War Breaker and Global Hawk.

Q. Before we go into those projects, I want to -- I want to touch on an issue that you briefly just mentioned, that many of SAIC's projects are classified.

Do you mean by that that they are classified by law as government secrets?

A. Yes, sir.

Q. Are you allowed to talk about classified, secret matters that you have worked on?

A. No, sir.

Q. Was the work that you did, though, on what became the patents in this case, classified?

A. No, sir.

Q. So is that -- the reason that you're able to testify about it today is because it was not a classified project?

A. That's correct, sir.

Q. Now, you mentioned a word, or maybe it's two words -- I'm not sure -- before I asked you those questions, and it was War Breaker.

What was War Breaker?

A. War Breaker was a program that networked together a lot of real-time simulators so they could be evaluated, the different combat systems could be evaluated in real-time.

And it was also used as an analysis for critical -- critical problems that were being faced.

Q. So let's talk about critical problems. Was there a particular critical problem at the time you were working on the War Breaker project at SAIC that commanded your attention?

A. Yes, sir.

Q. And -- and did this challenge that you encountered at War Breaker turn out to be important to the invention in this case?

A. Yes, sir.

Q. What -- what was that challenge?

A. The challenge was we were in the first Iraq war, and the Iraqis were firing terrorists missiles into Israel. These were called scuds, and they presented some serious problems that -- we were having difficulty encountering them.

Q. What -- what was the particular problem with the scud missiles and their launchers?

A. Well, the -- the scud launcher is a truck, and it could actually hide under tunnels or under bridges. And it could come out and set up and fire and go back into hiding in less than 10 minutes.

Q. Now, did this problem of scud missiles lead to a new project for you and for SAIC?

A. Yes, sir, it did.

Q. What was that project called?

A. That project was called Global Hawk.

Q. What role did you play in the Global Hawk project?

A. SAIC had a contract to provide system engineering and the technical support to the program office that was doing the development of this -- of this system, and I was the program manager.

Q. Now, did the Global Hawk program introduce you

to some problems or issues that would later be important to you and your team in coming up with the invention in this case?

A. Yes, sir.

Q. Let's find out a little bit more about it.

What is Global Hawk?

A. I -- I did bring a picture, so I thought I'd show it.

Q. Okay. Can you show us that picture?

A. It just came up.

So I'll tell you about it then?

Q. Yes, please.

A. This is a picture of the Global Hawk, and you can't tell by looking at this picture, but this is a very, very big aircraft. From tip of the wings is about 120 feet. So this is pretty large.

It's got no pilot, so this is what they call an unmanned air vehicle, and it has sensors that can see -- see the ground in very good resolution. And it also flies very high. It flies at 60,000 feet.

And if you've taken a jet from Dallas to New York, they fly about 30,000 feet. So this flies three times higher than a commercial jet.

Q. Okay. Now, you mentioned that this is --

THE COURT: Excuse me, Mr. Cawley. Did

you say it has no power.

THE WITNESS: No pilot.

THE COURT: No pilot. Okay.

THE WITNESS: Nobody driving, sir.

THE COURT: I wasn't sure how it got up there.

THE WITNESS: Sorry for my accent.

Q. (By Mr. Cawley) Let me pick up on that.

It had no pilot. You said it was an unmanned aircraft?

A. Yes, sir.

Q. Well, didn't the military already have unmanned aircraft? Sometimes we hear them called drones?

A. Yes, sir.

Q. Well, why couldn't the military's drones solve the scud problem?

A. Well, the problem that we had were these were terrorist weapons, and they could come out anytime during the day or night and shoot. And the low-flying drones couldn't see very far, both sides, so it would take a lot of them to cover them. And they really couldn't stay up in the air.

This one could stay up in the air for 24 hours, and it could be replaced. So it was always up

there, and it could see a very far distance.

Q. Okay. Well, what about satellites?

Satellites are very high, and they stay up all the time.

Why couldn't they see the scud missiles?

A. Well, they could. But a satellite also flies over three or four times a day, depending on the type of satellite. So there were still gaps when the enemy could come out and attack.

Q. So how would the Global Hawk solve the problem of scud missiles?

A. Well, it's probably easier for me to just show you what the concept was.

Q. Please do.

A. So here -- here's the Global Hawk, and we sort of knew the general area that these bad guys were going to come out and shoot the rockets. So we would place the -- the Global Hawk over there so it could watch this area 24 hours a day.

We also needed to get the information very quickly to the ground, because we didn't have a lot of time. So there was a public commercial satellite that was used. And when a picture was taken, it would beam that picture through the satellite to an operator on the ground.

So the concept here was that when one of these scud launchers would come out -- and that's a picture of the scud launcher in the bottom left-hand corner -- the Global Hawk sensor would get a picture of it, and it would very quickly be able to transmit it through the satellite to an operator on the ground who had resources that could be brought in.

And in this case, this is a picture of an F-15. And he would send a message to the F-15, and the F-15 could attack the missile launcher.

Q. Now, was there a particular issue about the security of communications in this Global Hawk system?

A. Yes, sir.

Q. What was that?

A. Well, to my knowledge, it was one of the first times that we were using commercial public infrastructure for operating a critical military system.

Q. Okay. You said some words there I want to make sure I understand.

Let me ask this question: How had the military -- after all, this was being done for the military, right?

A. Yes, sir.

Q. How had the military traditionally kept its communications secure?

A. Well, they would -- they would build their communication systems and own their own communication systems, and they would build in whatever was necessary encryption and hardness. And that was the practice up until this time.

Q. How is Global Hawk different?

A. Well, Global Hawk was using a satellite that other people could rent to relay TV or make network connections between one facility and another facility in two different countries.

Q. So you're telling us that there are satellites orbiting over the Earth that are just owned by businesses?

A. Yes, sir.

Q. And those -- their businesses could lease out bandwidth or transmission capability of that satellite?

A. Yes, sir.

Q. So, for example, for anybody who has satellite TV or may see those dishes in people's yards, that's coming from some satellite that a business owns; is that right?

A. That's correct.

Q. So are you telling us that the military that made the decision, rather than to use its own satellites, to simply lease or rent space on a

commercial or public satellite?

A. That's correct.

Q. Why did they do that?

A. Well, the picture sizes and the radar image sizes were very large, and it would have really taxed the military-owned systems. So it was the first time we really started moving lots and lots of information very quickly.

Q. Now, did the military's decision to use a commercial satellite create any particular security issues?

A. Yes, sir.

Q. Tell us about that.

A. Well, we sure didn't want any of this to be intercepted. And so measures were taken to make sure that all of the transmissions were very secure.

Q. Was Global Hawk a success?

A. Yes, sir.

Q. Did it take down scud missiles?

A. No, sir. The Iraq war was over by the time the first ones were in the air.

Q. Where is it being used?

A. It's not -- it's being used today in both Iraq and Afghanistan.

Q. Who at SAIC worked on this Global Hawk project

with you?

A. We had a number of engineers, but Dr. Bob Short and Dr. Vic Larson also worked on this project.

Q. Now, Mr. Munger, did Global Hawk, this project you've just described to us, even after the project was finished, influence your thinking about future security issues?

A. Yes, sir.

Q. Tell us about that.

A. Well, there are two aspects. It -- it became clear to me that we were really going to have to move information around the battlefield very quickly and very securely. And there are battles that could be anywhere. I mean, we couldn't have projected that we were going to be in Afghanistan.

So what I realized that the internet was going to need to become an asset for the security of the nation, and that was going to take some really good secure technology for doing it.

The other -- the second part of this was that business was being conducted over the internet more and more every day. It was just the beginning. We were buying books at Amazon, but it also meant that we were going to -- we really needed to make the internet safe for business, because it was going to be important to

the nation.

Q. So what did you do in response to your thinking about these future security issues?

A. The first thing I did was I went and talked to my -- my management all the way up to the CEO, and I asked them if we could put together a small team to take a look at this problem, and they agreed. They broke a few of us loose to work on it.

And the other thing was that I wrote a -- I wrote a paper called Aladdin.

Q. Okay. Let's -- let me show you Plaintiff's Exhibit 365.

Is this a copy of the paper that you wrote?

A. Yes, sir.

Q. And you see the title up there at the top, Aladdin? Do you see that?

A. Yes, sir, I see that.

Q. Why did you call the paper Aladdin?

A. Well, the concept that was presented in the paper is we wanted to be able to bring the right people together very quickly to make decisions in support of military operations.

And the idea was that you wanted to make it so easy that you could rub Aladdin's lamp and the genie would make everything connect, and so the soldier would

get the support that he needs.

Q. So who read the Aladdin paper?

A. The Aladdin paper was distributed in DARPA. It was provided to other engineers and scientists in the company, and some of them provided it to their sponsors like the Army.

Q. The United States Army?

A. Yes, sir.

Q. Now, you mentioned something that I want to -- I want to make sure we understand what you were referring to, because I think it may come up again. You said DARPA. What is DARPA?

A. DARPA is the Defense Advance Research Project Agency.

Q. All right. So did the efforts that you were making, the small group that you had assembled within SAIC, and this Aladdin paper, did this lead to the project that eventually produced the invention in this case?

A. Yes, sir, it did.

Q. Who was that project for?

A. That project was for a company called In-Q-Tel.

Q. What is In-Q-Tel?

A. In-Q-Tel was a company formed by Congress to

invest in very early, promising technology that would have application both commercially and would help the CIA.

Q. The Central Intelligence Agency?

A. Yes, sir.

Q. Why wouldn't the CIA just do it themselves?

A. Well, if -- if it also -- if the technology was useful to the CIA and also had commercial application, it would be -- it would cost less to provide that capability to the CIA than if they had to develop and maintain it in-house.

Q. So are you saying that this was a way of farming out to private enterprise the development of technology that the CIA might want to use without having to spend a lot of government money to do it?

A. Yes, sir.

Q. Why are companies like yours, your company back then, SAIC, interested in working with In-Q-Tel?

A. There were -- there were two aspects. One, we -- we were getting funded to do the research, which was the model for SAIC. And, two, we were also allowed to keep the invention rights.

Q. And what did the CIA get?

A. Well, the CIA got the -- got to test and to utilize on a limited basis anything that was developed.

Q. So did the C -- did your company, SAIC, get a contract with this congressionally set up company, In-Q-Tel to pursue your ideas?

A. I'm sorry. Would you repeat the question?

Q. Sure.

Did your company, SAIC, get a contract with In-Q-Tel to pursue your ideas for the CIA?

A. Yes, sir.

Q. Let me show you Plaintiff's Exhibit 311. Is that a copy of the contract between your company and In-Q-Tel?

A. Yes, sir.

Q. I see at the very top there it actually says In-Q-IT.

Why is that?

A. They went through a name change.

Q. Okay. So is this -- even though it says In-Q-IT, this is still the same company, In-Q-Tel, set up by Congress?

A. Yes, sir.

Q. What was the project that was -- this contract was for?

A. Well, we had proposed to them survivable VPN. But the concept was they were interested in having their agents be able to connect and use the internet to -- to

very privately connect back to resources that might help their agents.

Q. Well, surely the CIA has its own communications equipment.

Why did they need to be able to use the internet?

A. Well, they -- they -- they have a lot of communication capabilities themselves, but this would have been a complement, and the internet was becoming used more and more all over the world.

Q. And was the potential use of the internet by agents of the CIA similar to the issues that you faced in Global Hawk and wrote about in the Aladdin paper?

A. Yes, sir.

Q. What was the amount of the contract that SAIC entered into with In-Q-Tel?

A. It was approximately $3-1/2 million.

Q. Now, at the time you undertook this project, did you assemble a team of people to work with you?

A. Yes, sir.

Q. And were you and your team already familiar with some ways to make internet communications more secure?

A. Yes, sir.

Q. So -- so some -- some ways to make internet

communication secured already existed at the time you started on this project.

Is that what you're telling us?

A. Yes, sir.

Q. For example, didn't online companies that were selling things -- I think you mentioned Amazon -- didn't they have security?

A. Yes, sir, they did.

Q. What was it called?

A. It was called https.

Q. What does https stand for?

A. Hypertext transport protocol secure.

Q. So why wouldn't that kind of security have worked for the CIA?

A. Well, it was basically a point-to-point communication to a server. And they wanted the flexibility to be able to reach various computers on -- on the fly.

Q. Could you do that with https?

A. No, sir.

Q. Were there other ways that were available at this time to secure limit on the internet?

A. Yes, sir.

Q. What was that?

A. Virtual private network.

Q. We have already heard some about that, but I guess you're the first witness to tell us about it.

What is a virtual private network?

A. Well, I -- it's probably easiest to take the three words. There's virtual, private, and network. So I'm going to look backwards, because it's easier for me. If we start with network -- we saw some pictures -- but if we think about two computers with a wire between it that has the capability to transfer files or voice or stream video, those two -- those two computers are networked together.

If I put a third computer up and put a wire between them and I can now transfer information between all three, that's a network, and you could keep adding computers. So that's what a network is in very simple terms.

So then we're going to go to private. We had virtual private network, so private is -- if I have those three computers in my house with the door locked and somebody would have to come in and tap the wire, because I've got -- it's in my house -- that's called private. And it would be difficult for somebody to see the traffic between those three computers.

So virtual means that it's going to have the same sort of levels of -- of -- of safety and privacy,

except that if I had a computer out over the internet -- and we've already heard that you can hear things; people can hear traffic over the internet -- but if I secure that with something that encrypts the traffic and makes it safe, that's now become the virtual private network.

So those -- that's my easy definition, sir.

Q. Okay. Well, besides your easy definition, you're aware that Judge Davis has defined for us all what a virtual private network means in your patent, aren't you?

A. Yes, sir.

Q. Remind us -- we'll take a look at what Judge Davis has told us the meaning of virtual private network as it's used in the patent.

Can you read that to us?

A. Yes, sir.

A network of computers, which privately communicate with each other by encrypting traffic on insecure communication paths between the computers.

Q. Thank you, sir.

Now, Mr. Munger, you didn't invent virtual private networks, did you?

A. No, sir.

Q. What did you and your team invent?

A. We invented an easy way to automate their

set-up.

Q. Did your team consider virtual private networks as a possible solution for the In-Q-Tel and CIA project?

A. Yes, sir. It was promising.

Q. Did your team look at and study a variety of software and hardware that was available in the late 1990s to set up or create VPNs?

A. Yes, sir.

Q. For example, did your team look at some software that Microsoft offered at that time which would set up a VPN?

A. Yes, sir.

Q. Did you look at the software of other companies that could be used at that time to set up a VPN?

A. Yes, sir.

Q. Were there some hardware products that could also be used to set up a VPN?

A. Yes, sir.

Q. Did you find that there were any problems with these products that you and your team studied?

A. Yes, sir.

Q. What was it?

A. The biggest problem was the complexity in --

in the number of steps that it took to get to the -- to VPNs to communicate.

Q. Can you give us an example?

A. You might have to type in as many as 15 different settings and make sure they were all correct before the VPN would work.

Q. Did -- your team at SAIC, which included Ph.D.s in this field, as well as other people who are highly expert, did they have trouble setting up VPNs with the available software?

A. Yes, sir.

Q. And do you understand that Dr. Short, who is not in the courtroom anymore but will be later, will be able to actually demonstrate what was required to set up a VPN back in this time period?

A. Yes, sir, he will.

Q. Did you think that these products that were available were appropriate solutions for what the CIA needed?

A. No, sir.

Q. So how long did your team wrestle with this problem of the undue difficulty and complexity of setting up virtual private networks?

A. I would estimate four or five months.

Q. What did you feel that you needed to

accomplish to solve that problem?

A. Well -- well, we really wanted it to become as easy as making a telephone call. We wanted it so easy anybody could use it, and that it pretty much happened in a few seconds or so.

Q. Okay. So you had realized, as you were struggling with this problem, you and your team, that you wanted to make it easy.

But was it easy to make, creating a VPN simple?

A. No, sir.

Q. But did your team working on this issue eventually have a breakthrough that solved the problem?

A. Yes, sir.

Q. How did it happen?

A. It was in September of 1999, and we were visiting a professor up at Columbia University in New York, that had been working on making phone calls over the internet.

And on the train ride back, we were talking about -- this is Dr. Bob Short, myself, Dr. Vic Larson. We were on a train ride back from New York to the Washington area, and we were talking about how we wanted it to be as -- as an example, as simple as people understanding how to make a phone call.

And Dr. Short said -- came up with the idea. I mean, it was startling. He said, well, how do we make a phone call, or how do we make a connection on the internet? And his -- his a-ha at the time was that people that used the internet knew -- could remember how to go to Amazon.com or eBay.com, which is entering a domain name.

And what he realized was that if we could make people, or a piece of software that was entering a domain name and doing look-up, automatically trigger the virtual private network that we had a way forward.

Q. How did you feel when he made that suggestion, when he got that idea?

A. Well, I mean, we've all struggled with problems. We think about them over a very long time, and you don't feel like you're making a lot of progress. You have the goal; you kind of know what you'd like to achieve.

But when he said it, it was kind of like, wow, I mean, this is it. This is -- this is a way to focus how we could possibly pull this off.

Q. Now, even after Dr. Short had this idea on that train ride, did you still have work to do?

A. Oh, yes, sir.

Q. How long did it take between that breakthrough

idea and the time that you had the details of the invention worked out?

A. I'd probably say three or four months.

Q. Okay. Let me show you Plaintiff's Exhibit 367.

What is this document?

A. This is a progress meeting with a company that we talked about before, In-Q-Tel, and we -- we named our technology. I mean, it went through a lot of names. You've heard NetEraser and all sorts of things.

But at this time, we were calling it In-Q-Net in honor of our research sponsor. And in this presentation are the first presentation of the ideas of that automation.

Q. So are there a lot of ideas in this presentation?

A. Yes, sir.

Q. Had nothing to do with your invention?

A. That's correct.

Q. But is this the first document you know of in which the idea for your invention was presented?

A. Yes, sir.

Q. And that was in January of the year 2000?

A. Yes, sir.

Q. After your invention, how long does it take a

user to set up a virtual private network?

A. A few seconds.

Q. And will Dr. Short actually be able to show us that in the courtroom?

A. Yes, sir.

Q. And who would use your invention to set up secure internet communications?

A. As I mentioned before, basically anybody. Any individual that wanted to connect with any other individual or their company or small businesses. Pretty much anybody could use it, sir.

Q. So did you file for patents on your invention?

A. Yes, sir.

Q. And as part of your employment agreement with SAIC, did you and your co-inventors agree that you would transfer your patent rights to SAIC?

A. Yes, sir.

Q. Let me show you Plaintiff's Exhibit 9 just quickly.

Is this some documents filed with the Patent & Trademark Office that contained the assignments of the application that eventually became the '135 patent?

A. Yes, sir.

Q. And the same question with regard to Plaintiff's Exhibit 7.

Is that a document filed with the U.S. Patent & Trademark Office that contains the assignment from you and your co-inventors of the application that became the '180 patent to SAIC?

A. It is.

Q. What role did you play, Mr. Munger, in applying for the patents?

A. I worked with the patent attorneys in helping to draft the specifications and reviewing the patent, sir.

Q. And let me show you Plaintiff's Exhibit 2.

Is this the document that is something called the file history; that's the whole record of the communications back and forth with the Patent Office?

A. Yes, sir.

Q. And is Plaintiff's Exhibit 5 the same thing for the second patent?

A. Yes, sir.

Q. Let's take a look at Plaintiff's Exhibit 3. Do you recognize that document?

A. Yes, sir.

Q. What is it?

A. That's what we call the '135 patent, sir.

Q. When did the '135 patent issue? When did the Patent Office actually approve and issue that patent?

A. That was in December of 2002.

Q. So, Mr. Munger, how did you feel when you got that first patent?

A. Well, I was pretty excited. It was my first patent, and -- I don't know. We always grow up hearing about Ben Franklin and Thomas Edison and Alexander Graham Bell. It was an interesting feeling to become a member of that club.

Q. And let me ask you to look at Plaintiff's Exhibit 6.

What's that document?

A. This is what we call the '180 patent.

Q. This is your second patent that was approved and issued by the United States --

A. Yes.

Q. -- Patent Office?

Did you continue during this time, Mr. Munger, to work on software to deliver to In-Q-Tel?

A. Yes, sir.

Q. What -- what did you call that software?

A. NetEraser.

Q. Why did you give it that name?

A. One of the primary things that we were working on with them was a different technology called address hopping. And the goal of that software was -- of that

technology was to mask the existence of the communication on the internet.

Q. So did you deliver prototype software -- NetEraser software to In-Q-Tel and to the CIA?

A. Yes, sir.

Q. Did the CIA use it?

A. I -- they tested it, but I can't tell whether they used it, sir.

Q. Well, how is it that you don't know if they used it or not?

A. Their communication technologies are very secret, and I -- I -- I didn't have the need to know about it, sir.

Q. Now, at this time, in -- in 1999 and 2000, you've recently finished the NetEraser project.

Did you think that your invention and your team's invention was ahead of its time?

A. Yes, sir.

Q. Why do you say that?

A. Well, at the time, I was using a computer at home, and it worked. But we were using a dial-up connection, which was very slow. And where we saw the promise of this was in -- in voice and in screening video.

And though in my research I was lucky enough

to work with very high capable networks, it was really -- it was going to take time before households got the large bandwidth which would demand this type of security.

Q. But even though you had that feeling that your invention might be a little ahead of its time, was your company, SAIC, free to try to do something with the invention?

A. Yes, sir.

Q. Did you ask any others to help evaluate the work and prospects for your invention?

A. We did.

Q. Who did you talk to?

A. One of the ones that I worked with and provided support to was Cambridge Strategic Management Group.

Q. What is Cambridge Strategic Management?

A. It was a consulting firm that the company hired to take a look at the technology and -- and its market viability.

Q. Okay. What did Cambridge conclude?

A. They concluded -- we had them both look at the whole body of technology. But they concluded that the automation was the most promising commercially.

Q. Let's look at Plaintiff's Exhibit 359.

Is this the presentation that was given to your company, SAIC, by Cambridge?

A. Yes, sir.

Q. And if we look at Page 3 of that presentation, what did Cambridge have to say about your automation invention?

A. Well, they said that we had patented technology that allows -- that could play a significant role in providing hassle-free VPN connections and enhanced security.

Q. Okay. And did they also attempt at least to place some kind of value on what this technology might be worth?

A. Yes, sir.

Q. Let's look at the next page.

What do they say?

A. Well, they said that a net present value, which is what is it worth, if it was a lump sum today, would be approximately $190 million.

Q. Now, Mr. Munger, have you seen various estimations for what this technology might be worth over the years, high and low?

A. Yes, sir. And they're all over the place. The only thing that this said to me was that -- that it was a promising technology.

Q. Okay. So what did you do then?

A. The company had -- we were coming to the end of In-Q-Tel's contract, and the company decided that they might want to attempt to roll the technology out into a company and seek investment.

Q. Why did they need money from investors?

A. Our technology was still in prototype form. It wasn't ready to go out to the market. It wasn't -- it still required development.

Q. So why didn't SAIC just do that themselves?

A. It's not their culture to try to set up and run themselves a commercial -- a commercial company. They're a company that sells engineers for hours plus fee, sir.

Q. Well, what kind of companies did you go talk to, to try to raise money for your invention?

A. We talked to venture capitalists.

Q. What is a venture capitalist?

A. Well, a venture capitalist is an investor that is looking for brand new companies, early start, that possibly have very high pay-off. So they're usually willing to take more risks, and they expect that if the company does well, they're going to make more money on their investment, sir.

Q. And are there venture capitalists, for

example, in investing in technology start-up companies.

A. There are, sir.

Q. Now, what -- what time period are we talking about that you went out on the road to talk to venture capitalists about the possibility of investing in your invention?

A. This was springtime, 2001.

Q. Spring of 2001, was this a good time to be out looking for money for a high-tech start-up company?

A. It was the worst time.

Q. Why do you say that?

A. Well, we're in a recession now. But in 2001, we were right in the middle of what was called the dot.com bust. And it particularly hit hard on technology companies.

So investment in new ventures was very hard to find.

Q. So how many companies did you talk to, to try and raise money for your invention?

A. Approximately 30.

Q. 30?

A. Yes, sir.

Q. Let me show you Defendant's Exhibit 3192.

What's this?

A. This is a memo from Mr. Ed Hendrick, who works

in the SAIC Commercialization Group, to our SAIC CEO, giving him the status of our investment search.

Q. Okay. If we could see Page 2 of that document, does this page list some of the potential venture capital companies that you talked to about the possibility of raising money?

A. Yes, sir.

Q. The second page -- or I guess, the third page, more?

A. Yes, sir.

Q. Then the one after that?

A. Yes, sir.

Q. How many are on the list in total?

A. I think when I counted, I believe there's 30 on that list, sir.

Q. And where were they located?

A. Some of them were in the Silicon Valley just south of San Francisco, some in New York. And there's probably a couple spread around in other major cities, sir.

Q. Okay. Did any of these companies invest in -- in your invention?

A. No, sir.

Q. Why did you -- why do you think you couldn't find investors at that time?

A. Well, there was the tightness of funds, but also most of these companies that we talked about were trying to prop up their companies that they had present investments in. And they also were looking, if they had new money to invest, in, one, companies that are very close were already going out to their first customers and ready to -- to make money, sir.

Q. Were you ready to go out to your first customers for your invention?

A. No, sir. We needed seed funds to mature our product, sir.

Q. When you mature your product, what does that mean?

A. Well, we had a prototype, and we needed to develop it into a product. And it was just in beta, and until it's ready to take the first customers for test and evaluation, sir.

Q. In addition to these venture capital companies, did you also talk to some companies about the possibility of going into a development agreement with you so that you could develop your invention, bring it to maturity together?

A. Yes, sir.

Q. Who did you talk to about the possibility of doing that?

A. We talked to Morgan Stanley. We talked to eBay. We talked to Amazon.com.

Q. And what did you propose to those companies?

A. Well, again, we were looking for development dollars. And part of that discussion was on a -- some of our other technology for robust VPNs.

Q. And did any of those companies agree to co-develop your invention with you?

A. No, sir.

Q. Why did you think you couldn't find a company at that time that was willing to co-develop your invention?

A. I think those companies are used to buying things -- off-the-shelf-solutions that are all ready to go, sir.

Q. Did you have a product on the shelf ready to go?

A. No, sir.

Q. Now, you told us that you spent a lot of time on the road in this time period, trying to find investors for your invention.

Did others -- people back at the shop keep on working on the software for the invention?

A. Yes, sir, they did.

Q. But did the company, SAIC, eventually decide

that it had to stop the development of your invention?

A. Yes, sir.

Q. Why -- why did that happen?

A. Well, it was clear that we were not going to get investment, and they decided to shut down the commercialization effort and allow the technical team -- there was a budget, and there was some money left in it -- they allowed the technical team to continue development on the prototype to where it became -- to where it became a beta.

Q. When did SAIC decide that it would no longer put new funds into the development?

A. June of 2001.

Q. And what was the plan?

A. The plan was to continue with the remaining funds to develop the product and also return to government customers, which was something that SAIC is used to, and see if we could possibly interest them in continuing the development effort.

Q. Okay. Let me take out a couple of minutes there to ask you about something we heard about this morning, this company called Aventail.

Did SAIC own a company called ANX?

A. Yes, sir.

Q. What business was ANX in?

A. They were in the business of connecting parts vendors for the automobile industry to automobile manufacturers.

Q. And did ANX have a need for secure communications?

A. Yes, sir.

Q. So what product did they choose to accomplish that?

A. Aventail.

Q. Why didn't they choose your invention?

MR. POWERS: Objection, Your Honor. That's calling for speculation at least for ANX's decision for which Mr. Munger he can't --

THE COURT: Restate your question.

Q. (By Mr. Cawley) Why do you think that they chose something other than your invention?

MR. POWERS: Same objection.

THE COURT: Objection is sustained.

Q. (By Mr. Cawley) Did SAIC also invest money in Aventail?

A. Yes, sir.

Q. When was that?

A. I believe the fall of 2001.

Q. Do you know why SAIC decided not to continue to invest money in your invention?

A. No, sir.
Q. Did you continue working on the beta?
A. Yes, sir.
Q. And how was progress going in the late summer of 2001?
A. It was going well.
Q. Let me show you Plaintiff's Exhibit 94. What is this document?
A. This is an e-mail from Dr. Bob Short to Mr. Don Foley, who was one of the upper managers in SAIC.
Q. And what does he tell him about the progress on the beta version of your invention?
A. Well, he says that he thought people would be surprised and pleased with the beta product that is coming out of this final push.
Q. Okay. You know what? I apologize. We've been using this word beta several times now.
What is a beta?
A. A beta is a -- is a product that is not quite ready for full distribution out in the market. But it's generally ready to have a community outside the company or outside the developers test and evaluate it and give it feedback, so you can harden it up so you're ready for release.

Q. So what was Mr. Short telling us about the progress on the beta on August 22nd, 2001?

A. Well, he thought it was going very well, sir.

Q. Did anything happen shortly thereafter which made it more difficult for you and some other members of your team to spend time trying to find a way to make your invention successful?

A. Yes, sir.

Q. What was that?

A. On September 11th, the Twin Towers were attacked.

Q. And what effect did that have on you and your company?

A. Well, I think probably everybody in this room knows where they were on that day, and shortly after myself and others on the team really started looking for ways that we might be able to prevent future attacks by terrorists.

Q. Did you yourself launch a program for that purpose?

A. Yes, sir.

Q. Tell us about that.

A. Well, we thought that data, the collection of all materials, information -- all information about terrorist activity is that we might be able, through

data mining and software, connect the dots and get indications and warnings that might prevent future attacks, sir.

Q. When did that project get off the ground?

A. We got it started in the November/December timeframe of 2001.

Q. And how did it affect your work schedule?

A. Well, this was for the FBI. And in January, Dr. Vic Larson and myself went full time in the FBI headquarters to integrated prototype using these concepts, sir.

Q. And how long were you located full time in the FBI headquarters working on this anti-terrorism project?

A. About a year.

Q. Was that project a success?

A. Yes, sir.

Q. Now, did your -- the time that you devoted to that project distract you from working on commercializing your invention?

A. Yes, sir. There was some activity, but it definitely put it on the back burner.

Q. You say it put it on the back burner, but even though it was on the back burner, was it part of your job to continue to work on finding an interest in your invention, if you could?

A. Yes, sir.

Q. And did you have some success around that time period?

A. Well, in the summer of 2002, we -- we got interest from SafeNet.

Q. Who is -- or what is SafeNet?

A. Well, SafeNet is a company that developed VPN clients. That's one of the things they did, which what we were interested -- we actually used their product and automated it in one of our early prototypes, so we had a relationship with them. They're very well respected in the security area. So we talked to them about licensing our technology, sir.

Q. And did they enter into a license for your technology?

A. Yes, sir.

Q. Let me show you Plaintiff's Exhibit 134. Is that a copy of the technology license agreement between Science Applications International Corporation and SafeNet?

A. Yes, sir.

Q. What degree -- what rate or amount did SafeNet agree to pay in this agreement?

A. 20 percent.

Q. Was there a cap on that amount?

A. No, sir.
Q. What was your team's reaction to the entry into this agreement?
A. We were pretty excited.
Q. Well, what happened then?
A. SafeNet and -- and I was part of this; I supported them a little bit in this -- talked to -- talked to some other customers, made some contacts and -- but they couldn't get the interest that they wanted.
Q. Okay. Were they going to be required to spend money to develop your invention into a working product?
A. Yes, sir.
Q. And did they decide that they weren't willing to do that?
A. That's correct, sir.
Q. Let me show you Plaintiff's Exhibit 344. What is this document?
A. This is a letter to a Mr. Hendrick, who, as I think I mentioned before, he's in our commercialization group. And they hoped that managed service markets would be favorable and would -- but they hadn't been able to rationalize the capital expenditures to commercialize the product and market the potential.
Q. What was the reaction to this letter back at

SAIC?

A. Yes, sir. Well, the other thing this letter did was return our IP and cancel the license, and we were very disappointed.

Q. Okay. Now, around this same time, though, Mr. Munger, did you meet someone who did believe that they could help make a success of your invention?

A. Yes, sir. One of the people that SafeNet introduced me to was Mr. Kendall Larsen.

Q. Now you've already told us about Dr. Vic Larson, one of the inventors. Is Kendall Larsen related to him in some way?

A. No, sir. They're not related at all.

Q. So what did Mr. Larsen do?

A. Mr. Larsen was very excited about the technology. And in 2004-2005, he approached SAIC, raised some money, and started VirnetX, sir.

Q. How did he raise money for -- to start the company, VirnetX?

A. He went out to friends and family, and there was an investment bank that also located some matching funds.

Q. Now, just to avoid confusion, did you actually think of the name VirnetX?

A. Yes, sir.

Q. And was that a name you were using within SAIC to describe the work on your invention?

A. Yes, sir. In the spring of 2001, that effort, this organization was called VirnetX.

Q. So did SAIC agree to let Mr. Larsen name his company VirnetX when he formed it?

A. Yes, sir.

Q. What was the relationship between SAIC and VirnetX?

A. Well, there was a license arrangement that could lead to the transfer of the patent, and also we -- we could -- we were going to provide some technical support.

Q. Technical support to do what?

A. The technical support was -- it had been awhile since 2001. This is the end of 2005. So we wanted the inventors to come back together, take a look at any changes to the network situation and technology, and propose to him how to go forward to develop a product.

Q. And did you work on that project?

A. Yes, sir.

Q. So, Mr. Munger, when did you first suspect that Microsoft was using your invention?

A. Well, as part of that -- that study that --

that Mr. Larsen asked us to do, he was very interested in securing instant messages -- instant message and voiceover IP.

So we decided to take a look at a live communication server, and one of the engineers that -- when we licensed it and installed it, asked me to come into the lab and take a look at a screen.

And the screen had a box on the screen, and it had a place to enter a domain name, and underneath there was a button which said the TLS, which stands for Transport Later Security.

And because there was only one button and a domain name, it made me suspicious that it looked very automatic and it -- and it was using a domain name.

Q. Did you see anything else that made you suspicious around that time?

A. Well, because of that, I went to the internet and saw in the -- in the public literature on the internet the discussion of mutual TLS VPNs between servers.

And I also saw literature on peer-to-peer (sic) -- I may not be saying that right -- PNRP, that discussed a domain name and the ability for automatic connections using that domain name.

Q. Now, based on what you were able to see with

the live communication server screen and the things that you found on the internet, did you know for sure that Microsoft was infringing your patents?

A. No, sir.

Q. What would you need to see to know for sure?

A. You would really have to take a look at the code, the software code that Microsoft is using.

Q. Is the Microsoft code available for you to look at?

A. No, sir.

Q. Can you go out and buy a copy of it?

A. No, sir.

Q. Can you find it on the internet?

A. No, sir.

Q. Had you ever seen it?

A. No, sir.

Q. But is it your understanding that VirnetX has retained an expert, Professor Mark Jones, who has been allowed to see and study the Microsoft source code?

A. Yes, sir.

Q. And you understand that he will testify about the results of his study later in the trial?

A. Yes, sir.

Q. Now, what did you do about your suspicions?

A. Well, I told -- I told the attorneys at -- at

SAIC that had been supporting the team. I told my management superiors. I told the commercialization group that had -- had worked the relationship with VirnetX. And because I was under contract to VirnetX, I told Mr. Kendall Larsen.

Q. What did SAIC do after you told them your suspicions that Microsoft was infringing the patents?

A. Well, I think they had a couple of independent teams take a look at it, and then they wrote a -- a -- there was a letter written to Microsoft.

Q. Let me show you Plaintiff's Exhibit 120.

MR. POWERS: Your Honor, before we go into this, I'd just like some foundation as to whether this witness was actually aware of this time and involved.

We have no objection to the exhibit, as I had previously advised the Court, but right now, there's no foundation that this witness was involved in the letters in any way at the time.

THE COURT: All right. Proceed.

Q. (By Mr. Cawley) Were you familiar with the effort to try and resolve your suspicions of Microsoft?

A. Yes, sir.

Q. And were you aware that SAIC was going to communicate with Microsoft?

A. Yes, sir.
Q. Send them a letter?
A. Yes, sir. I -- and I -- I saw this letter at the time that it was sent.
Q. Okay. Let's take a look at Plaintiff's Exhibit 120.
MR. CAWLEY: First, go, if you would, please, back to the beginning of the letter.
Q. (By Mr. Cawley) To whom was the letter addressed?
A. It was to Mr. Anoop Gupta.
Q. And who was he?
A. He was a businessman at Microsoft in the Unified Communications Group.
Q. And why was the letter sent to Mr. Gupta?
A. Our desire was to have business discussions --
Q. Right.
A. -- with Microsoft.
Q. Okay.
MR. CAWLEY: So let's go down now to the body of the letter.
Q. (By Mr. Cawley) You see that at the beginning, SAIC indicates to Mr. Gupta that they are writing to introduce an opportunity for SAIC and Microsoft to enter into a mutually beneficial business arrangement in the

pursuit of a premiere service offering in the internet communications market.

Do you see that?

A. Yes, sir.

Q. And did this letter to Mr. Gupta identify your patent?

A. Yes, sir.

Q. And, apparently, just below that, it indicates that a copy of the patent was even sent; is that right?

A. Yes, sir.

Q. And down below we see that it was requested that SAIC would like to contact Mr. Gupta in the next week or so to discuss the possibility of offering Microsoft a license to the '135 patent; is that right?

A. Yes, sir.

Q. And you also see that the letter specifically named Live Communications Server 2005 and Microsoft Office Communicator 2005, correct?

A. Yes, sir.

Q. Now, did Mr. Gupta ever respond to this letter?

A. No, sir.

Q. Did Microsoft respond to this letter?

A. Yes, sir.

Q. Let me show you Plaintiff's Exhibit 121.

Is this a letter that SAIC received back from Microsoft?

A. Yes, sir.

MR. CAWLEY: Let's go down to the bottom.

Q. (By Mr. Cawley) It's not Mr. Gupta who wrote her, is it? Who wrote her back?

A. Their patent counsel.

Q. Mr. Jerry -- looks like Gnuschke, Microsoft's Division patent counsel; is that right?

A. Yes, sir.

Q. And let's take a look at the highlighted portion of this letter.

Did he indicate at the conclusion of his letter: I expect, however, that at some point, we will discuss Microsoft patents, which SAIC must license.

A. Yes, sir.

Q. Did you read this letter when it came in?

A. Yes, sir, I did.

Q. What was your reaction?

A. I found the letter threatening.

Q. Did SAIC send another letter?

A. Yes, sir.

Q. This time to Mr. Gnuschke?

A. Yes, sir.

Q. Let me show you Plaintiff's Exhibit 98.

Is this a letter that was sent back to Mr. Gnuschke in June of 2006?

A. Yes, sir.

Q. And in addition to this letter back to Mr. Gnuschke, did SAIC attempt to call Mr. Gupta, the Microsoft businessman that they had sent the first letter to?

A. Yes, sir.

MR. POWERS: Object, no foundation, unless this witness was involved, Your Honor. The foundation hasn't been laid.

THE COURT: Lay the foundation.

Q. (By Mr. Cawley) Were you involved in discussions about how to contact Mr. Gupta?

A. I received this information from Kendall Larsen, who was having weekly meetings with Ms. Boone, and she -- in those weekly meetings, she was telling him that she was trying to make that contact, and he told me.

So that's the foundation of my knowledge, sir.

MR. POWERS: In that case, Your Honor, I'm going to object to double hearsay and move to strike.

THE COURT: All right. Sustained.

Q. (By Mr. Cawley) What did you decide around

this time, Mr. Munger, had to be done to make your invention a success?

A. We felt that we were going to have to defend our patents so that we had an opportunity to go into the market and compete.

Q. And what were you going to do in order to make that happen?

A. I made the decision with the counsel and with the advice and discussions with managers and both VirnetX and SAIC to move over to VirnetX.

Q. So did you leave SAIC and join VirnetX?

A. Yes, sir, I did.

Q. Why did you do that?

A. I thought that they were going to need more inventors to help them, technically. They did not have a lead technical manager. And also that -- to support whatever was needed to protect our patents, sir.

Q. What is your position at VirnetX?

A. I'm the chief technology officer, and I'm an employee, a member of the Board of Directors.

Q. Do you own stock in the company?

A. Yes, sir.

Q. How much of the company do you own?

A. Approximately 2-1/2 percent.

Q. Around this time, did SAIC decide that it

would re-do its deal or arrangement with VirnetX?

A. Yes, sir.

Q. What were the terms of the new arrangement?

A. The new arrangement was that VirnetX would take the lead in the litigation, and when I came over, the idea at SAIC was that we would still be taking that lead. VirnetX would take the lead.

And there was -- the patents would be transferred over to VirnetX, and there was a rearrangement in the splits of -- of revenue.

Q. And what was that?

A. Is that as a result of settlement or -- or litigation, that VirnetX would get 65 percent, and SAIC would get 35 percent.

Q. And in fact, were the patents transferred, pursuant to this new arrangement, from SAIC to VirnetX?

A. Yes, sir, they were.

Q. And I'll show you Plaintiff's Exhibit 10?

Is this a copy of a filing with the Patent Office that contains copies of the assignments of the patents from SAIC to VirnetX?

A. Yes, sir.

Q. Now, did you -- have you learned that Microsoft eventually responded to that second letter from SAIC?

A. I did, sir.
Q. Let me show you Defendant's Exhibit 3015. Is that the letter from Microsoft?
A. (No response.)
Q. And what's the date of that letter?
A. September 12th, 2006.
Q. So SAIC's second letter was written in June 2006?
A. Yes, sir.
Q. And this letter responding did not -- was not dated until September of 2006, right?
A. That's correct, sir.
Q. Three months later?
A. Yes, sir.
Q. By this time, were you gone from SAIC?
A. Yes, sir. I was gone in July.
Q. Did you ever see this letter before this lawsuit started?
A. No, sir.
Q. As far as you know, did anyone at VirnetX even know about this letter from Microsoft?
A. No, sir.
Q. How has -- how has VirnetX gone about defending its patent rights?
A. It -- it raised money and filed suit for this

trial, sir.

Q. And what became of the rest of the team, your team of inventors?

A. On the following spring, Dr. Bob Short came over, and by the summer, we had two more of the coinventors and a software developer that had been working with us on the project.

Q. So all four of the inventors of one patent now work at VirnetX; is that right?

A. That's correct, sir.

Q. And on the other patent, four of the five inventors work there?

A. Yes, sir.

Q. What about the one who doesn't?

A. He left SAIC around the year 2000, sir.

Q. Now, have you, at VirnetX, continued to work to develop software that uses your invention?

A. Yes, sir.

Q. Why have you done that?

A. There's three reasons.

The first reason is that -- and it's called Gabriel. We'll probably hear a lot about that during the trial here.

Q. Is that the name you've given the VirnetX software that uses your invention, Gabriel?

A. That's right, sir.

Q. Okay. Why have you chosen to continue to develop the Gabriel software?

A. Gabriel software provides a basis for offering a secure domain name service so that people can get domain names and instantly connect by VPNs.

We are talking to companies that may want to license the technology, and the source code is foundation code to allow them to put the capability into their products, if that's worthwhile for them, and also to support this trial.

Q. What do you mean to support this trial?

A. Well, we didn't know that we would -- you know, we had already started the -- the litigation, that we wanted to be able to demonstrate our invention in court.

Q. Is the Gabriel software finished?

A. No, sir.

Q. What stage is it in?

A. It's now in a beta stage, and we have gone out and are having a few people give us advice and -- and -- and test it, sir.

Q. Now, does software like Gabriel have to work on a computer with an operating system?

A. Yes, sir.

Q. What operating system did you choose to design Gabriel to work with?

A. Microsoft Windows.

Q. Why did you make that choice?

A. Ninety percent of the computers in the world are running Windows operating systems, so it was -- it was an obvious choice to want to make sure our product was going to run on the majority of the computers.

Q. And does Gabriel also use something called Microsoft crypto libraries?

A. Yes, sir.

Q. What are they?

A. Well, crypto libraries are software modules that if I put in plain English, like Hi, Mom, it will scramble it, and then bring it back, and you can transmit the scrambled part.

And on the other side, if you use that module on the other side, it will unscramble it, and the Hi, Mom will come out.

Q. And are these crypto libraries made available for the use of software developers who write applications that work on Microsoft operating systems?

A. Yes, sir.

Q. Why did you use them for Gabriel?

A. Well, Microsoft has very good libraries,

crypto libraries, and there was no reason for us to develop our own, so we're using what's available in the Windows operating system, sir.

Q. Have you had any interest in Gabriel?

A. Yes, sir.

Q. Let me show you Plaintiff's Exhibit 977.

What is this document?

A. This is a letter of intent between VeriSign, Incorporated, and VirnetX.

Q. And what is the letter of intent for?

A. We're doing a 90-day study, both technical and business-wise, to look at the opportunity of providing secure domain name services for -- for handheld devices.

Q. Smartphones, for example?

A. Yes, sir.

Q. Who is VeriSign?

A. Well, VeriSign is the company that runs the present domain name service for a dot com, like an amazon.com and dot net and dot org. So they've got a lot of experience in providing that kind of service, and they have an infrastructure that's scaled to do that worldwide.

Q. And when did VirnetX enter into this letter of intent with VeriSign?

A. In December, sir.

Q. December of what year?
A. 2009.
Q. 2009.
A. Yes, sir.
Q. Now, Mr. Munger, do you think that you and your company can ever be successful in selling your invention for internet security while Microsoft is still infringing?
A. No.
MR. POWERS: Objection, Your Honor. There's no foundation that Microsoft is infringing.
THE COURT: Overruled.
Q. (By Mr. Cawley) I'm sorry. What was your answer?
A. No, sir.
Q. Why do you say that?
A. I say that, because if they are infringing, they have the resources to -- to make it very difficult for us to compete.
Q. Thank you, Mr. Munger.
MR. CAWLEY: I'll pass the witness, Your Honor.
THE COURT: All right. Ladies and Gentlemen of the Jury, it's 10 minutes till 3:00. I think we'll take our afternoon break at this time.

We'll be in recess until 4:10 (sic).

COURT SECURITY OFFICER: All rise for the jury.

(Jury out.)

(Recess.)

(Jury out.)

COURT SECURITY OFFICER: All rise.

THE COURT: Please be seated.

I understand there's an issue before we bring the jury in?

MR. POWERS: Yes, Your Honor, there is, and it came up just in the last direct examination.

Mr. Munger referred to two potential demonstrations that Mr. Short was going to give, and one of those we had had notice of and had a chance to do an inspection pursuant to the pretrial order, but one of them we had not. And let me just describe briefly what they are so the issue is framed.

We were told, pursuant to the pretrial order, on time, with no objections, they were going to do a demonstration of the Gabriel software that we've heard about. And we went over and did that inspection.

We were not told that they were going to do a demonstration of the complexity or the attempt to set up some sort of prior art VPN, and that was just

alluded to by Mr. Munger in his testimony about what Mr. Short is intending to do.

And so if there is an intent to do that demonstration, then we would object, because we did not receive notice of it pursuant to the order, had no opportunity to inspect it, and we would object, although they did follow exactly the right procedure as to Gabriel, and we have no objection to that.

THE COURT: All right.

MR. CAWLEY: That was a misstatement by the witness or maybe me, Your Honor. He's not going to demonstrate a piece of software. He's going to talk about an exhibit that is in evidence.

THE COURT: All right.

MR. POWERS: In that case, we don't have a problem.

THE COURT: Okay. And why don't y'all just talk during the break about that. I think that could have been resolved.

MR. POWERS: I would have, but the statement was so clear on the record that it seemed a clear statement of intent, so I thought we should raise it.

THE COURT: All right. Bring the jury in, please.

COURT SECURITY OFFICER: All rise for the jury.

(Jury in.)

THE COURT: All right. Please be seated.

All right, Mr. Powers. You may proceed.

MR. POWERS: Thank you, Your Honor.

May I approach with some exhibits that may be entered?

THE COURT: Yes, you may.

CROSS-EXAMINATION

BY MR. POWERS:

Q. Good afternoon, Mr. Munger.

A. Good afternoon, sir.

Q. I'd like to begin at the part of your testimony where you were describing the work you did with In-Q-Tel to get started on the projects that led to the inventions you patented.

A. Yes, sir.

Q. Now, I believe you testified that In-Q-Tel is what -- is the entity that gave you the initial funding to do the work that led to the patents-in-suit; is that true?

A. That's true, sir.

Q. And In-Q-Tel did that work -- gave you that money, and that was about $3.5 million?

A. Yes, sir.

Q. They gave that you money before you had actually made the inventions, right?

A. That's correct, sir.

Q. All right. Now, you then gave the results of your work to In-Q-Tel for their evaluation, didn't you?

A. Yes, sir.

Q. And you had discussions with In-Q-Tel about what they were -- when they had questions when they were trying to make it work or some question about it, you had some interaction with them during that process, didn't you?

A. Yes, sir.

Q. So you knew they were using the software you delivered.

A. Yes, sir.

Q. All right. Now, they then gave it back to you, didn't they?

A. I'm not clear on that, sir.

Q. All right. In that case --

MR. POWERS: Your Honor, may I approach and hand the witness his deposition?

THE COURT: Yes, you may.

MR. POWERS: Would Your Honor like a copy?

THE COURT: No. That's fine.

Q. (By Mr. Powers) Mr. Munger, do you recall having your deposition taken in this case?

A. Yes, sir.

Q. And a deposition is taken under oath, just like the testimony we're having here in Court.

A. Yes, sir.

Q. Okay. And you recall that we talked about this exact issue in your deposition, about your work with In-Q-Tel, giving them your work, and whether you got it back.

A. Yes, sir.

Q. And you recall you testified that you did get your work -- your box back from In-Q-Tel?

A. That's correct. I did testify at that time that we got it back, sir.

Q. All right. And you have no reason to doubt the accuracy of the testimony you gave under oath in your deposition, do you?

A. I later learned from Dr. Short, who actually did the thing, that he wasn't sure that it came back to us. But that's the only reason that I have some doubt at this point, sir.

Q. But your best testimony that was based on your knowledge was it was returned.

A. I thought it was returned when --
Q. All right.
A. -- I made that statement, sir.
Q. And In-Q-Tel, by virtue of funding the work that you did, got a license to the patents and any patents that would come out of it, right?
A. Yes, sir, they did.
Q. For free, right?
A. Yes, sir.
Q. And you and SAIC went back to In-Q-Tel to ask for further funding, didn't you?
A. Yes, sir.
Q. And In-Q-Tel said no, right?
A. That's correct, sir.
Q. And they said no after they had evaluated the technology you gave them and then returned it, right?
A. Yes, sir.
Q. Okay. Now, based on your discussions with In-Q-Tel, do you recall that they were unhappy with the performance of the technology that you had given them?
A. No, sir.
Q. Well, let's see if we can refresh your recollection.
Do you -- let me first ask you a simple question. Do you know, at In-Q-Tel, someone named Don

Brezinski?

A. Yes, sir. That name is familiar to me.

Q. That's one of the people that you were dealing with there?

A. Yes, sir, I believe so.

Q. And do you know someone at In-Q-Tel named Joy Dorman, a woman named Joy Dorman?

A. That one doesn't ring a bell.

Q. Do you know an Andy Halliday, H-A-L-L-I-D-A-Y?

A. That name is -- that name is familiar to me, sir.

Q. Also, one of the people you were dealing with there?

A. It's likely.

Q. And do you know a Gilman Louie, L-O-U-I-E?

A. Yes, sir, definitely.

Q. Gilman Louie is the President and CEO of In-Q-Tel, right, or was at the time?

A. Was at the time, yes, sir.

Q. Now, do you recall that In-Q-Tel's decision not to re-fund your research was made in the 2001 time period?

A. Yes, sir.

Q. Did you ever hear or learn from anyone that Mr. Louie, the CEO of In-Q-Tel, said the NetEraser

project should be placed in the living dead category or any words to that effect?

A. Not until today, sir.

Q. Did you -- do you recall hearing that Mr. Brezinski, which is B-R-E-Z-I-N-S-K-I, felt the project that you had led did not live up to the expectations? Ever hear anything to that effect?

A. No, sir.

Q. I'd like you to look at Exhibit 31 and 32, DX 31 and 32. It's in the binder I just put in front of you.

You learned of the decision by In-Q-Tel not to fund the continuation of your research. You did learn that, didn't you?

A. Yes, sir.

Q. And that was about the June -- June 2001 time period?

A. Yes, sir.

Q. And is it your testimony that you had no idea what the reason for that decision was?

A. Yes, sir. I had an understanding of why they weren't going to fund it.

Q. If you turn to Page 3 of Exhibit 3132.

MR. POWERS: And, Chris, could you blow up the bottom paragraph, please.

Q. (By Mr. Powers) Let me know when you have that in front of you, Mr. Munger. Do you see that?

The first sentence says Mr. Brezinski and Ms. Dorman commented that the product had not lived up to expectations. This is under the heading of Mr. Halliday giving an overview of the NetEraser project.

Do you see that?

A. Yes, sir.

Q. Did that help refresh your recollection that one of the reasons that In-Q-Tel did not fund the completion of your work was that the technology you had given them did not live up to expectations?

A. No, sir.

Q. You just don't -- you just don't recall one way or the other?

A. Well, I don't -- I never got that kind of negative feedback in my discussions with them, sir.

Q. If you turn to the next page --

MR. POWERS: Chris, could you bring that sentence from Mr. Louie?

Q. (By Mr. Powers) It says: Mr. Louie commented that the NetEraser project should be placed in the, quote, living dead category, close quote, with little or no attention paid to it.

Does that help you recall that you heard something to that effect during the same time period when In-Q-Tel decided not to fund?

A. No, sir.

Q. It is true, though, that just about that time, In-Q-Tel decided -- did decide not to fund your project, right?

A. That's a correct statement, sir.

Q. All right. That's correct or incorrect?

A. That's correct.

Q. Okay. Thank you.

So you know, don't you, that In-Q-Tel and the CIA don't actually use the technology that you gave them.

A. I can't say that for sure, sir.

Q. That's what you believe, isn't it?

A. I -- I really couldn't say, sir.

Q. Well, let's look at your deposition, and look at the April 23 deposition at Page 87. Let me know when you have it.

And I'll read it from Page 87 in your April 23rd deposition, Lines 21 through 24.

QUESTION: Do you know whether any government entity is using the technology developed by SAIC?

ANSWER: I do not know of any government

entity using the technology developed by SAIC.

That was what your testimony at deposition, wasn't it, Mr. Munger?

A. Yes, sir. That's a correct statement.

Q. And it was true then?

A. Yes, sir.

Q. And true now?

A. Yes, sir.

Q. All right. Now, let's talk about your company, your employer at the time, SAIC, and its support of your -- of your project.

Now, you -- you referred in your direct testimony to the CEO of SAIC.

Do you recall that?

A. Yes, sir.

Q. And who's he?

A. Dr. Bob Beyster at the time, sir.

Q. And you made a presentation to the CEO in March of 2000 seeking funding, didn't you?

A. I was one of the presenters, yes, sir.

MR. POWERS: Could you bring up DX3139, please, Chris?

Q. (By Mr. Powers) And let me know when you have it in front of you, Mr. Munger.

A. What was the number again, sir?

Q. 3139.

Do you have it in front of you?

A. Yes, sir, I do.

Q. Great. Thank you.

This is the presentation you were just referring to?

A. That was one of -- one of the presentations, yes, sir.

Q. And it's a presentation that you prepared part of and presented part of, correct?

A. I did not author most of this presentation, sir.

Q. But part of it, you did?

A. It's -- it's likely I could have contributed to it, yes, sir.

Q. Okay. And it's a presentation that you -- that was for, at least in part, requesting funding for your project from Dr. Beyster, correct?

A. Yes, sir.

Q. All right. And if you turn to Page 5 of the document -- and I'll be referring to the -- there's a lot of pages -- page numbers in these documents. I'll be referring to the one in the bottom right-hand corner where it will say -- it will have the exhibit number and then .005 or .05, just because it'll make it easier.

A. Thank you.
Q. Do you have that in front of you?
A. Yes, sir, I do.
Q. Now, if you go to the last bullet --
MR. POWERS: Chris, could you bring that up, please?
Q. (By Mr. Powers) -- this is the description to your CEO about the current environment addressing your proposed technology, right?
A. Yes, sir.
Q. And one of the aspects of the -- of the current environment was that there were a lot of companies addressing the same issue you were going after, and you said, quote, the race is on, exclamation mark, close quote, right?
A. Yes, sir.
Q. So it's true that as of this March of 2000 time period, there were a lot of different companies trying to address the same problem that you were thinking about, and you knew you were in a race with those companies, true?
A. Yes, sir. This -- this timeframe was not necessarily about present technology. It was a year before Beyster's discussions later.
Q. This -- this presentation to him was in March

of 2000, right?

A. Yes, sir.

Q. And the title of this particular page is the current environment, right?

A. Yes, sir.

Q. So your group was trying to convey to your CEO what the current environment was that you were going to be competing against, right?

A. Yes, sir.

Q. And you knew that you were in a race against several other companies addressing the same problem; is that fair?

A. Yes, sir.

Q. Okay. Now, in this document in March of 2000, you asked Dr. Beyster to support and agree to an investment of $7 million in your project, right?

A. I was part of the group that did that, yes, sir.

Q. And the number you asked for was $7 million?

A. I don't know. I'd have to refresh my memory.

Q. Go to Page 26.

A. 26? Thank you.

Q. The page that's called Recommendation. Let me know when you're there.

A. Yes, sir, I see that.

Q. And the recommendation that's included in the box in bold at the bottom is: Commit $7 million of staged investment now, right?

A. Yes, sir.

Q. That's what you and your team were requesting the CEO of your company to agree to, true?

A. Yes, sir.

Q. And Dr. Beyster did not agree to commit that 7 million, did he?

A. That's correct.

Q. In fact, Dr. Beyster and SAIC invested $7 million in Aventail, didn't they?

A. Yes, sir, later.

Q. Now, let's go forward to June of 2001, which is that same -- June of 2001 was the same time period that In-Q-Tel was saying: We're not going to fund anymore.

Do you recall that?

A. Yes, sir.

Q. It was in that same time period that SAIC said, not only we're not going to give you 7 million more dollars, we're going to, quote, pull the plug, close quote. That's true, isn't it?

A. Yes, sir.

MR. POWERS: Could you pull up DX3141,

please.

Q. (By Mr. Powers) Let me know when you have it.

A. I have it, sir.

Q. Okay. Now --

MR. POWERS: First, let's bring up the -- Chris, if you could, the to and the from. Bring that up a little larger so we can see it. Maybe it's just me. That's better.

Q. (By Mr. Powers) The e-mail is dated June 18 of 2001, and it's from a Mr. Edward Hendrick.

Do you see that?

A. Yes, sir, I do.

Q. Edward Hendrick was an SAIC executive, correct?

A. Yes, sir.

Q. And he was the executive involved in the process of deciding whether to commercialize and support the research project you were working on, true?

A. Yes, sir.

Q. In the first paragraph --

MR. POWERS: And, Chris, if you could bring that up, please.

Q. (By Mr. Powers) -- it says: Thought you would like to know that Duane and Don Foley made the decision last week to pull the plug on VirnetX and return to

trying to get additional government funding to continue development of the technology.

Do you see that?

A. Yes, I do, sir.

Q. You were told in this June of 2001 time period, that your company had decided to pull the plug on your project?

A. Yes, sir.

Q. And you knew that the reason for that was the success of one of your competitors, Aventail; is that right?

A. That's one of the reasons, yes.

MR. POWERS: Chris, if you could pull up -- pull up the last paragraph, please. Sorry, the next to the last paragaraph.

And that's just not going to be legible at least to my old eyes, but let's see if I can read it.

Can you make that any larger?

And Chris has that look on his face that means no, so I'll just read it.

Q. (By Mr. Powers) It says: From my perspective, the straw that broke the camel's back was the loss of the ANX beta site as they decided to go with an Aventail solution.

Now, let's -- let's stop there for a

minute and make sure we know who we're talking about. It says ANX beta site. ANX was a company that SAIC owned, true?

A. That's true, sir.

Q. And one of the things that had happened during the discussions with Dr. Beyster and internally within SAIC was the need to get somebody to prove the technology at a beta site, true?

A. True, sir.

Q. And you tried to get a lot of people to serve as that beta site to take your technology and prove that it could work. That's what you were trying to do at the time, right?

A. Yes, sir.

Q. And, in fact, Dr. Beyster, your CEO, specifically said: I'd like that beta site to be ANX, which SAIC owned, true?

A. I'm sorry. Would you repeat that question?

Q. Sure. In addition to you generally wanting beta sites to prove the technology, your CEO, Dr. Beyster, said he wanted you to use ANX as a beta site.

A. Yes, sir, that's correct.

Q. And instead of choosing your technology for the beta site, ANX chose Aventail's, right?

A. That's correct, sir.

Q. And Aventail was a competing technology offering a secure, easy form of internet access, true?

A. Yes, sir, I assume so.

Q. Now, the next sentence after the part I read says, quote, incidentally, SAIC is considering an investment in Aventail.

You knew that at the time, around June of 2001?

A. I didn't know that until it came up as part of the preparation for the trial, sir.

Q. But you did learn that SAIC, in fact, invested $7 million in Aventail in late 2001.

A. That's a correct statement, sir.

Q. And, in fact, that investment in Aventail of $7 million came after 9/11, didn't it?

A. Yes, sir.

Q. So let's talk for just a minute about your attempts to get various types of entities, various types of companies, interested in your technology. You testified about some of this on your direct examination, correct?

A. Yes, sir.

Q. Now, one of the groups that you testified about was a venture capitalist. You testified you met

with about 30 and that none of them agreed to fund your technology.

Do you recall that?

A. Yes, sir, I do.

Q. But did you actually have meetings with them, didn't you?

A. Probably not all 30, but it was a large number, yes, sir.

Q. And you personally helped attend those meetings to give a demonstration of and an explanation of the technology that you thought they should be interested in, true?

A. An explanation, yes, sir.

Q. And after receiving -- and they, at least those that met with you, were interested enough to meet, right?

A. Yes, sir.

Q. And on direct examination, you said, well, it was a horrible time, because there was a recession, and people didn't want to do this type of investment. They were at least interested enough to meet with you and hear what you had to say and hear your explanation of your technology, true?

A. Yes, sir.

Q. But after hearing it, they said no; is that

correct?

A. That's correct, sir.

Q. Now, another avenue, another path that you went down was to try to get companies who would be involved in internet-type transactions interested in potentially using or partnering with your technology, true?

A. Yes, sir.

Q. And you described a few of them. I believe you said Morgan Stanley, eBay, and Amazon, right?

A. Yes, sir.

Q. And there were more than that, weren't there?

A. There could be. I just don't recall the others as much.

Q. There were a large number, weren't there?

A. I don't know how -- what a large -- you know, it could have been twice that number, yes, sir.

Q. Now, when you -- and when you personally went to those companies, you gave an explanation of the technology and how it worked and what it could accomplish and tried to sell it to them, right?

A. Yes, sir.

Q. And each of them said, thank you, but no thank you; is that fair?

A. That's correct, sir.

Q. Now, let's talk about SafeNet for a minute. You -- you testified in your direct examination that SafeNet was interested in your technology in the summer of 2002, true?

A. Yes, sir.

Q. And that they entered into a license agreement and then later terminated it, right?

A. Yes, sir.

Q. Now, you also -- and you said that it terminated because customers weren't interested, and there really wasn't a market for it.

Do you recall that testimony?

A. Yes, sir.

Q. But SafeNet also received your information about your technology, true?

A. That's correct, sir.

Q. And you're aware that SafeNet did a technical evaluation of your technology?

A. I -- I assume that they did, yes, sir.

Q. You knew Mr. Becker at SafeNet?

A. Yes, sir.

Q. And you know that he was a technical person there who was evaluating your technology from a technical point of view?

A. Yes, sir.

Q. And did you learn from Mr. Becker that he was unsatisfied with your technology?

A. No, sir.

Q. Did Mr. Becker ever tell you personally or did you hear from any source that Mr. Becker thought your technology did not make connecting easier?

A. No, sir, I don't recall that.

Q. Now, you testified that SafeNet terminated the agreement, and you showed us the letter which did so.

Do you remember that on direct examination?

A. Yes, sir.

Q. And SafeNet did so at the time when it had a right to terminate without paying SAIC any money, true?

A. That's correct, sir.

Q. So despite the 20 percent that you testified about, SafeNet actually paid nothing; isn't that right?

A. That's correct, sir.

Q. And they did that after they evaluated your technology, true?

A. Yes, sir.

Q. Now, you also testified, I believe, that you met a man by the name of Kendall Larsen. Let's talk about him a bit.

Did you first meet him in connection with a SafeNet discussion or a SafeNet-related discussion?

A. Yes, sir, I did.

Q. And at that time, Kendall Larsen -- and I'll say Kendall Larsen to distinguish him from other Larsons that are in this case -- Kendall Larsen was at a company called Phoenix, true?

A. That's correct, sir.

Q. And you went to Phoenix to make a presentation to try to get them interested in your technology, true?

A. Yes, sir.

Q. And they said thank you, but no thank you?

A. That's correct, sir.

Q. And immediately thereafter, Mr. Larsen left Phoenix and went to a company called Osprey Ventures, true?

A. Yes, sir.

Q. And asked you to come in and make a presentation to Osprey to try to get them interested in funding your proposal, right?

A. Yes, sir.

Q. And they said thank you, but no thank you; is that fair?

A. That's fair, sir.

Q. All right. So in this summer of 2001 time period when In-Q-Tel had decided not to fund --

A. (Sneezes.) Excuse me.

Q. Bless you.

When In-Q-Tel had decided not to fund your project and SAIC had decided to pull the plug, at that point, SAIC tried to work its government connections to get funding, true?

A. Yes, sir.

MR. POWERS: And, Chris, if you could put up from the opening Page 11.

Q. (By Mr. Powers) Is this a fair summary of the government entities to which you tried to get interest in your technology?

A. I can certainly verify all, and I don't remember the FAA, but it's -- that's a possibility, also.

Q. So at least in terms of what's on Page 11, you recall trying to get the CIA, Homeland Security, the FBI, OSIS, and DARPA all interested in your technology and -- is that true?

A. That's correct, sir.

Q. And they all said no?

A. That's correct, sir.

Q. And they said no despite the fact that SAIC has very good connections with those agencies, true?

A. Yes, sir.

Q. It works with those agencies on a regular

basis, and that's its primarily business, is the federal government, right?

A. Yes, sir.

Q. And they said no despite the fact that the government has a free license to your patents, true?

A. Yes, sir.

Q. Now, the FAA -- let's just look at that briefly.

MR. POWERS: Could you bring up 3525, please. DX3525. I think that's the wrong exhibit.

Could you bring up DX3268. 3268.

Let's bring up the first page, please, Chris, and blow that part up.

Q. (By Mr. Powers) Mr. Munger, is Exhibit 3268 is a typical type of presentation you were making to these government agencies?

A. Yes, sir, it is.

Q. You used pretty much the same presentation for each one of them?

A. With variation, yes, sir.

Q. Okay. And your primary pitch to each of these government agencies, the argument you made to try to sell them, was that you could have easy, fast, secure internet access for their use, true?

A. Yes, sir. That was one of the key aspects

that we presented.

Q. And they all said no?

A. Yes, sir, they said no.

Q. Now, with respect to Kendall Larsen for a moment, after he moved from Phoenix to Osprey, he then moved from Osprey to being on his own, right?

A. Yes, sir.

Q. And that was the point at which he was trying to raise money to start what became the company VirnetX, not the technology VirnetX; is that fair?

A. Yes, sir.

Q. All right. Now -- and Mr. Larsen became the CEO of VirnetX once it was formed?

A. Yes, sir.

Q. And there was a period of six months to a year when VirnetX was formed as a company and Mr. Larsen was running it where you weren't at VirnetX; you were still at SAIC, true?

A. That's true, sir.

Q. Okay. Let's talk about -- well, one other prior art technology that you described in your direct examination was https.

Do you recall that?

A. Yes, sir.

Q. Now -- and you said that htp -- https is

what's typically used when we do a credit card swipe at the grocery store or at Wal-Mart, true?

A. I -- I don't know that for sure, but it's possible, yes.

Q. That's your understanding, isn't it?

A. I -- I don't know how the swipe machine works at Wal-Mart, sir.

Q. Well, but you do understand that https is the standard way that commercial financial transactions are protected around the internet. I believe that's what you testified on your direct examination; is that right?

A. I -- I know https from a client to a browser to order a book on a server. I don't know other uses in the back end of business.

Q. All right.

A. But I do understand that, sir.

Q. That's fair enough. So let's take that example.

So if you were going to amazon.com and ordering a book, you understood that that transaction, when you give the credit card number, et cetera, was treated by https, true?

A. True.

Q. That https is easy. You don't have to do anything. You just plug in your credit card and say

order, right?

A. Yes, sir.

Q. Very easy, very fast.

A. Yes, sir.

Q. And secure, right?

A. Yes, sir.

Q. Now, let's go back in time to 1998. And you testified on your direct examination that you had this idea, and you wrote this paper called Aladdin in August of 1999.

Do you remember that testimony?

A. Yes, sir, I do.

Q. Now, in fact, you had actually gone to a DARPA meeting in February of 1998 on this subject, security on the internet, hadn't you?

A. No, sir.

Q. You had not? All right. So let's talk about that.

MR. POWERS: Let's bring up Exhibit 3418, DX3418.

Q. (By Mr. Powers) Let me know when you have it in front of you, Mr. Munger.

A. That's 3148?

Q. 3418.

A. Oh, I'm sorry. I apologize. I have it, sir.

Q. This is a DARPA information assurance principal investigators' meeting in February of 1998 in Annapolis, Maryland?

A. Yes, sir.

Q. And Annapolis is very near your house, isn't it?

A. Yes, sir, that's correct.

Q. You went to this particular meeting, didn't you?

A. No, sir.

Q. You were aware of this meeting, though, weren't you?

A. No, sir.

Q. Do you recall submitting a proposal to DARPA that related to the discussion of this meeting?

A. No, sir.

Q. Let's look at the proposal.

Now, could you look at Exhibit DX3541? Let me know when you have it.

A. I have it, sir.

MR. POWERS: Chris, let's bring up the very first -- just the part at the top. Perfect.

Q. (By Mr. Powers) Now, let's make sure we understand what the terminology means.

Information Assurance BAA Outline. Do you see

that?

A. Yes, sir, I do.

Q. You know what that means, don't you?

A. Yes, sir.

Q. BAA Outline is an organization related to DARPA that you submit proposals to for funding?

A. Yes, sir.

Q. And Exhibit 3541 is an internal SAIC draft of a response to a request by DARPA for proposals for funding, right?

A. Yes, sir.

Q. And so this is an internal draft that you had some role in preparing?

A. Yes, sir.

Q. And so the point of this was to submit something to DARPA that would ask them to get funding for your NetEraser project, fair?

A. That's correct, sir.

Q. Now, let's talk about DARPA for a minute. DARPA stands for Defense Advanced Research Projects Agency?

A. That's correct, sir.

Q. So this is an agency designed to fund development of technology that might be useful for the government, particularly, the Department of Defense?

A. Yes, sir.

Q. And DARPA is very involved in the internet, aren't they?

A. Yes, sir.

Q. And internet security?

A. Yes, sir.

Q. Now -- and the proposal that you were seeking funding for was your NetEraser project. You wanted funding from DARPA as part of that, right?

A. Yes, sir, the address hopping.

Q. Now, when you were preparing this proposal, one of the -- there's an outline that you have to follow that DARPA gives you, and you have to fill -- fill in responses throughout, true?

A. That's correct, sir.

Q. So if you could turn to Exhibit 3541 to Page 6.

MR. POWERS: And, Chris, if you could pull up Section J that starts in italics all the way down to the last bullet underneath it. Let's just look at that.

Q. (By Mr. Powers) Let me know when you have it.

A. Yes, sir.

Q. So just to orient ourselves, J is Demonstration and Immigration Plan, the part in italics,

and then it says: Offerors should describe how their results could be integrated with solution other than IA contractors currently developing or are likely to develop -- facilitating systematic approaches to the large capabilities described above.

That part in italics is the part in the DARPA form that you have to respond to, fair?

A. Yes, sir.

Q. All right. And the part underneath that, which are all the little bullet points, those are drafts that you and your group created that would be responsive to that point; is that correct?

A. Yes, sir.

Q. And the second bullet down says, quote, what about the DVPN effort?

Do you see that?

A. Yes, sir.

Q. Now, that refers to dynamic virtual private networks, doesn't it?

A. Yes, sir.

Q. So you knew in September of '98 about the dynamic virtual private network, didn't you?

A. No, sir.

Q. Even though you put it in this form to DARPA?

A. That's correct, sir.

Q. So you put it in the form, but you didn't know anything about it.

A. Very little about it.

Q. But you knew it was a competitor that was already on the market in '98.

A. No, sir.

Q. But you knew enough about it to use its right initials, didn't you?

A. Yes, sir. The -- there was a list of programs that we had to say we were willing to work with to do demonstrations, and so we were going to list it, and I wrote a question mark, because I probably didn't understand what it was about when I found on their program list.

Q. So that statement, what about the DVPN effort, that was actually your question that you put in?

A. Yes, sir, I believe I wrote that.

Q. And someone answered that question, didn't they, in a later draft?

A. To -- enough to put it -- I can't -- I can't remember our response, but we probably listed programs we were willing to work with, yes, sir.

Q. Would you look at DX3038, please.

A. 3038?

Q. 3038.

MR. POWERS: Let's bring up the first whole part of it.

Q. (By Mr. Powers) Do you have that in front of you Mr. Munger?

A. Yes, sir I do.

Q. 3038 is a later internal SAIC draft response to DARPA following up on what we just looked at, which was DX3541, right?

A. Yes, sir.

Q. And if you go to that same spot -- it's on Page 14 this time.

MR. POWERS: Let's bring up Section J again, please, Chris.

Q. (By Mr. Powers) Let me know when you're there, Mr. Munger.

A. I'm there, sir.

Q. So you have the same boilerplate sort of form section of demonstration and integration plans, true?

A. Yes, sir.

Q. And now we have a later draft, internal, written by SAIC, you and your team, about how to respond to that section, correct?

A. Yes, sir.

Q. And, again, the second bullet down starts off with what about the DVPN effort, which is the same text

that we saw in the prior exhibit, true?

A. Yes, sir.

Q. But now it's filled in. BBN is doing. We are not willing to give this to them. Leave it unsaid, question mark.

Did you write that as well?

A. I can't recall, but it's very possible that I wrote that, sir.

Q. So you knew that BBN -- a company called BBN was doing DVPN, right?

A. Yes. I probably discovered that they were one of the contractors in that other DARPA program.

Q. So you knew that something called dynamic virtual private networks was being actually used by a company called BBN, right?

A. Yes, sir.

Q. And you knew that BBN was a competitor of yours.

A. Yes, sir.

Q. Now let's turn to Exhibit 3107, please, in front of you. Let me know when you have it, Mr. Munger.

A. I have it, sir.

Q. Thank you.

This is the final submission that you gave to DARPA requesting funding, right?

A. Yes, sir, it looks like it.

Q. And if we go down to Section J -- this time it's at Page 32 of the final text.

Do you have that in front of you?

A. Yes, sir, I do.

Q. The actual final text of your response in Section J runs about a full page, doesn't it?

A. Yes, sir.

Q. And you don't mention DVPN, the dynamic virtual private network, or BBN's use of it, do you?

A. No, sir.

Q. And that was the suggestion that you had made in the last draft, leave it unsaid, right?

A. We probably didn't feel it was necessary.

Q. It wasn't -- you thought it wasn't necessary even though the whole point of this question is how you're going to work with other technologies that DARPA might use, right?

A. Yes, sir.

Q. That is the question DARPA's asking you in Section J, how will you work with other technologies we're using, right?

A. Yes, sir.

Q. And you knew that DARPA was working with DVPN.

A. Yes, sir, that's one of their programs.

Q. So dynamic virtual private networks, you knew was prior art in 1998, being a program within DARPA. You knew that.

A. No, sir, I did not know that it had any prior art.

Q. Well, you knew it was before your invention. This is '98. You haven't had that magical train ride yet coming back from New York, right?

A. That's correct, sir, but I did not know any of the underlying technology in those programs -- that program.

Q. But you knew it was being used by a competitor of yours in the same field for network security. You knew that.

A. Knew what was being used, sir?

Q. DVPN.

A. The program name?

Q. Yes.

A. Yes. There was a program named DVPN, yes, sir.

Q. Okay. So let -- now let's talk about Aventail.

You also knew that Aventail, as a product, existed before your patents, true?

A. No, I don't know that, but I have heard that

Aventail had a product out before ours today, sir, yes, sir.

Q. And you don't deny that, do you?

A. No, sir, I don't deny that.

Q. Now, you concluded that ANX was going to be close to your patent claims if it was using Aventail, didn't you -- didn't you?

A. I think I made a statement about 14 months before 2000 -- the summer of 2001 in an e-mail that said that, yes, sir.

Q. Let's look at DX3339.

A. That was 33 --

Q. 3339.

A. I'm sorry. I'm hearing 3330 --

Q. 3339.

A. I've got it now, sir.

Q. Okay. Is Exhibit 3339 an e-mail that you wrote in May of 2000?

A. Yes, sir. I've got no reason to believe that that isn't an e-mail from me.

Q. And you write this to Bob Short, Vic Larson, Doug Schmidt, and Thomas Swartz, right?

A. Yes, sir.

Q. And the subject line says: It's NetEraser and ANX, true?

A. That's true, sir.

Q. And this is at a time when you're trying to get ANX to be a beta site for your technology, right?

A. No, sir. This is well before then.

Q. And yet you say, quote, it sounds like ANX is getting very close to touching on our patent claims in DNS, Gif, right?

A. Yes, sir, I said that.

Q. Now, you testified earlier that you were aware that SAIC, after denying your request for $7 million, did invest $7 million in Aventail in 2001.

Do you recall that?

A. Yes, sir, I do.

Q. Let's fix the date on that.

MR. POWERS: It will be DX3174.

Actually -- I'm sorry -- it's 3474.

A. I thought I was losing it.

Q. (By Mr. Powers) No. I can't read my own handwriting sometimes.

A. 3470?

Q. 3474.

A. I don't seem to have it, but we can proceed, if it's important.

Q. If you don't have it, I'll give you mine.

MR. POWERS: May I approach, Your Honor?

THE COURT: Yes, you may.

A. Thank you.

Q. (By Mr. Powers) Does this help refresh -- does Exhibit 3474 help refresh your recollection about the timing of SAIC's investment of $7 million in Aventail, that it was October of 2001?

A. No, sir. I -- I'm afraid that I -- this is something that I only learned in preparation for this trial, sir.

Q. But you did know it was post 9/11, that you know.

A. I can look at this date and see that, yes, sir.

Q. Now, you had earlier testified that one of the things that made it hard for you to get money was that in 2001, there was a recession.

Do you recall that?

A. Yes, sir.

Q. But that recession didn't prevent SAIC from investing $7 million in Aventail, did it?

A. No, sir.

Q. And you also testified that one of the problems you faced was that 9/11 caused a re-focus of your energies within SAIC to different areas, true?

A. Yes, sir.

Q. But SAIC, post 9/11, still invested $7 million in network security with Aventail even after 9/11.

A. That's correct, sir.

Q. All right. Now, another technology that you were aware of was a technology called PPTP, true?

A. I know the name, yes, sir.

Q. And it's Pointe2Pointe Tunneling Protocol?

A. Yes, sir.

Q. And you knew that that existed before your work on their NetEraser.

A. That's correct, sir.

Q. And you knew that that was a say of setting up a VPN automatically. You knew that?

A. No, sir, I didn't.

Q. You know that now, don't you -- don't you?

A. I heard your -- your opening, and you say that they have an automatic approach. That's the first time I've heard that, yes, sir.

Q. So in all of your investigations of the prior art and the state of the technology that you testified on direct examination, you didn't look at PPTP and how it worked?

A. No, sir, we didn't.

Q. Now, another technology that pre-dated your work was one called SSL, right?

A. Yes, sir.

Q. And that's another way of providing network security before your work on NetEraser; is that true?

A. Yes, sir, that's true.

Q. Let's talk for a minute about what happened when you left SAIC and moved to VirnetX.

That was in the summer of 2006, correct?

A. July 2006, yes, sir.

Q. All right. And when you did so, Kendall Larsen was the CEO of VirnetX at that time, right?

A. Yes, sir.

Q. And still is today?

A. That's correct, sir.

Q. And Kendall Larsen is also Chairman of the Board of VirnetX?

A. Yes, sir.

Q. So he's your boss.

A. Yes, sir.

Q. And he had been directing -- Kendall Larsen had been directing the technical efforts of VirnetX before you arrived; is that fair?

A. That's -- that's correct, sir.

Q. And one of the technical efforts that you became aware of when you joined VirnetX was VirnetX's work with a company called Magenic.

Do you recall that?

A. Yes, sir.

Q. Magenic was another different company that VirnetX had hired to do some technical work on your NetEraser technology, right?

A. Yes, sir.

Q. And Magenic was working with a Microsoft product at that time, the Live Communication Server.

A. Yes, sir.

Q. And the purpose of that work, as you learned it from Mr. Larsen, was to modify Microsoft's Live Communication Server in order to add the VirnetX patented technology to it, right?

A. No, sir.

Q. Would Mr. Larsen know that better than you since he was directing it?

A. He probably -- he might have.

Q. All right. Well, Mr. Larsen will testify later, and we'll get his testimony.

Now, the objective of the Magenic work, though, was to try to implement your patented technology. That was the objective, wasn't it?

A. That's -- that's a correct statement, sir.

Q. So let's look at DX3536. Let me know when you have it.

A. I have it, sir.

MR. POWERS: Bring up the first, oh, six, seven lines. That's perfect.

Q. (By Mr. Powers) This is a work order between VirnetX and Magenic, and it's in 2006 --

A. Yes, sir.

Q. -- before you arrived?

A. Yes, sir.

Q. And so this is one of the things Kendall Larsen, VirnetX's CEO, was managing and running before you arrived?

A. Yes, sir, that's correct.

Q. Have you ever seen this document before?

A. I don't recall it, no, sir.

Q. Let's look at the next page and see if it helps you recall.

MR. POWERS: There's a section, Chris, on Page 2 that starts: Goals, deliverables, work plan, and schedule. And let's take that all the way down to the bullet points that are the second set of bullet points.

Oh, it's going to be hard to read, isn't it?

Q. (By Mr. Powers) Can you read that, Mr. Munger?

A. Yes, sir.

Q. Okay.

MR. POWERS: And can the jury read that? It's a little far off.

I will read it in the record so that it's clear.

Q. (By Mr. Powers) Under project goal, it says, quote, the goal of the project, in short, is to come up with a solution for encrypted secure communication stream between multiple messaging end points.

This will be accomplished by implementing a first phase of a wheel-and-spoke architecture with VirnetX at the center, connecting different corporate architectures. This needs to be accomplished using as simple a method as possible while utilizing VirnetX's patents.

Do you see that?

A. Yes, sir.

Q. Do you understand that that was the goal, the Magenic project, before you arrived, or is that just something we have to rely on Mr. Larsen for?

A. This is almost a surprise to me, sir.

Q. So Kendall Larsen is the person who can answer that?

A. Yes, sir.

Q. All right. Do you -- did you ever have a discussion with Kendall Larsen as to why he was

attempting to modify Microsoft's Live Communication Server and Office Communicator in order to use the VirnetX patented technology?

A. There was no discussion about modifying a Microsoft application.

Q. Well, you weren't there.

A. With me. The answer to that specifically with me, sir.

Q. I'm talking about the period before you arrived.

Did you ever ask Mr. Larsen, Kendall Larsen, or did he tell you why he was trying, before you arrived, to modify Microsoft's Office Communicator and Live Communication Server in order to use VirnetX's patented technology?

Did you hear anything from him about the reason for that?

A. I'm looking for the word modify, but there was no discussion about modify, sir.

Q. And those two products, Microsoft Office Communicator 2005 and Live Communication Server 2005, you understand that those are two products, which in this lawsuit, VirnetX is saying infringed VirnetX's patent back then.

True?

A. That's true, sir.

Q. And yet you have no explanation for why Mr. Larsen, Kendall Larsen, is trying to modify those products in order to use the VirnetX patents; you just don't know.

Is that fair?

A. I'm sorry. I still have a problem with the word modify.

But he had an effort to provide security platforms for those, and that's -- that's my understanding of what was going on.

Q. But you really don't know the answer, because we'd have to ask Mr. Larsen for that?

A. I think so, yes, sir.

Q. All right. Now, let's talk a little more about Gabriel. Actually, one quick question before we get there.

On direct examination, you testified about a company called Cambridge Strategy Management, right?

A. Strategic, yes, sir.

Q. Strategic management. Sorry.

And that was a company that SAIC hired to tell them whether there was a business opportunity out there in this space, true?

A. That's correct, sir.

Q. Cambridge Strategy Management -- or Strategic Management didn't actually assess the quality of your software and decide that that specific software had that value, did it?

A. No, sir.

Q. All right. Now, let's move, then, to Gabriel. In your direct examination, Mr. Cawley asked you why did you continue development of Gabriel after you came to VirnetX.

Do you recall that question and your answer?

A. Yes, sir.

Q. And you gave three answers, three reasons, the first being so that you could have a secure domain name service product, right?

A. Yes, sir.

Q. The second being to support licensing?

A. Yes, sir.

Q. And the third would be to support this litigation?

A. That's correct, sir.

Q. In fact, weren't the priorities and the reasons exactly the reverse in that order?

A. No, sir.

Q. Do you recall -- you say you remember the Board of Directors, right?

A. Yes, sir.

Q. And the Board of Directors actually addressed this precise issue, didn't they?

A. Yes, sir.

Q. Would you look at 3161, please, Exhibit 3161?

Tell me when you have it. Do you have it in front of you?

A. Oh, yes, sir. I'm sorry.

Q. All right. Exhibit 3161 is a presentation to the Board of Directors in March of 2008 of VirnetX, right?

A. Yes, sir.

Q. That's after this litigation started, over a year after, right?

A. Yes, sir.

Q. And you're a member of the Board of Directors at this time, weren't you?

A. Yes, sir.

Q. And if you turn to Page 22 of the document, there's a page that -- the title is Gabriel Technology Thrust Objectives.

Do you see that?

A. Yes, sir.

Q. Now, the first stated purpose or objective is to support IP licensing.

Do you see that?

A. Yes, sir.

Q. In fact, Gabriel has not been licensed to anyone, has it?

A. No, sir.

Q. The second stated purpose, which you had put last in your testimony, was embody patented methods to support litigation.

That's the same way you're referring to it here, wasn't it?

A. Yes, sir.

Q. And the third and last here, but your first, was prepare technical product for providing direct product and services to the public as appropriate.

Do you see that?

A. Yes, sir.

Q. So as of March of 2008, in terms of the listing for Gabriel and Gabriel's objectives, having a real product was third and last and only as appropriate.

True?

A. No, sir.

Q. Is that not what it says?

A. Oh, let me read what it says.

Yes, sir.

Q. Now, within VirnetX, you understood that the

purpose -- the primary purpose, actually, of the work you were doing on Gabriel was to support this litigation?

A. No, sir.

Q. You didn't?

Did you ever hear inside VirnetX the Gabriel software being referred to as, quote, vaporware, close quote?

A. No, sir.

Q. Never heard of it?

A. No, sir.

Q. Do you know what the phrase vaporware means?

A. Yes, sir.

Q. It means software that doesn't really exist, that's just sort of appear to be software but doesn't really exist.

Is that fair?

A. Yes, sir. That's a fair estimate in my definition.

Q. Would you look at Exhibit 3260, please.

Let me know when you're there.

A. I'm there, sir.

Q. Exhibit 3260 is an internal e-mail within VirnetX, isn't it?

A. Yes, sir.

Q. It's from a man named Gordon Warren to you and other people in July of 2008, correct?

A. Yes, sir.

Q. July 2008 is a few months after the Board meeting we just looked at in March of 2008, right?

A. Yes, sir.

Q. And Gordon Warren is an engineer at VirnetX, isn't he?

A. Yes, sir.

Q. He's one of the people who's actually working in the Gabriel software, right?

A. Yes, sir.

Q. And what he says is: Vic, group-shmoop -- with my apologies to the court reporter, that's S-H-M-O-O-P -- it's all vaporware, with a little smiley face at the end.

Do you see that?

A. Yes, sir.

Q. Now, you received this e-mail from Mr. Warren.

A. Yes, sir. I'm an addressee on it.

Q. So you knew that Mr. Warren in July of 1998 (sic) was saying as to Gabriel, it's all vaporware?

A. No, sir.

Q. Well, the subject of this e-mail is file registry -- file share registry change working on

Gabriel software, right?

A. Yes, sir.

Q. All right. And you know Mr. Warren was working on Gabriel at the time; that was his primary job, right?

A. Yes, sir.

Q. And he's saying it's all vaporware?

A. I think he might be referring to some aspect of the file share registry, which is not our total code, sir.

Q. Okay. Now, when you were working on Gabriel for VirnetX, you did nothing to determine whether Gabriel will infringe somebody else's patents, do you?

A. Would you repeat the question?

Q. Certainly.

You're working on Gabriel as a possible product, true?

A. Yes, sir.

Q. That's what you just said.

And you don't do anything to decide -- to figure out whether Gabriel would infringe somebody else's patents, do you?

A. No, sir. I haven't done that.

Q. And VirnetX doesn't have a policy of asking anyone to do that, does it?

A. There's no written policy like that, no, sir.
Q. Or unwritten policy, is there?
A. Not that I know of, yes, sir.
Q. Now, let's look at Exhibit DX3259, please.
Let me know when you have it.
A. I have it in front of me, sir.
Q. Exhibit 3259 is an e-mail from you to Vic Larson, one of your co-inventors, and Bob Short, one of your co-inventors, and others in November of 2007, right?
A. Yes, sir.
Q. And you're addressing a user's guide for Gabriel as of -- in November of 2007, right?
A. Yes, sir.
Q. And you attached that user's guide that you had reviewed and worked on, true?
A. That's true, sir.
Q. And one of the things this user's guide does is stipulate the sign-in procedure when the developers are going to work on Gabriel software, right?
A. That's correct, sir.
Q. So if you personally went to go work on the software or when anyone else did, they would have to log in to Gabriel using a password that had bene selected for that purpose, true?

A. Yes, sir. It was actually to download the -- this was part of it, to download the software.

Q. And if you look at Page 13 of the document, this is -- this is the actual Gabriel user's guide draft as it exited in November of 2007?

A. Yes, sir.

Q. Which you attached to your e-mail?

A. Yes, sir.

Q. Now --

MR. POWERS: Chris, if you could pull up from the text in between the two boxes all the way down to the box -- to the last box.

Q. (By Mr. Powers) This was the log-in screen that was used in the Gabriel development software at that time, right?

A. Yes, sir. For about a two-week period, that's a correct statement.

Q. And we've all used log-in screens where you have to type in a user name and then a password, and that's what you did in this process?

A. Yes, sir.

Q. And you personally logged in more than once to this process using this password and user name?

A. Maybe twice, yes, sir.

Q. And others on the team did as well?

A. Yes, sir.
Q. And the user name that you used was VirnetX, right?
A. Uh-huh.
Q. The name of the company?
And the password that was selected was MS$42009? (sic), question mark, correct?
A. Yes, sir.
Q. MS stood for Microsoft, didn't it?
A. Yes.
Q. $4 meant are we going to get money from Microsoft?
A. That's correct, sir.
Q. And 2009?, question mark, was stating when you hoped to get money from Microsoft?
A. That's correct, sir.
Q. So your password that your development team used for Gabriel was, are we going to get money from Microsoft in 2009?
A. That's correct, sir.
Q. And is it still your testimony that the primary purpose of Gabriel wasn't linked to this litigation?
A. That's a correct statement, sir.
Q. Despite the fact that the password was

directly linked to this litigation?

A. Yes, sir.

Q. All right. Let's talk about the dates on which you had the ideas for the claimed inventions that are in this case.

You understand that's a concept that we're calling conception?

A. Yes, sir.

Q. Have you heard that term before?

A. Yes, sir.

Q. And conception is when you have the idea for what you later claim to be your invention?

A. Yes, sir.

Q. Now, did you ever tell Kendall Larsen what those dates were for those patents-in-suit?

A. I can't remember.

Q. Let me show you Exhibit DX3428.

Let me know when you have it.

A. 3428, I have it, sir.

Q. Exhibit 3428 is a set of answers that VirnetX gave under oath to questions that Microsoft asked them in this litigation.

Do you understand that?

A. Yes, sir.

MR. POWERS: Your Honor, at this point,

would it be appropriate to have the Court instruct the jury what an interrogatory is, or I can ask the witness the question but --

THE COURT: Yes, I can do that.

Ladies and Gentlemen -- or Ladies of the Jury, an interrogatory is a written question that is sent to the other side during the course of the pretrial proceedings where they provide a sworn answer to those questions.

You may proceed.

MR. POWERS: Thank you, Your Honor. If we can dim the lights again. Thank you.

Q. (By Mr. Powers) Now, one of the questions that we asked VirnetX -- that Microsoft asked VirnetX was Question 6, which starts at Page 5 of the document.

Let me know when you're there.

And it says: Separately, for each claim of each of the patents-in-suit, state the date in which the claimed inventions were conceived.

And you understand that's a question of when you had the idea, right?

A. Yes, sir.

Q. All right.

MR. POWERS: And, Chris, why don't you bring up the last -- let's bring up the whole -- the

whole answer to that.

Q. (By Mr. Powers) The whole first paragraph is a bunch of objections, and the last paragraph is the answer, and it says: VirnetX responds that the inventions claimed in all of the patents-in-suit were conceived no later than September 23, 1999.

Do you see that?

A. I see that, sir.

Q. And September 23rd, 1999 is the date of that train ride that you testified about in direct examination, right?

A. Yes, sir.

Q. Now, if you go two pages in, to No. 9, you see that the person who verifies that those answers are true is Kendall Larsen.

Do you see that?

A. Yes, sir, I do.

Q. Now, Kendall Larsen wasn't actually with you on that train ride, was he?

A. No, sir.

Q. He doesn't know of his personal knowledge when any of the inventions were made, does he?

A. No, sir.

Q. He wasn't there.

A. He wasn't there.

Q. So did you tell Kendall Larsen the information that he verified under oath that all the inventions were made in September of 1999?

A. No, sir.

Q. In fact, the statement in Exhibit 3428 that all the inventions and all the claims were conceived no later than September 23rd, 1999, that's not true, is it?

A. I don't believe that's true.

Q. In fact, one of the claim requirements for the '135 is a secure target website, right?
'135 patent, if you want to look at that, I'd be happy to get it.

A. I beg your pardon, sir?

Q. Do you need the patent in front of you to do that?

A. Yeah. You're looking at the '135?

Q. The '135.

A. I can probably pull it up.

Q. The '135 patent was in the original binder being used with Counsel at Exhibit 3, I believe.
Yes, Exhibit 3.

A. Well, I've also got it at 120, but there's another copy that's here in a couple of places.

Q. There's a lot of copies of that patent in this courtroom.

A. Yes, sir.

Q. So using Exhibit 3, which is the one that used in your direct examination, what -- what are the requirements of the claims -- and let's just take, for example, Claim 10 -- is a secure target website. Sorry. Claim 1.

A. Claim 1, sir?

Q. Yes. If you look at Claim 1 --

MR. POWERS: Let's bring it up.

Q. (By Mr. Powers) -- do you see secure target website down there in the middle of the third step? It's highlighted on the screen if you -- if you want --

A. Yes, sir. I see Claim 3 on this -- Step 3 in Claim 1, yes, sir.

Q. And that step in Claim 1 of the '135 patent includes a requirement of this secure target website?

A. Yes, sir.

Q. Now, that concept of a secure target website had not been conceived as of September of 1999, right?

A. Yes, sir. With that definition, the triggering was looking for secure target website.

Q. Let me make sure I understand your testimony.

Are you saying that, yes, secure target website was conceived on September 23rd, 1999?

A. It was -- it was conceived -- the only thing

that was conceived on the 23rd was the revelation of the triggering using DNS.

Between then and the time we applied for this patent, there would have been a continuing unfolding of the methods necessary to put in a patent.

Q. So let's be -- let's make sure the testimony is clear.

You said the only thing that was conceived on September 23rd was that secure DNS; the rest came later?

A. I would think that -- again, there might have been a couple of things, but I would think that the bulk of the methods and our understanding of how to do it would have evolved over the next three months, yes, sir.

Q. And when you say would have evolved over the next three months, you mean were not conceived on September 23rd, 1999?

A. That's correct, sir.

Q. All right. And so as to the bulk of the '135 claims, Mr. Larsen's sworn statement in the interrogatory response was not true?

A. That's correct, sir.

Q. All right. And it's also not true for the '180 patent, is it?

A. Going back to the 23rd?

Q. Right.

A. Yes, sir, that's also correct.

Q. All right. Now, Victor Larson, not Kendall Larsen now -- Victor Larson was one of your co-inventors at SAIC, correct?

A. That's a correct statement, sir.

Q. And one of the things that you and Victor Larson and Bob Short discussed, three -- three of the inventors, was the relationship between the technology called SIP and your technology, right?

A. There were discussions about it, yes, sir.

Q. And could please tell the jury what SIP is?

A. Session Initiation Protocol.

Q. And Session Initiation Protocol is a technology that you understand or thought was being used by Microsoft, true?

A. Yes, sir.

Q. All right. Now, could you turn to Exhibit 3257, please?

Let me know when you have it.

A. All right, sir.

Q. Exhibit 3257 is a collection of two e-mails within SAIC in the November of 2005 time period, right?

A. Yes, sir.

Q. And you were still at SAIC at this time, as was Victor Larson and Bob Short?

A. That's correct, sir.

Q. And if go -- then there's two e-mails here.

MR. POWERS: Let's bring up, please, Chris, first the bottom one.

Can the jury see that one? The type is a little hard to see, okay?

I can't see it on the screen either, so I'll read it.

Q. (By Mr. Powers) First, Mr. Munger, you were copied on this e-mail from Bob Short in November of 2005, weren't you?

A. Yes, sir.

Q. And the subject of the e-mail is SIP Secure.

Do you see that?

A. Yes, I do, sir.

Q. Now, you know that SIP Secure referred to the use of SIP, which is this Session Initiation Protocol, plus an additional type of technology, for example, TLS or SSL?

A. Yes, sir.

Q. And TLS and SSL are just two different ways of doing -- making a communication secure, right?

A. Yes, sir.

Q. And you didn't invent those and you don't claim that those infringe, do you?

A. It's not clear that they infringe or not.

Q. You don't have an opinion that they do. You haven't concluded that, have you?

A. No. I have not looked into it, sir.

Q. Okay. Now, Mr. Short, your co-inventor, says to you and others in November of 2005, quote, I find myself losing the bubble on what distinguishes us from SIPS.

Do you see that?

A. Yes, sir.

Q. So, Mr. Short, your co-inventor, is saying to you, I can't figure out why we're any different or better than this SIP Secure, true?

A. That's what the e-mail says, yes, sir.

Q. All right. And if we go to the e-mail above it, it's an e-mail from Victor Larson, your co-inventor, back to Bob Short, responding to his earlier e-mail, right?

A. Yes, sir.

Q. And Victor Larson, one of your co-inventors, says, quote: I did not come away from the Thursday/Friday meetings with a strong feeling that our patent provided any amount of protection against reasonably secure approaches for SIP, parens, i.e., TLS, close parens, close quote.

Do you see that?

A. Yes, sir.

Q. So that's your co-inventor saying our patents don't protect against that technology, SIP plus TLS, true?

A. Yes, sir, he had a strong feeling.

Q. Okay. And you didn't write back to him saying, well, no, our patents do cover that, did you?

A. No, sir.

Q. All right. And you understand that the products you say infringe here use SIP plus TLS.

A. I understand that, yes, sir.

Q. The very same products that your co-inventor said your patents don't protect are the same products which are now -- you're saying do -- are covered by the patent.

A. That's what we're saying, yes, sir.

Q. Okay. Now, let's talk a little bit about Kendall Larsen.

He -- at VirnetX, he's the person who negotiates the key contracts, isn't he?

A. Yes, sir.

Q. Including licenses or anything else. That's part of his job.

A. Yes, sir.

Q. And at this point, all of the attempts that have been made at VirnetX to license either the patents or the technology has not resulted in any license, true?

A. Yes, sir.

MR. POWERS: Pass the witness, Your Honor.

THE COURT: All right. Redirect?

MR. CAWLEY: Thank you, Your Honor. Just a few questions.

REDIRECT EXAMINATION

BY MR. CAWLEY:

Q. Mr. Munger, let's talk about this password, MS4$2009, question mark, that you showed us in Defendant's Exhibit 3259.

What document was that in again?

A. That was in a first attempt to try to set up what steps you take to install Gabriel software and download the domain name into that software.

Q. Is that an internal document to VirnetX, or did it go out into the world?

A. Well, sir, there was only five of us that would have seen that document.

Q. And was that document written and who used that password in that document?

A. Dr. Vic Larson told me that he did that

password.

Q. Okay. So he put that password in there, didn't send it to anybody outside the company.

Was the lawsuit already filed by then, this lawsuit?

A. Yes, sir.

Q. And was this lawsuit at that time set for trial, not now but in the year 2009?

A. Yes, sir.

Q. How many employees are there at VirnetX?

A. There's 12 employees.

Q. Twelve employees.

And would you say that they -- at the time Mr. Larson used that password were all anxious about how this lawsuit is going to turn out?

A. Very.

Q. How long was that password in that document?

A. Maybe two weeks.

Q. Two weeks.

You testified, when I was asking you questions before, about your delivery of the NetEraser prototype to In-Q-Tel and the CIA. And I asked you if you knew whether or not the CIA had actually used your invention.

Do you remember that?

A. Yes, sir.

Q. And you said, I believe, you didn't know one way or the other.

A. Yes, sir.

Q. Then on cross-examination, you were just shown some deposition testimony where you said you didn't know if the CIA was using your invention; isn't that right?

A. That's correct.

Q. Is that inconsistent in any way in your mind?

A. No, sir.

Q. You don't know if they're using it, and you don't know if they're not. Is that the truth?

A. That's the truth, sir.

Q. Okay. You were asked some questions about several different kinds of prior art, https, DVPN, and Aventail.

First of all, you told us before that you helped work on your patents. So are you generally familiar with the phrase prior art?

A. Yes, sir.

Q. And do you understand that prior art means something that was written about or used or existed before a certain date?

A. Yes, sir.

Q. So it doesn't really tell you anything about whether a particular technology used your idea just

because it's, quote, prior art, does it?

A. No, sir.

Q. Well, let's talk about the things that you were -- were asked about that were called prior art, meaning only that they were around before your invention.

You testified that https was fast and secure, but would it have solved the needs of the CIA?

A. No, sir.

Q. Why not?

A. Because it only went from a client to a server and wasn't flexible enough to route to other machines, sir.

Q. All right. You were asking about a piece of prior art called DVPN.

Do you remember that?

A. Yes.

Q. You were asked several questions about that.

And do you remember this morning that Microsoft's lawyer in the opening statement told this jury that in February of 1998, there was a meeting in Annapolis, Maryland, hosted by DARPA, where DVPN was discussed?

Do you remember that?

A. Yes, sir.

Q. And do you remember that Microsoft's lawyer told this jury that you were at that meeting?

Did you hear that?

A. Yes, sir.

Q. Mr. Larson, is that true?

A. Well --

Q. Mr. Munger, is that true?

A. I was not at that meeting, sir.

Q. Are you confident about that?

A. Yes, sir.

Q. Have you had an opportunity within today to review an attendee list for that meeting?

A. Yes, sir, I did.

Q. And is that list a Defendant's exhibit marked by the Defendants as an exhibit in this case and admitted into evidence, Exhibit 3011?

A. Yes, sir.

Q. Is your name on that list?

A. No, sir.

Q. Another piece of prior art you were asked about is Aventail.

Do you know if ANX was using Aventail in May of 2000?

A. No, sir.

Q. And a few minutes ago, you were asked a lot of

questions that would seem to be trying to get you to agree that Mr. Larsen at VirnetX had tried to modify the Microsoft Live Communications Server product.

Do you remember that?

A. Yes, sir.

Q. Let's go over that again, because I know you testified about it in your direct examination.

Was there a period of time when Mr. Larsen had formed the company VirnetX, but you still worked at SAIC?

A. Yes, sir.

Q. And did he hire you and SAIC to do something?

A. Yes, sir.

Q. What did he hire you to do?

A. He hired us to recommend to him a -- how to technically develop a product that had been updated from our previous experience.

Q. And what would that product work with?

A. It would work with any application.

Q. And, specifically, did you explore the possibility, on behalf of VirnetX, of it working with Microsoft Live Communications Server?

A. Yes, sir.

Q. Were you going to modify the Live Communications Server?

A. No, sir.

Q. Were you instead going to make a product that would work along with it to provide automated security?

A. That's a correct statement, sir.

Q. But in the course of exploring the possibility of doing that, what did you begin to suspect?

A. I began to suspect that what Magenic was doing -- this is after I got there -- that they -- they weren't making progress and they might not have understood technically the right approach to go forward with, sir.

Q. All right. And, finally, Mr. Munger, you testified both on the questions I asked you, and then you were asked about it again by Microsoft lawyers, that you approached venture capitalists about raising money for your invention and they said no.

You approached co-developers about co-developing, and they said no. SAIC said no. Various government agencies said no.

Mr. Munger, in the face of all that, do you still believe in your invention?

A. Yes, sir.

Q. Can you explain?

A. What -- what this is going to provide is an easy way for any machine to connect to any other machine

safely. And I also think that the market is now here with handheld smart phones that are becoming computers that we have on our hip; people are going to reach to their homes; that this is -- it's finally become a technology whose time has arrived.

MR. CAWLEY: No more questions, Your Honor.

THE COURT: Thank you. Any recross?

MR. POWERS: Nothing further, Your Honor.

THE COURT: All right. Thank you.

You may step down, Mr. Munger.

All right. Ladies and Gentlemen -- Ladies of the Jury, it's going to take me a while to break that habit this week.

It's 20 minutes till 5:00. I think we're going to go ahead and recess for the day. We'll start back in the morning at 9:00 o'clock. So get a good night's rest tonight.

Please try to be here a few minutes before 9:00 so that we can get started, hopefully, promptly at 9:00.

Please remember my instructions this evening. Don't discuss the case among yourselves or with anyone else. Don't make any independent investigation. Don't read anything, if you should see

anything in a newspaper or on television.

So you are recessed at this time. You can go to the jury room and head on to your homes.

COURT SECURITY OFFICER: All rise for the jury.

THE COURT: All right. Members of the Jury, if you would, please be sure to leave your notebooks and your notepads in the jury room. The court security officer will secure all those and get them back to you tomorrow.

(Jury out.)

THE COURT: All right. Very well.

Is there anything further from the Plaintiffs?

MR. CAWLEY: No, Your Honor.

THE COURT: From the Defendants?

MR. POWERS: No, Your Honor.

THE COURT: All right. We're going to be in recess. It's 4:40. I'm going to ask everyone to remain in the courtroom for about five minutes and allow the jury to get to their cars to the elevators ahead of you.

So, Ms. Ferguson, you're in charge as far as dismissing everyone.

Be in recess.

COURT SECURITY OFFICER: All rise.

(Court adjourned.)

* * * * *

CERTIFICATION

I HEREBY CERTIFY that the foregoing is a true and correct transcript from the stenographic notes of the proceedings in the above-entitled matter to the best of my ability.

/s/_____ _____
SUSAN SIMMONS, CSR Date
Official Court Reporter
State of Texas No.: 267
Expiration Date: 12/31/10

/s/_____ _____
JUDITH WERLINGER, CSR Date
Deputy Official Court Reporter
State of Texas No.: 731
Expiration Date: 12/31/10

EXHIBIT F3

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX	*	Civil Docket No.
	*	6:07-CV-80
VS.	*	Tyler, Texas
	*	
	*	March 9, 2010
MICROSOFT CORPORATION	*	9:00 A.M.

TRANSCRIPT OF JURY TRIAL
BEFORE THE HONORABLE JUDGE LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPEARANCES:

FOR THE PLAINTIFFS: MR. DOUGLAS CAWLEY
MR. BRADLEY CALDWELL
MR. JASON D. CASSADY
MR. LUKE MCLEROY
McKool-Smith
300 Crescent Court
Suite 1500
Dallas, TX 75201

MR. ROBERT M. PARKER
Parker, Bunt & Ainsworth
100 East Ferguson
Suite 1114
Tyler, TX 75702

APPEARANCES CONTINUED ON NEXT PAGE:

COURT REPORTERS: MS. SUSAN SIMMONS, CSR
Ms. Judith Werlinger, CSR
Official Court Reporters
100 East Houston, Suite 125
Marshall, TX 75670
903/935-3868

(Proceedings recorded by mechanical stenography, transcript produced on CAT system.)

APPEARANCES CONTINUED:

FOR THE DEFENDANT:
MR. MATTHEW POWERS
MR. JARED BOBROW
MR. PAUL EHRLICH
MR. THOMAS KING
MR. ROBERT GERRITY
Weil Gotshal & Manges
201 Redwood Shores Parkway
5th Floor
Redwood City, CA 94065

MS. ELIZABETH WEISWASSER
MR. TIM DeMASI
Weil Gotshal & Manges
767 Fifth Avenue
New York, NY 10153

MR. DANIEL BOOTH
Weil Gotshal & Manges
700 Louisiana
Suite 1600
Houston, TX 77002

MR. RICHARD SAYLES
MR. MARK STRACHAN
Sayles Werbner
1201 Elm Street
4400 Renaissance Tower
Dallas, TX 75270

MR. ERIC FINDLAY
Findlay Craft
6760 Old Jacksonville Highway
Suite 101
Tyler, TX 75703

* * * * * *

P R O C E E D I N G S

(Jury out.)

COURT SECURITY OFFICER: Please rise.

THE COURT: Please be seated.

All right. I understand the parties have

a matter or two before we bring the jury in.

MR. SAYLES: Yes, Your Honor. If it please the Court, Dick Sayles for Microsoft.

Your Honor, this afternoon a witness to be called is Mr. Brett Reed, who is the Plaintiff's damages expert. I'll be cross-examining him.

And one of the issues related to his testimony is some approximately 80 exhibits to which Microsoft cannot agree to admissibility.

And, Your Honor, in keeping with the -- the spirit of how matters such as this are handled in this district, we have agreed in every respect where we can agree.

We're not asking that they establish a business records predicate or any sort of a thing like that. These objections to these particular exhibits go to the -- the heart of their damage model.

And the nature of the exhibits is the same objections that I brought forward in the motion to strike Mr. Reed and -- and that was denied at pretrial, and -- and the motion in limine and the motion concerning the entire market value, and those were all denied.

And having the experience of -- of been around for a while, I know that a pretrial ruling of

that nature doesn't preserve anything. Microsoft is very intent on preserving its position and its objections with regard to these particular damages that it believes are irrelevant financial data not tied to the demand for the technology at issue.

The -- the problem is that there are some 80 of these. And if they were handled one by one and tendered by the Plaintiff and objected to on a one-by-one basis, it would obviously take a long time to do that.

I have spoken with Jason Cassady for the Plaintiff at some length. We have prepared lists of the exhibits that they intend to tender in evidence. And when they do, we have written out what our objections to those exhibits are. And we in no way wish to diminish the importance of those objections.

We do not wish to waive those objections, but we do want to suggest to the Court or discuss with the Court a convenient and realistic manner in which to handle those important objections to these exhibits.

And similarly, the Plaintiffs have properly disclosed to us last night demonstratives that they intend to use with Mr. Reed. And as you might imagine, those demonstrative aids are based upon the underlying documents to which we object, and, therefore,

we have the same objection to those demonstratives. And we have prepared numbered sets of those. And I don't think this morning is necessarily the time to go into this in great detail, although if that were the Court's wish, we're prepared to.

But I wanted to speak with the Court this morning to offer as a possible solution that the Plaintiff has agreed that they will tender their exhibits in a written list to which we have our written objections, which we can provide to the Court in advance of this afternoon and obtain a ruling.

There are only two exhibits which we have separated out of that that have unique, special objections to them. And those would not take long.

But I wanted to bring that up with the Court, because I expect we want to move this case along. And when we get to Mr. Reed this afternoon, I know that Your Honor will want to keep things moving. And so that's the issue.

And if -- if the Court would indulge us and permit us to handle it in a manner that I have suggested, we'll work together to do that.

THE COURT: And you're basically wanting to make a record on these; is that --

MR. SAYLES: I definitely want to make a

record. We do -- we would really, of course, like you to sustain our objections.

I will say, as I argued in the pretrial motions, our objections go to the heart of their damage model, and we do want to make a record. I mean, it's not like we want to make a record and, therefore, I am not intent and serious about the objections.

But, yes, we do want to make a record. That's correct.

THE COURT: Response?

MR. CASSADY: Your Honor, Mr. Sayles correctly stated that these are all subject to motions that were filed, either motions to strike or motions in limine that the Court has already ruled on in the Plaintiff's favor.

We have no objection to putting these exhibits in -- in a list format, such as Mr. Sayles suggested, so that the Court can rule on these in groups and, hopefully, alleviate the burden of running through these 80-some-odd exhibits on a one-by-one basis.

In general, I'll just state for the Court, these are documents such as licenses, Microsoft's financial data, and summaries of that financial data.

So as Mr. Sayles said, this does go to the core of VirnetX's damages case, and I think the

rulings that the Court has already made on the motions to strike and motions in limine go straight to these documents.

MR. SAYLES: Indeed they do, Your Honor. But as I say, I've learned the hard way that that doesn't preserve anything.

THE COURT: Right. I think what I would like to do on these is when we get to Dr. Reed or before -- even before we get to him, I'd like to just hear a little bit of testimony and get a little deeper into what these documents are. The Court is aware of the -- I think it's Resneck -- ResNet (sic) case out of the Fifth Circuit.

MR. CASSADY: ResQNet.

THE COURT: ResQNet, yeah, that's it. That -- and I'd like to hear a little argument on that. And I understand Judge Folsom has a new opinion out. Anyway, I'd just like to just delve into it a little deeper and give it -- give it one more look. And I'll consider your objections at that time.

MR. SAYLES: All right.

THE COURT: And I might give the jury a little extra time for lunch today, and we might -- might -- we can probably do it in 30 minutes, don't you think?

MR. SAYLES: Yes, Your Honor, I do think so.

MR. CASSADY: I have no problem with that, Your Honor.

MR. SAYLES: And, Judge, if I may, this is just for my personal information.

I'm going to be handling this witness, and, naturally, if there are objections when the witness is testifying in front of the jury, I will make the objections.

But with regard to presenting Your Honor with legal arguments outside the presence of the jury related to the admissibility of these documents, may I have assistance from my team in doing so?

THE COURT: Yes, you may.

MR. SAYLES: All right.

THE COURT: All right. What else before we bring the jury in?

MR. BOBROW: Just a brief matter, Your Honor, if I may.

First of all, we have reached agreement with the Plaintiff on the further admissibility of four more exhibits for Defendant's exhibit list.

If I may --

THE COURT: Can we just bring those up in

front of -- we'll take those up in front of the jury once they come in.

MR. BOBROW: All right. And then the second issue is, is that last night we filed a bench memo on the Dynamic VPN issue.

As you've heard, Dynamic VPN, Microsoft's prior art in this case that invalidates these patents, we have been unable to meet and confer process to resolve the Plaintiff's objections to a number of Dynamic VPN exhibits.

My sense is, is that there will be testimony on Dynamic VPN probably on Wednesday or Thursday of this week, and we simply wanted to alert the Court to that; number one, that we filed that memo and, number two, that it will need to be resolved as that evidence, we hope, will be coming in in our case.

THE COURT: All right. We'll take that up either late this afternoon or perhaps in the morning.

Remind me about it again at the end of the day.

MR. BOBROW: Thank you, Your Honor.

THE COURT: Anything further?

MR. McLEROY: Your Honor, when should we offer our list of exhibits that were admitted?

THE COURT: As soon as the jury comes in,

I'll give you an opportunity to do that.

Anything further?

MR. CAWLEY: No, Your Honor.

THE COURT: All right. Bring the jury in, please.

COURT SECURITY OFFICER: All rise for the jury.

(Jury in.)

THE COURT: Please be seated.

Good morning, Ladies of the Jury. Ready to get going?

All right. Very well.

Mr. Cawley -- let's see. Yes, Mr. Cawley, you may call your next witness.

MR. CAWLEY: Thank you, Your Honor. Do we want to introduce the exhibits first?

THE COURT: Yes. We will do exhibits first. Does Plaintiff have any additional exhibits to offer this morning?

MR. McLEROY: No additional exhibits, Your Honor, but we do have a list of the exhibits admitted yesterday for the Court.

THE COURT: Okay. Very well.

MR. McLEROY: May I approach?

THE COURT: You may provide those to,

Ms. Ferguson. Thank you for preparing that.

MR. McLEROY: You're welcome.

THE COURT: Does Microsoft have any exhibits it wishes to offer?

MR. POWERS: Yes, Your Honor. We have, I believe, four that we wish to offer this morning as to which there's no objection. We have a similar list as to what was admitted yesterday.

May I approach?

THE COURT: Now, the similar list you have, are those the exhibits that were admitted yesterday?

MR. POWERS: Exactly.

THE COURT: Okay. Now, what are the four exhibits you wish to offer today.

MR. BOBROW: Thank you, Your Honor.

The four exhibits are Defendant's Exhibits 3032, 3066, 3253, and 3577.

THE COURT: Okay. Any objection?

MR. McLEROY: No, Your Honor, I don't believe we do.

THE COURT: All right. Be admitted. All right. And you may bring the list up, Mr. Powers.

MR. POWERS: Thank you, Your Honor.

THE COURT: All right. Mr. Cawley, you

may call your witness.

MR. CAWLEY: Thank you, Your Honor.

As this next witness, the Plaintiff, VirnetX, would call to the stand Dr. Bob Short.

THE COURT: All right.

MR. POWERS: Your Honor, may I approach with the --

THE COURT: Yes, you may.

ROBERT D. SHORT, III, Ph.D., PLAINTIFF'S WITNESS, PREVIOUSLY SWORN

DIRECT EXAMINATION

BY MR. CAWLEY:

Q. Would you please introduce yourself to the jury please, sir?

A. My name is Robert Dunman Short, III.

Q. Mr. Short, I want to make sure that we are able to hear all of your testimony, so I think, as we've seen from yesterday, don't get too close to that microphone, or it starts making popping noises. But please make sure you're speaking more or less into it.

Why are you here?

A. I'm one of the co-inventors on the patents in this case.

Q. What did you invent?

A. We invented a way to make it much easier for

the average user to have a safe connection on the internet.

Q. Is your invention important?

A. Yes, sir, I believe it is.

Q. Why do you say that?

A. There's lots of information going across the internet. Some of it is not very important. A lot of it is very important. People's bank account information, credit card information, family pictures. And there's a lot of bad people out there trying to get that information and -- and use it.

Q. So are you listed as an inventor on the two patents in this case, along with Mr. Munger, that we heard from yesterday?

A. Yes, sir.

Q. And were there others on your team who were also inventors?

A. Yes, sir.

Q. Who were they?

A. We had Dr. Vic Larson and Mr. Mike Williamson and Dr. Doug Schmidt.

Q. Okay. Which of those people worked for this company, the Plaintiff in this lawsuit, VirnetX?

A. Four of the five. There's Gif and myself and Vic Larson and Mike Williamson.

Q. Well, will your other inventors be here to testify in Court?

A. No, sir.

Q. Why is that?

A. We had pretty limited time, so I think that's the reason.

Q. All right. Where do you live?

A. I live in Loudon County, Virginia, outside of Washington, D.C.

Q. Are you married?

A. Yes, sir. 32 years now.

Q. Okay. And is your wife here?

THE COURT: Mr. Cawley, excuse me. This might be a good time for me just to explain to the ladies of the jury that prior to trial, both sides gave me an estimate of how much time they thought the case would take. And then I told them -- arrived at an amount of time, a number of hours that they had to present their case.

So both sides are operating under some time constraints, which will make the trial shorter for you and, hopefully, keep them more focused. But when the witness referred to a shortage of time, I wanted you to understand where that came from.

So each side's operating under that same

constraint.

Excuse me, Mr. Cawley. I just wanted to get that in.

MR. CAWLEY: Thank you, Your Honor. I appreciate that clarification.

Q. (By Mr. Cawley) You say you're married. Is this your wife here with you in the Court today?

A. Yes, sir.

Q. And you have children?

A. We have four children and two grandchildren.

Q. Did you go to college?

A. Yes, sir.

Q. Could you tell us about the schools that you went to and the degrees that you got?

A. I started my -- my education at Virginia Tech. I studied electrical engineering. Received a degree in 1974, a bachelor's degree.

I stayed there for another year of study in applied mathematics, received a master's in applied mathematics there.

Then I went on to Purdue University, which is in Indiana, and studied electrical engineering, where I received a Ph.D. in 1978.

Q. So you got your doctorate or your Ph.D. in 1978?

A. Yes, sir.

Q. So at that time, I guess, at least as people refer to it in your field, you became Dr. Short.

What did you do after you got your Ph.D.?

A. I went to a company called Sperry Corporation in Massachusetts.

Q. What kind of company was Sperry?

A. Sperry was a multi-division company that had a fairly broad area that they worked in. For example, they had one division that did sonar systems for submarine warfare, radar systems. And there's another one you may have heard of, Sperry-Univac, which is one of the very early computer-makers.

And then there was Sperry New Holland -- you may have heard of that -- which made farm equipment.

Q. What did you do at Sperry?

A. My first project at Sperry, I was at the Corporate Research Center, and I was working on some advanced methods for detecting, identifying, and tracking Soviet submarines.

Q. Soviet submarines?

A. Yes, sir.

Q. How long did you stay at Sperry Corporation?

A. That was till -- about nine years, I believe.

Q. Nine years?

What did you do after you left Sperry?

A. I went to a company called ARCO Power Technologies.

Q. What does ARCO do?

A. ARCO you may know better as Atlantic-Richfield. It's an oil and gas company, and they had a subsidiary called ARCO Power Technologies that I worked for.

And what we did, we were working on some pretty advanced radar techniques for looking over the polar cap for incoming Soviet ballistic missiles. This was during the Cold War.

Q. So you were developing radar systems that would detect Soviet missiles in the event of an attack?

A. Yes, sir.

Q. Now, is it fair to say that your work at both of these companies, Sperry and ARCO, had mostly military applications?

A. Yes, that's right.

Q. When did you leave ARCO?

A. I left ARCO probably in the mid-'90s, '95 to '96, maybe '97. I'm not sure. Somewhere in that range.

Q. Okay. And where did you go to work?

A. I went to a company called SAIC.

Q. All right. And that's the -- what's the full

name of that company?

A. Science Applications International Corporation.

Q. And that's a company that Mr. Munger already worked at by the time you joined it, correct?

A. Yes, sir.

Q. Did you meet Mr. Munger for the first time at SAIC?

A. That's correct.

Q. Why did you decide to leave ARCO and go to work at SAIC?

A. SAIC was really a very interesting company. It was employee-owned. It was founded by a nuclear physicist. Their management was all very technical and just very good, very talented. It was an exciting place to go, and I decided to go there.

Q. What did you begin doing? What kind of projects did you begin working on at SAIC?

A. The first project was a secure satellite communication system supporting the Global Hawk program.

Q. Now, we heard -- I guess you didn't hear yesterday, because you weren't in the courtroom when Mr. Munger testified. But the rest of us heard testimony from Mr. Munger yesterday about the Global Hawk project. Is that the unmanned aircraft that was used -- or at

least conceived, initially, to deal with scud missiles?

A. Yes, sir.

Q. What did Mr. Munger do on that Global Hawk project?

A. Gif was the chief architect, which meant that he -- he kind of -- he kind of worked on the -- whoops -- excuse me -- on the high-level concepts and architecture of what the system ought to look like and what the system ought to do.

Q. What did you do?

A. I -- I was system engineer and detail design for this -- this secure satellite communication network that we created.

Q. Now, you mentioned satellite communication. We heard yesterday from Mr. Munger that the satellites that the Global Hawk communicated with were not owned by the military but were public or commercial satellites; is that correct?

A. Yes, sir, that's correct.

Q. Was this unusual for a military project?

A. This -- this was definitely something that was new at that time period, yes, sir.

Q. Did it create some particular challenges?

A. Yes, it did.

Q. What -- what were they?

A. Well, you know, prior to that time, military used something called Mil SatCom, which they owned all those assets. They secured all -- all those satellites. So things were secured by the military.

When they started using the public or the commercial satellites -- these are the same kind of satellites that TV comes down on and that kind of thing -- you had to worry about securing information that was coming across the satellites, because anybody could listen in on those, and if you didn't have some mechanism of -- or some way of securing them, then the bad guys could intercept your communications.

Q. And were you able to solve this challenge for the Global Hawk project?

A. Yes, sir, we did.

Q. Was Global Hawk a successful project?

A. It was very successful.

Q. Is it used today?

A. Yes, it is, sir.

Q. And did members of your team at SAIC actually play a role on the ground?

A. Yes, sir. There were members of my team -- this was back not long after 9/11, when they went into Afghanistan, and then went into Iraq. We had members of our team take our system out and set it up and operate

it to help the soldiers.

And they were able to get real-time pictures of the battlefield and actually save -- saved lives with it.

Q. Now, Dr. Short, was your experience with Global Hawk important in leading to the inventions in this case?

A. Yes, sir, it was.

Q. What was the next project you became involved with at SAIC after Global Hawk?

A. This was a project that came to be known in the early days as NetEraser.

Q. NetEraser?

A. Yes, sir.

Q. And what did Mr. Munger do? What was his role on that project?

A. Well, he was our chief architect again, serving a similar role as he did in the Global Hawk where he was looking at kind of high-level concepts and ideas and how to put the thing together and what it -- how it should work.

Q. Sounds like what you're trying to say, Dr. Short, is that Mr. Munger would think of some ideas, then you were stuck with making it work.

Is that about it?

A. Yes. We've had that relationship for almost -- I don't know -- 20 years now maybe.

Q. And is that the role you played on the NetEraser project?

A. Yes, sir.

Q. Who was the NetEraser project for?

A. This was done for a company called In-Q-Tel, which was set up by Congress -- and I believe this was in the opening statements -- to help the CIA identify emerging technologies that -- to promote commercialization of those technologies in a way that would support the CIA's mission.

Q. And what in particular did the CIA need you to help them do?

A. Well, they were looking for ways to provide really secure communication between their -- their agents and their operatives out in the field back through to either the home office or regional offices, and be able to do that across the internet in a way that couldn't be detected or couldn't be intercepted.

Q. All right. Dr. Munger (sic), you -- you've have just taken us up -- Dr. Short -- sorry.

A. That's all right.

Q. You've just taken us up to the NetEraser project, and you've just described for us the need that

the CIA had to be able to compute and communicate safely over the internet.

But right now, before we go on with that story, I'd like you to help us understand better some of the things that we've already heard about in the case and some of the things that we're going to be hearing about when we continue your story about how you came up with that invention.

So tell us, please, what is the internet?

A. Well, I brought some pictures that will help that.

Q. Okay.

A. This is kind of a simple example of how most users interact on the internet or with the internet. And most users, they've got a computer in their home at their kitchen desk, table, or, you know, they have a laptop that they're connected to the internet.

They may be in an internet cafe with a laptop even, but they're sitting at their computer. And they want to access information that's on the internet. Maybe they're shopping on the internet; maybe they're doing online banking. But they're trying to access information and interact generally with another company, companies on the internet, quite often.

So they're -- they're going through this cloud

here.

Q. Let me -- let me -- excuse me for interrupting you.

A. Yes, sir.

Q. -- Dr. Short, but I want to make sure we understand what we see on the screen.

The thing in the upper left that's labeled remote user, what is that a picture of?

A. This is -- this is the user's computer.

Q. That's -- that's supposed to be a laptop computer like several of them that we see around the courtroom?

A. Can be a laptop, can be a desktop in the kitchen.

Q. Okay. On the far right lower corner, what is that gray box?

A. This down here is what's often referred to as a server computer or a data server. It's generally setting at some company. Like if you go in to shop at JC Penney's, they'll have these data servers where you're actually going and getting information.

Q. Okay. So the thing in the lower right is also a computer but a different kind of computer?

A. Yes, sir.

Q. Does it have a screen usually?

A. Normally not.

Q. Okay. So -- so it doesn't -- it's not a computer that people sit down and look at things on the screen and type on a keyboard?

A. That's correct.

Q. And in the middle you've got something labeled internet that looks like a cloud. Why have you drawn a cloud there?

A. Well, people generally put a cloud there because -- my hand is shaking; I'm sorry. I have this -- I lost my mouse.

You have to pardon my hand shake. I have this hereditary problem.

They -- generally, what really the internet is all about is, there's a very large number of computers, and they're interconnected with communication lines of some form -- wires or fibers or something -- that really make up the internet.

Q. Now, you've -- you've drawn a whole bunch of little computers inside what we first saw as the cloud; is that right?

A. Yes, sir.

Q. Is there a particular name for what most of those computers are?

A. Well, these are -- these are routers, what are

called routers.

Q. Routers?

A. Yes.

Q. And what is a router?

A. A router is a special computer that is designed to help to send information across the internet. And what they do is a router has multiple communication paths coming into it. And so information will come in from one side, and the router will look at, well, where's that supposed to go?

And based upon where it's ultimate destination is, it will decide what's the best path to send it from here? And then it will forward it along that path to the next router.

And that router basically does the same thing until, ultimately, it gets to its final destination.

Q. Now, I see that you've drawn the router computers in your picture as having screens or monitors.

In fact, do routers usually have screens or monitors?

A. Routers do not, no, sir.

Q. Why have you drawn these little computers with screens?

A. Well, I put screens on them, because it makes them look like computers. I mean, most of us think of

computers having a screen. And so it's just more natural.

Q. Where -- where are these router computers located?

A. These are located throughout the country. For example, there will be a router in this courthouse somewhere that these computers are connected to across a radio link.

And then the router in this courthouse is then connected through some -- some internet service provider connection to a router at that provider, and then that provider has a router connected to another router. And so it just kind of spreads out.

Q. In fact, not only all over the country but all over the world?

A. That's right.

Q. Who owns the internet?

A. Well, no single person on organization owns the internet. It's -- it's owned by a very fairly large number of organizations, people that -- that operate collaboratively in a way where they interconnect with each other.

And so you'll have -- you'll have information being sent from one person -- or one organization's router will go to another organization's router to

ultimately get it to the destination it's supposed to go to.

Q. Now, Dr. Short, when someone wants to send a message over the internet, how does the internet know where that message is supposed to go?

A. They use something called a -- let's see if I can get over here -- something called an IP address.

Q. What's that?

A. An IP address, as you see down here in the -- in the lower right, is a -- on the internet is a four-digit sequence. It's unique to that computer's location on the address. So every computer's public ad -- excuse me; sorry -- public address on the internet has a very unique sequence of four numbers.

Q. So every -- every computer hooked up to the internet has its own number?

A. Yes, sir.

Q. Well, if -- if a user wants to use the internet, though, to send a message to that computer, how does the user keep track of all those numbers?

A. Well, fortunately, users don't have to. And the people who -- who invented the internet were actually, I think, had a lot of foresight and actually a lot of insight about people. And they realized that people aren't very good at remembering a lot of numbers.

I'm terrible at remembering numbers.

But people are good at remembering names and words and particularly words that they associate.

For example, if you know you want to go to a web page at Google, then it's easy for you to remember Google.com, but you're not going to the remember their numeric address.

Q. Is there a name for that -- that -- I guess name -- is there a name for the name Google.com?

A. Yes, sir. Those -- those became known as domain names.

Q. So Google.com is a domain name?

A. Yes.

Q. And Amazon.com is a domain name?

A. That's correct.

Q. And CNN.com is another domain name?

A. That's correct.

Q. Okay. How does that work then?

A. Well, the way that works -- to talk about that, let's go and look at how this -- this actually goes across the internet when I have this address, okay? This address is being used to send this information that we have depicted as -- as an envelope here, because it's a lot like sending mail. You know, you put an address on the mail -- on the envelope and you send it -- send

it across the internet.

And these routers are using that number to decide how do I send it?

Q. So that's how the router uses that number, right?

A. Yes, sir. That's right.

Q. But now tell us how the domain name helps people send messages just like that without having to remember the numbers.

A. So the way that works -- and I'm going to use Google that I mentioned earlier as -- as an example. Most people probably know what Google is, but for those who might not, on the internet, one of the very useful things you can do is -- is search for information.

There's all kinds of information on the internet.

You can get recipes on the internet. You can get how do I fix something on the internet. If you have a -- if you have a broken appliance, you can go on the internet and find out what the part is that you need.

You can shop on the internet. It's amazing the amount of information on the internet.

The problem is that there's so much information, how do you find it? And there's some very popular search sites -- and Google is one of those --

that allows you to go to Google and you type in some key words that you're searching for.

So if it's information about something, you type in the things you want information about, and Google will go out on the internet and come back and say, here's a list of sources of -- of information that you can go to, to read about this subject.

Q. Okay. So you've told us why someone might want to find the Google page for their computer, but -- but tell us how that works.

A. Yes.

So the way that works is, if I want to go and get this -- to the search page is, I use this domain name, www.google.com. And so I go to my web browser, okay, and I'm going to type in Google.com, but before I do that, the inventors of the internet had to come up with a system or a way to translate that Google.com into the numeric address.

And what they came up with was this thing called a domain name service.

Q. Have you drawn another box that is labeled domain name service?

A. Yes, sir.

Q. What does the domain name service do?

A. What the domain name service does is think

of -- think of it as a big phone book, okay? So say -- say you want to get your car fixed and you want to call Midas and get an appointment, but you don't know their phone number.

You go to the phone book and you look up Midas and across from Midas is the phone number.

Well the domain name service is very similar. Is -- is you know you want to go to Google, but you don't know how to get there, okay? So the -- the internet system itself, including the user computer, can use this domain name service and go to it to look up -- look up that name -- that name and find the corresponding address.

So you type in Google.com. You hit return on your browser, and your computer takes care of the rest. It sends a request for a name look-up called a name look-up to this domain name service, and that domain name service looks up the name just like you would in your phone book, except it's all done by computers. And it finds the corresponding numerical address.

That numerical address is then sent back to your computer. So now your computer knows what numerical address to go to to get that -- that Google page that you want, and to do that it builds what's called a packet.

And a packet is like a chunk of data with addressing on the front of it. And that's the way all information on the internet sends using these packets. The address that was just received from the domain name service is put into the destination. That tells the entire internet, when it sees that packet, where to -- where are we trying to send this -- this information to? And then the source address over here is the -- that's the address of the user's computer. And the reason that's important is that tells Google where to send the reply back to.

So that request goes across the internet to the Google data server, and the Google data server looks at the page request and says, oh, you want our search page. It loads the search page into a packet, one more packet, sends it back across the internet.

And in this case, the destination address is your computer address, and the source is this data server.

So it sends it back. The user computer then takes that information and displays that picture.

Q. All right. Dr. Short, are these communications that you've shown us that go across the internet typically secure?

A. No, sir.

Q. Can you show us an example of how a normal communication on the internet would not be secure?

A. Yes, sir.

So we'll continue with this. Now, you've gotten your Google search page, and say you want to find out about the Caldwell Zoo in Tyler. Maybe you want to find out if they've got some event scheduled or what their hours are or how to get there.

But you type in Caldwell Zoo into the search engine or the browser page. Now the user computer builds that -- that request into this -- in this packet again and sends it over to Google. But now what happens is there's a hacker somewhere in this network.

Now, remember, this network is this very large number of computers, very large number of connections, and they can't all be secure.

Q. Who might this hacker be?

A. Pardon?

Q. Who might this hacker be?

A. He could be -- he could be somebody in Russia. He could be somebody in China. The amazing thing is you have hackers now who do this for a living. They -- they just -- they just scan the network trying to get information that is useful to sell.

Q. Okay. If after the hacker eavesdrops on the

information, then what happens to this packet that the user is trying to send to Google to find out about the Caldwell Zoo?

A. So he gets -- he sees that packet. He sees the request that you've made. But the packet -- typically, the packet just goes on its way. And there's no indication to you; there's no indication to Google that anybody has even seen that information.

Q. Okay. Dr. Short, but why do we care? In other words, why do we care if someone knows in Russia or China, or wherever they may be, that we looked up information about the Caldwell Zoo?

A. Well, you probably don't care about that.

Q. Is there other kinds of information, though, that we care about a lot?

A. Yes, sir. You know, like I mentioned, there's -- there's credit card information; there's bank account information; there's personal identification information; there's, you know, your pictures, your e-mail, all kinds of things across the internet that you just wouldn't want bad people to get ahold of.

Q. Can you give us an information -- an example of how a hacker might intercept confidential business information?

A. Yes, sir.

In a business sense, you may have an employee -- in this case, we'll use the business Acme.

Q. Is that a building that you've drawn over on the right?

A. Yes, sir. This is an office building; maybe it's their corporate headquarters.

And -- and it's got an internal network here with, you know, people's desktops and laptops all connected internally. Then it has a connection out to the internet.

And -- and you may have employees that are out on the road who are doing sales or doing, you know, business on the road, and they want to securely be able to send messages back. They want to be able to send messages back to Acme.

So -- so in this case, say we have an employee who's maybe sitting at the airport waiting for the plane, who's been in a meeting and has learned that -- that their competition is doing things that requires them to really cut their prices to, you know, possibly win a contract or proposing them.

So he or she wants to send this back to the -- to the corporate office to give them a heads up that we got to do something here. You would not want that intercepted by somebody that could then provide that

information to their competitors.

So, again, we have this hacker who intercepts that packet, is able to see what the confidential information is. The packet goes on its way. There's no indication that that message has been compromised in any way. But, in fact, it has.

Q. All right. Thank you for those explanations, Dr. Short.

Let's go back now to the story of your invention, and I think that before you gave us those explanations about the internet and the problem of internet security, I think you were at the point where you were working on what -- a project for the CIA, a project that you called NetEraser, and that you were trying to find a way to make internet communications more secure.

Do you remember that?

A. Yes, sir.

Q. In the course of that project, did you and your team research some of the security solutions that were already available by, let's say, the late '90s when you were doing your work?

A. Yes, I did.

Q. So were there already some ways to secure information traveling across the internet?

A. Yes, sir.

Q. Well, for example, lots of people back then, probably, were already buying books on the internet with a credit card.

Could hackers see that information?

A. Typically not.

Q. What kind of technique was being used to keep that kind of communication secure?

A. There were techniques referred to as encryption.

Q. Encryption. Can you show us how encryption works for protecting internet communications?

A. Encryption is -- we think of encryption as scrambling information in a way that somebody who doesn't know how it was scrambled doesn't know how to unscramble it.

And in computers, the way this information is scrambled is there's something called a secret key.

And -- and this secret encryption key is combined with a set of methods to take this information that you can read, and you apply the secret key with these methods, and what comes out is this scrambled data.

And then this scrambled data -- you see what's happening here. The user computer has this encryption

capability. It is taking the information that's in this data packet and is using the secret key to scramble them.

Now, the only way to unscramble this information is to know what the secret key is. The methods themselves are known, but it's not good enough to know the method. You have to know the secret key.

So this packet gets sent on its way. It gets intercepted again by a hacker. Now, the only way the hacker can decipher or understand what this message here is, is they have to have the secret key to unscramble it.

Since they don't have the secret key and the only other computer that has the secret key is going to be this data server from this computer right here at Acme, that computer is the only one that's going to be able to unscramble the message. So that's the way it's protected.

Q. Are there any limitations on this internet encryption technology that you just described?

A. Well, what I illustrated here was a -- a point-to-point encryption.

Q. What do you mean by that?

A. Well, what I mean is that the encryption started up here, and then it ended here (indicates), and

then that's where the message ended.

Q. So what -- what good is this point-to-point encryption technology?

A. Well, it's very useful for a lot of -- a lot of applications on the internet where you're going -- where you're using your web browser, and you -- you want to do like online banking, or you want to do shopping and you put in your credit card, because the information only goes to this computer here. And this is the computer that's -- that's handling the online banking for you.

So as long as it's secure between those two points, you're okay.

Q. Is there a name for this point-to-point encryption technology?

A. The -- the most common version of this is what's called https.

Q. What do the initials https stand for?

A. It's hypertext transfer protocol secure.

Q. Did you research this https point-to-point security technology when you were looking for a solution for the CIA?

A. Yes, sir.

Q. Was it good enough for what the CIA needed to do?

A. No, sir, it was not.

Q. Why not?

A. Well, they wanted to allow their employees and agents who were remote to have access into their private network, to resources inside their private network.

Q. Could a point-to-point do that?

A. No, sir.

Q. So if this kind of security that was available in the late '90s wasn't good enough for what the CIA needed, was there another kind of technique for securing internet communications that you were familiar with and that you and your team considered in the late '90s?

A. Yes, sir.

Q. What was that?

A. That was a class of techniques called virtual private networks.

Q. We've heard about virtual private networks already, but even though Mr. Munger explained to us what the words mean, can you explain to us now, how does a virtual private network work?

A. Yes, sir. Go back to the Acme example. You recall we have this Acme facility here, being the corporate office, and inside it is a network with computers on it.

And this network is referred to as a private

network. And the reason it's private is that it's physically secured by the building itself and the locks on the doors, so somebody outside the building doesn't have access to information flowing through that private network.

A virtual private network allows one to extend the privacy on this private network across the public internet to some computers remotely connected on the internet.

Q. Okay. How does it work?

A. So one example of how it works -- we'll go back to the message: Cut our prices. And you notice in this example, we have some private addresses here corresponding to this private network.

And in this case, the scrambling is occurring not only on the information, but it's also scrambling the addresses.

Q. So what happens then?

A. So this scrambled packet is put inside what I'll call the public -- the public packet. And the reason I call it the public packet is that it has the public addresses used to route this across the internet.

So that's going to go on its way. Again, you know, our bad guy is intercepting it, but you notice this bad guy, all he sees is all the scrambled data

here. They're not even going to be able to tell that it's a packet, frankly, because it's just garble to them.

Q. Is the hacker able to see the address of the recipient where the message is going?

A. No, sir.

Q. Is he able to see the content of the message?

A. No, sir.

Q. So what happens then with the message?

A. Well, that message arrives here at Acme. It gets -- this private packet gets unscrambled. And so now this computer here knows where to send the private packet within that private network. So it sends it up to the desk up here.

Q. Now, you -- you've shown us a simple message, Cut our prices today, but what kinds of information or data can be sent over these virtual private networks?

A. All right. You can really send any kind of information. You know, any information that can be sent over a network can be sent over a virtual private network.

Q. And how is the virtual private network different from the encryption technology you told us about a few minutes ago?

A. Well, you notice in this case, the -- the

remote computer was able to send this message to a computer within the private network; in other words, had access to computers or resources within that extended network.

Q. So when you and your team were doing this work on behalf of the Central Intelligence Agency in the late '90s, did virtual private networks already exist?

A. Yes, sir.

Q. And were you and your team already aware of them?

A. Yes, sir.

Q. So did you then evaluate the products that were available to set up VPNs as part of your project for the CIA?

A. Yes, we did.

Q. And were there various kinds of software and hardware that could be used to set up VPNs back then?

A. Yes, sir.

Q. Did you and your team buy them and study them?

A. We did. We looked at -- we looked at a number of different products that implemented what was becoming the industry -- appeared to becoming the industry standard in virtual private networks using IP SEC.

Q. Were they practical solutions?

A. Once you had them set up, they worked. They

were -- they were -- they were difficult to set up and pretty complex, which for the average user, they certainly were not practical.

Q. Did you -- in fact, you and your team of experts sometimes have problems setting them up?

A. It was not unusual for us to go through a setup procedure and have it not work and then have to debug or figure out what mistake that we made and go back and fix it and do a couple of iterations to get it to work.

Q. So, Dr. Short, can you -- instead of just telling us that, can you actually show us an example of the kind of things that would have to be done to set up a VPN in this timeframe?

A. Yes, sir.

Q. Let me show you Plaintiff's Exhibit 983. What is this document?

A. Let me put my glasses on.

This is the -- it's a -- it's a how-to help document provided by Microsoft support to help users with the steps that one goes through to set up a -- an IP SEC tunnel, which is a VPN, in the Windows 2000 operating system.

Q. Have you blown up the pages of this exhibit large so that you can walk the jury through what was

required?

A. Yes, sir.

MR. CAWLEY: Your Honor, may I request that the witness step down to an easel over here?

THE COURT: All right.

Q. (By Mr. Cawley) Now, Dr. Short, this is the first page of Plaintiff's Exhibit 983?

A. Yes, sir.

Q. I notice that there are a number of dates on it. Can you tell us about those dates?

A. Well, there's a date down here in the corner (indicates), January 27th, 2010. That's the date this was -- was printed out.

There's a couple of dates up here (indicates), July 13th, 2010, which it's -- Microsoft's office is notifying users that this is when they end their official support on the Windows 2000 operating system.

Q. What does this document tell us how to do?

A. This document is going to take a user through the steps of the things, the steps you go through to set up a virtual private network in the Windows 2000.

Q. Now, when was the Windows 2000 software available?

A. That came out in 2000.

Q. Okay. And did you -- is this a document from

Microsoft?

A. Yes, sir.

Q. It's available on the internet to tell anybody who wants to know how to set up a VPN using the software available back in 2000; is that right?

A. Yes, sir.

Q. Okay. And did you use documents and software similar to this to set up VPNs when you were evaluating security on the internet for the CIA?

A. Yes, sir, we did.

Q. Actually set up VPNs similar to the way you're about to show us?

A. Yes, sir.

Q. All right. So, Dr. Short, using this document, basically, as an instruction manual, take us through the steps that would have been required, say, back in 2000 if somebody wanted to use Windows 2000 to set up a VPN.

A. Okay. So this -- the instructions, in terms of the steps, start here on Page 2 of the document, begins with creating an IP SEC policy.

Q. Okay. What would you have to do to get that accomplished?

A. There's -- there's five steps here that are outlined for creating this policy.

The first one is -- is you have to run something called MMC. And once you start the MMC, you have to load something called the IP security snap-in. And then having loaded that snap-in, you click start and run and then type in this secpol.msc. And so that's the first step.

The second step here is right click on the security policies for your local machine, and then you're going to click and say I want to create an IP security policy. So that's the second step.

The third step, clicking next, asks you to type in a -- a name here -- I can do it this way -- a name for your security policy, so you can refer to it in the future.

And then you go on to the fourth step. You want to clear this activate default response rules because you're going to do some manual -- enter in some manual rules. Click next.

And then finally the fifth step is click finish.

Q. Okay. So you've done those five steps. Do we have a VPN?

A. No, sir.

Q. What's the next thing we've got to do?

A. Okay. Now we're going to start actually

defining what's in the VPN as in how does it behave. And the first step there is -- it's this thing called the filter list --

Q. Okay. And how many things do you --

A. -- from Net A to Net B.

Q. I'm sorry. How many things do you have to do to set this up?

A. Well, there's nine steps here.

The first step, you're wanting to use this wizard, and once you get in the wizard, you're going to add to create a new rule.

After that step, you're going to go to the IP filter list tab, and you say, I want to add an IP filter list.

And then you go to the third step. You're going to clear -- in this case, you're going to clear the use add wizard check box, because you're going to do things manually, and then click add.

And then on the fourth step -- this is where it gets kind of interesting because you have to start defining your -- your private address locks on each side. And there's -- there's a source address on one -- on one side; there's a destination address for the other side.

And so the first thing is you're going to find

this source address. And the source address is -- what you're doing is specifying a specific IP subnet.

You remember those IP numbers I told you about, those four numbers? Well, you have to identify one of those four numbers of that set of four numbers called the IP address, and then there's something called subnet mask, which is -- that's -- that's a network engineering term that limits what you can put on that network.

You go to step five, and now you have to do the same thing on the destination side. You're going to specify the subnet here, which includes, again, another IP address, and then another subnet mask.

This is where -- this is partly where I say the average user is going to become overwhelmed, I mean, because unless you're a network engineer, you don't even know what this stuff means. And so you really need a network engineer to help you through this process.

You go on to step six, and you clear the mirrored check box, and then you specify something called protocols, which, basically, is what kind of communication will you allow over this VPN. And you say I don't allow any kind.

And then in step eight, you're going to -- you're going to click the description and type in a

description, and then finally, here you click okay and close out.

Q. Okay. With all those steps you've taken us through, do we have a VPN yet?

A. No. No, sir.

Q. What's the next thing we've got to do?

A. We now have to do the same thing pretty much to go from Net B to Net A because I got two sides to my VPN.

Q. Show us the steps for that. How many steps are there to do that?

A. Well, we have seven steps -- excuse me -- seven steps up here.

Q. Okay. Let me -- let me interrupt you.

Judge Davis told us just a little while ago that we all have limited time, so let's just cheat. Check off those steps, but don't tell us anything about it.

A. Okay. So there's seven steps.

Q. Okay. Do we have a VPN now?

A. No, sir.

Q. What have we got to do next?

A. Now I have to specify these -- these rules between Net A and Net B.

Q. How many steps to do that?

A. There's ten of those.
Q. Check all those off.
A. (Complies.)
Q. Now, what do we have to do next?
A. Now I have to go from Net B back to Net A and specify a rule for that. And I have seven steps on that.
Q. Now, do we finally have a VPN, Dr. Short?
A. Well, I've entered in all my parameters pretty much for my VPN, but because there's so much information being put in here and it's critical that that information is self-consistent, that is that it doesn't conflict with itself, that they recommend that you really kind of print it out and check it to be sure you've got everything the way you think you should have it.
Q. Can you show us that?
A. So this -- this is an example of what this printout would be here, and there would be a lot of values in here instead of these zeros. But this is the summary of all the configuration choices you made and all the parameters that you -- values that you entered in.
Now, the thing to keep in mind is that on a VPN, you have two sides. And so we've configured one

side.

Now, I've got another user -- nor network engineer really -- at the other side, who is doing the same thing.

Q. They've got to go through all these steps on the other end?

A. Yes, sir.

Q. And, in fact, this is a network, right?

A. Yes, sir.

Q. So it's not just two ends usually, correct?

A. If you're adding another -- another computer to the VPN, then you're going to go through this process again, yes, sir.

Q. How long did this take?

A. Including the time -- I mean, typically, the way this would work is a -- network engineers would be asked to set up VPNs.

And they would get on the phone with each other, and they would -- they would negotiate what this configured -- configuration should look like, because these values have to work within their -- their current network.

And so they would negotiate what those values ought to be, and then each would go and do their configuration.

Q. And how long would it take?

A. And so you're talking 30 minutes to an hour from the time that they've gone through and talked it out, they've put in the configuration, and then they check it out. And if it works the first time, they're really lucky, I think, or they've done it a lot of times.

Q. Okay. Well, once this is set up, does Microsoft then recommend that it be tested?

A. Yes, sir.

Q. And how would it be tested?

A. Let's see. I don't think that's it. Okay. Testing -- it talks about here testing your IP SEC tunnel, which, again, to remind you, this is our VPN -- they -- they have this tool called the IP security monitor. And they recommend you run this IP security monitor to see the activity going on in the virtual private network to make sure it's working.

And to do that, they recommend using something called a ping command, which is basically a request for an echo reply. It's where one computer sends an echo request to the other computer. The other computer gets that echo request and sends a reply back.

Q. Okay.

A. So that tells you you have a connection.

Q. Okay. Dr. Short, I think we'll come back to that echo test in a few minutes, but what if the test doesn't work?

A. Well, if the test doesn't work, then you need to go back to what did my configuration look like, and what could possibly be wrong?

And there's a good chance you're going to get on the phone with the network engineer on the other side, and they're going to talk it out and say, well, I'm not seeing any packets, or they're not encrypted, or what's the problem here and kind of go through and see if you can identify where the problem is.

Q. Okay. Dr. Short, I think we're through with that document. If you would return to the witness stand, please.

A. (Complies.)

Q. Now, Dr. Short, you've just shown us, using Microsoft's own instruction manual, how someone would have set up a VPN using Microsoft software in the year 2000.

Did you and your team examine products similar to this?

A. Yes, sir, we did.

Q. And did they have similar issues of being complicated and hard to do?

A. Yes. They were all very similar, in terms of the kind of parameters, the kind of choices you had to make. Some of them you had to put all this information -- type it into a text file. Some of them you had to type in commands to the device.

But they were all very similar in terms of the same kinds of parameters, the same kinds of choices, and the same kind of knowledge that you had to have to do that.

Q. So, Dr. Short, did this provide security in a practical sense?

A. You know, like I said earlier, I don't think so, because, I mean, it was difficult for me, and I'm not sure I ever got it right the first time. But for someone who doesn't have any network knowledge, I don't know how you would do it.

Q. How long did your team work on this problem until you had a break-through?

A. We -- we worked on this probably for three to six months. We had this vision of we're never going to bring this kind of security to the average user if we can't solve this problem.

Q. And did you finally have a break-through that at least was the beginning of your ability to solve this problem and the beginning of the invention in this case?

A. Yes, sir.

Q. Can you tell us about that?

A. Yes. We were -- we had gone up to New York City for a meeting, and we were on a train coming back, coming through New Jersey, and we had been thinking about this problem, and I realized, actually, there were two aspects to this problem.

One was that users type in -- or users initiate -- try to get on the internet and connect to things, but also applications do that without the user doing anything.

So we -- we really needed to figure out, how do we make VPNs so they just happen for people and they just happen for applications?

And we were -- we were talking about, you know how telephones work and that with telephones, people just dial the number.

And in the old days, you had the old rotary dial systems, and then they went to the touch tone, but they didn't change the way people made phone calls; they just changed from a rotary dial to a touch tone.

But all the changes were hidden from the user, so it was just very natural for the user, that they were getting a new way of doing connections.

So the thought was that somehow we've got to

figure out how to do this on the internet. And I started thinking about, well, how do connections occur on the internet? And I thought, well, people type in a domain name, okay? That's how people start a connection.

And then I said, well, how do applications start a connection? Well, they have a domain name that they do something called a get host by name, which it says give me the numerical address.

So I said, oh, it's the same thing, because when a user types in a domain name, hits return, the computer says, what's the address?

When an application says, I need a connection to a domain name, the computer says, I need an address. So I thought, oh, they're both connecting the same way. So the way we initiate VPNs is, we have to somehow trigger on the fact that this computer is trying to get a translation of this domain name to the corresponding computer address.

Q. And how did you feel when you had that idea on the train?

A. Oh, I was really excited.

Q. Did you tell Mr. Munger and Mr. Larson about it?

A. Yes, sir.

Q. What was their reaction?
A. They were excited, too.
Q. Did you still have work to do, though, on working out the details of your invention?
A. Yes, sir.
Q. And how much longer did your team work on the invention?
A. I would say for this -- for this initial concept, it was in September. By the end of the year, we kind of had all the pieces that we knew we had to bring together to -- to do this.

Because what we had to do was, all those things that you saw there were things you had to do, and you had to do them safely. Because if somebody was able to see what you were doing, then your VPN wasn't going to be secure.

So we had to figure out how to take all that and do it safely.
Q. Can you show us how you did that? What -- tell us how your invention works.
A. Yes, sir.
Q. I think you can tap the screen to get rid of that red arrow.
A. Hit clear?
Q. Clear last --

A. Oh, there it is.

Q. There you go.

A. Got it.

Okay. So the -- the first solution we came up with, which I'll talk about first, is what's often referred to as the '135 in this case.

Q. That's the '135 patent?

A. Yes, sir.

Q. Okay.

A. And in this case -- I'll refresh your memory. You remember, the way the normal DNS works, the user types in this name, the computer requests an address from the -- from this domain name service, gets an address back, and then uses that address, okay?

So what we had to do is, we had to get in the middle of that, because we wanted to trigger a VPN. Instead of just letting this thing go to the domain name service and come back with some unprotected address, we wanted to get in the middle of that.

So what we did was we created something called a DNS proxy.

Q. What's that?

A. A DNS proxy is -- it's -- it's a software module. Sometimes it's a computer. A lot of times it's just a software module, part of a computer, that is used

to process a domain name request before it gets to the domain name service.

So we said, ah, that's how we get in the middle of this.

So in this case, what happens is, the user has typed in the name. Now, instead of going to the domain name service, it goes to the proxy. The proxy looks at this and -- name and makes a determination.

The determination is, does this name correspond to a computer where I can set up and have a VPN? Can I have a secure connection with this -- with this computer?

Okay. If the answer is no, it's not one of those kinds of -- you know, it's not -- it's not that location. That computer can't do that.

Then it forwards that request on to the existing domain name service, which does its normal lookup and returns the public address for that.

If the answer is yes, that this name supports a secure connection, a VPN, then it builds something that we call a VPN request, which, basically, is, hey, I want a VPN with you.

Now, we needed something to handle that VPN request. So to handle that VPN request, we created something called a gatekeeper. And the gatekeeper, a

piece of software, can be a separate computer, doesn't have to be, just a piece of software that receives that VPN request. So that request goes over to the gatekeeper.

Now, the job of the gatekeeper is to take that request and build a VPN between the user's computer and this requested target here.

Q. So is the invention that you just showed us and described for us shown in your patent?

A. Yes, sir, it is.

Q. Let's -- let's take a look at Figure 26 of the '135 patent.

Is that the invention that you showed us?

A. Yes, sir.

Q. Can you -- can you point out some parts of it?

A. For example, you see the DNS here, proxy. You see the gatekeeper right here. I'm not very good at drawing here. And you see how the request for this -- this name lookup goes to the DNS proxy first before it goes to the DNS server.

And then -- so if it can support a VPN, the request goes down here to the gatekeeper, and the gatekeeper sets up this VPN, and you've got your VPN.

Q. All right. So, Dr. Short, you've just described to us your invention in the '135 patent, and

you've told us a lot of things that happened to set up a VPN, but remind us, in your invention, what does the user, the human being sitting at a computer, who wants to set up a secure connection, what do they have to do?

A. The user types in the domain name, just like before and hits return.

Q. Hits one key?

A. Yes, sir.

Q. And then your invention does the rest?

A. Yes, sir.

Q. Now, can you tell us about the second patent that you got, the '180 patent? How does that work?

A. Yes, sir.

The '180 patent is a -- is a second approach method that we came up later with, which uses something we call a secure domain name.

And so in this example, we've got -- this remote user actually wants to send something over to john.acme.scom. So in this example -- I'm sorry. I'm pointing here, and you can't see where I'm pointing. Up here (indicates).

And then this example is John sitting over here at this desktop here, and his computer has a secure domain name address, what we call it.

So the user types that in, hits return. Now,

normally what would happen is, this request would go to your normal domain name service.

Now, john.acme.scom is not in that -- is not in that directory, so it doesn't know where it is. It sends a reply back, says, I can't find this name, okay? So using our secure domain names, we had to come up with something we call a secure domain name service, okay?

So this is a service that knows how to handle secure domain names.

It can be just -- you know, like those other two examples with the proxy And gatekeeper, it can be a software module running on some computer, as long as you have access to it -- it doesn't matter where it is -- or it can be a standalone computer, either way.

Q. So what happens then?

A. So at that point, we have now the -- the user, again, types in this secure domain name, this .scom name, and it goes over to the secure domain name service.

Now, the secure domain name service, okay, looks at that to see if there's a corresponding secure address.

Q. What does that lock represent?

A. That lock represents, one, that the address is a secure address and that it can also provide

provisioning information back to the user's computer.

Q. And what's that?

A. And what I mean by provisioning information is -- you know, all those parameters I was doing over there where I was specifying addresses and -- and ultimately you have to specify keys and things like that, well, that's called provisioning information for a VPN.

And so some of that information could actually be provided by our secure domain name service back to the user's computer.

Q. All right. After the request goes to the secure domain name service, what does it do?

A. Okay. So that comes back to the user's computer, and then the user's computer can use that address and send an access request message across the VPN up to its destination, to John.

Q. Now, does this '180 patent require a gatekeeper?

A. No, sir.

Q. Now, Dr. Short, you've shown us a lot of pictures, and you've told us a lot about how your invention works and how it can set up a VPN.

Have you actually brought computers to the courtroom today, and can you actually show the jury what

is required here in the courtroom live to set up a virtual private network?

A. Yes, sir.

MR. CAWLEY: Your Honor, may the witness step down to this computer?

THE COURT: Yes, he may.

How much longer do you have on direct?

MR. CAWLEY: Fifteen minutes.

THE COURT: Well, let's go ahead and take a break, and we'll do that when we come back. We've been going for about an hour and a half.

Ladies of the Jury, we'll be in recess for about 20 minutes, until a quarter until 11:00. So enjoy your break, and remember my instructions. We'll be in recess.

COURT SECURITY OFFICER: All rise.

(Jury out.)

(Recess.)

COURT SECURITY OFFICER: All rise.

(Jury in.)

THE COURT: Please be seated.

All right. You may proceed, Mr. Cawley.

MR. CAWLEY: Thank you, Your Honor.

Q. (By Mr. Cawley) Dr. Short, I'm sorry. I think I had just asked you if -- if you could demonstrate to

us, live in Court, how your invention would set up a VPN. And I asked Judge Davis if you could step down to your computer over here, and I think he said you could.

A. Thank you.

Q. So would you turn on your computer and tell us when you're ready to go?

A. (Complies.)

Yes, sir.

Q. Okay. So let's first get clear what we see in the courtroom.

Is this your computer that you're standing next to?

A. Yes, it is.

Q. Is it hooked up to the internet?

A. Yes, sir.

Q. I see some wires coming out of it. One of those is a wire for electricity, right?

A. Yes, sir. It's a power cable.

Q. And there's also a wire that has connected your laptop to the projector so that the jury, when we get there, will be able to see on the big screen what's on your little screen.

A. Yes, sir. That's over here.

Q. All right. How is your computer connected to the internet?

A. There's a -- what's called a wireless device or a radio device that communicates over radio waves with what's called a wireless router in the courthouse.

Q. So Judge Davis and the other people in the courthouse make available a wireless connection to the internet; is that right?

A. Yes, sir.

Q. And is there anything special about this connection?

A. No, sir.

Q. So anybody who has a laptop computer like yours and many others in the courtroom that have the ability to connect wirelessly over radio waves can come in, and if Judge Davis gives them the password, connect to the internet that way, correct?

A. That's correct.

Q. All right. Is your computer connected to a virtual private network?

A. No, sir.

Q. Okay. Now, I also see that there's a computer in front of Mr. Munger.

A. Yes, sir.

Q. Is Mr. Munger's computer connected to the internet?

A. Yes, sir.

Q. How is Mr. Munger's computer connected to the internet?

A. He has a wireless card that is connected to a wire -- a little wireless cell card.

Q. What -- what does that mean?

A. Well, Verizon -- show it there -- Verizon makes this little cell card, which is actually like a little telephone, and you send data across it, and it's actually got a little wireless device in it where laptops can hook into that and then get to the internet.

Q. So Mr. Munger's computer is also connected to the internet wirelessly; is that right?

A. Yes, sir.

Q. But it's connected in a different way than your computer is?

A. Yes, it is.

Q. So is it fair to say that your computer is connected to one part of the internet and Mr. Munger's computer is connected to another part of the internet?

A. Yes, sir. It comes into the internet from two different locations.

Q. Now, let's get back to your computer.

What kind of software do you have running on your computer?

A. We have our -- what we call our Gabriel

connection software.

Q. What is the Gabriel connection software?

A. This is a development we've been doing for the last two and a half years. It's in beta right now, beta testing. We have users test it and give us feedback on it.

And it's running here in this window.

Q. Okay. So this -- this software that's running on your computer is called your Gabriel software, correct?

A. Yes, sir.

Q. You say that you and the other people at VirnetX have been working on it for how long?

A. Something like two and a half years, I think.

Q. Is it finished?

A. No, sir.

Q. Is it in a test stage?

A. Yes, sir.

Q. And what's that testing called?

A. We call it a beta test.

Q. Does this Gabriel software use your invention?

A. Yes, sir.

Q. Is there also Gabriel software on Mr. Munger's computer?

A. Yes, sir. He has a very similar window like

here.

Q. And does this software use the invention that you told us about just about 20 minutes ago that is in your patents that can be used to set up a virtual private network?

A. Yes, sir.

Q. Now, on the screen up here, we see what's actually the same as this screen of your computer; is that right?

A. Yes, sir.

Q. Okay. What's this big white rectangle or box that we see on the screen of your computer?

A. This is -- this is the Gabriel application window, what we call the client.

Q. Okay. And at the very top, is that window labeled?

A. Yes, sir.

Q. What does it say?

A. It says VirnetX Gabriel Connection.

Q. What do we see in the white part of the box?

A. Down here, we see two computers that -- that we can have connections with, secure connections.

Q. What's the first one called?

A. The first one you can see is called Gif.

Q. Can you use that arrow so we can see it?

A. You see that?
Q. Where is that computer?
A. That's -- that's Gif's laptop over there.
Q. Okay. And the second -- what's the name of the second computer?
A. The second, you see there, is www.acme.scom.
Q. Where's that computer?
A. That's -- that's a computer in Virginia at a data center.
Q. All right. Since Mr. Munger has a computer in the room, let's connect to him by a virtual private network. And first, let me ask you, before you do that -- take that down.

Can you show us -- how will we know if your invention is successful in establishing a virtual private network over the internet back to Mr. Munger's computer? How will we know that?

A. We have a little icon here that looks like a little clock next to Gif's computer. And if we have a secure -- he just -- he just moved his keyboard or his mouse, which told us that he's now active on his computer, so it changed the icon.
Q. Okay. So we see a little green --
A. Yes.
Q. -- bubble there?

A. And so when -- when we get a secure connection, a VPN, that icon is going to change, and there's going to be a little gold lock on the top of that icon, which means that it's secure.

Q. That little icon, that green bubble?

A. Yes, sir.

Q. Is it pretty small?

A. For us old people, it's small, yes, sir.

Q. And let me ask Mr. Munger to step away from his computer, because I want to see -- not step away, but I want to see not anything Mr. Munger is doing. I want to see what's working from your computer.

Using your computer hooked up to the internet and using your invention on your computer, can you show the jury what the user has to do to actually set up a virtual private network?

A. Okay. So I've selected connect. It says the word connection. And if I just hit the mouse button, which is the mouse button, that's going to start the connect process.

So this is negotiating a connection. And we'll see a gold lock show up --

Q. Is that it?

A. -- right there (indicates).

Yes, sir.

Q. By pushing that one button and using your invention, Dr. Short, did you succeed in setting up a virtual private network with Mr. Munger's computer?

A. Yes, sir.

Q. And is that the same kind of virtual private network that used to take network engineers going through all the steps that you showed the jury about 45 minutes ago?

A. Yes, it is.

Q. And you did that with one click?

A. Yes, sir.

Q. And would it be just as easy to set up a virtual private network with a computer in Virginia?

A. Yes, sir.

Q. Now, let's -- let's not go there, though. Let's stay with Mr. Munger's computer.

Do you remember that ping test that you told us about, that Microsoft suggested could be used to test the connection over the virtual private network?

A. Yes, sir.

Q. Can you do a ping or echo test over the virtual private network that you set up between your computer and Mr. Munger's computer?

A. Yes, sir. I just opened up a little application here that's the ping application. And so I

need to put this down so I can type.

So I typed in Gif's secure domain name, and we hit return, and it starts sending the ping request, okay? These are -- like I said before, these are the little echo requests going to Gif's computer; his computer sending a reply back.

And when a reply comes back, it prints out echo received. So it sent five ping requests.

Q. So just in that amount of time you just showed us, five times your computer sent a ping over the internet out somewhere in the world and back down to the courthouse to Mr. Munger's computer, which echoed it back around the internet to your computer?

A. Yes, sir.

Q. And what else do we see in this box?

A. We see -- remember, we talked about these private addresses that got scrambled. That's an example of one there, that 172.19.13.135. That's a private address that Gif's computer is using. And the little lock there says this is a secure VPN.

So that address can get scrambled before it goes out to VPN.

Q. Are you able to send messages securely back and forth to Mr. Munger using this virtual private network connection?

A. Yes, sir.
Q. Can you show us that?
A. Let me close this window.
We have a little chat application here we built that allows me to type in a message. It will send it to his computer.
Q. So you're typing a message at the very bottom?
A. Yeah.
Q. Looks like it says, hi, Gif, but you misspelled it.
So have you sent that message securely to Mr. Munger?
A. Yes, sir.
MR. CAWLEY: Mr. Munger, may I ask you to reply to it from your computer?
MR. MUNGER: Yes, sir.
Q. (By Mr. Cawley) Is that the answer that Mr. Munger just sent back through his wireless connection over the secure virtual private network in the internet over to your computer?
A. Yes. You notice it says Acme.com. This chat application is using the same VPN channel.
Q. All right. Thank you, Dr. Short.
Would you take the witness stand again, please?

A. (Complies.)

Q. Now, Dr. Short, you just told us or showed us a chat that was going back and forth over the virtual private network created by your invention between you and Mr. Munger.

Is your computer, as it's currently set up, accessing a website?

A. No, sir.

Q. Why not?

A. The -- we have -- we have something we call security policy for our VPNs, which allows you to control what the computer can access.

And Gif's laptop is not running a web server, and the www.acme.scom, that one has a security policy that's blocking any kind of access to a web server from that computer.

Q. What would you need to do to access a website?

A. All you would have to do on the Acme computer is change the policy for that laptop to say, allow the web service through.

Q. How long would it take to do that?

A. Five seconds.

Q. Five seconds.

And once you make that change in policy, is that persistent? In other words, does it stay that way

until somebody changes it again?

A. Yes, sir.

Q. Now, let's go back to the project -- your NetEraser project that you were doing with Mr. Munger at SAIC.

When did you deliver the NetEraser software to the CIA?

A. We delivered source code, I'm guessing, February/March timeframe of 2001.

Q. And did the CIA use the software?

A. I don't know.

Q. Why do you say that you don't know?

A. Well, the CIA is very protective about its methods and particularly communication methods.

So if -- if -- they didn't need us. They could take our software and do what they wanted to with it. Likely, they wouldn't tell us.

Q. All right. Yesterday, we heard quite a bit of testimony from Mr. Munger about trying to raise money for your invention, talking to venture capitalists, talking to various companies.

Did you participate actively in the effort to find investors for your invention?

A. No, sir. I was not actively involved in that side.

Q. Did you continue back at the shop to develop the software for the invention?

A. Yes, sir.

Q. Did your employer, SAIC, though, agree to invest money in that effort?

A. Yes, they did.

Q. Tell us about that.

A. We had -- we had a meeting briefing to our CEO, Dr. Bob Beyster, in -- I believe it was January 2001. And we knew that the -- the -- the In-Q-Tel contract was phasing down, and we were looking for SAIC to invest to further the development of our prototype and to try to help commercialize these ideas.

Q. So how much money did they invest?

A. As a result of that meeting, Dr. Beyster approved 1.7 million, which was used to keep us going.

Q. Okay. And this is during the time that Mr. Munger was out on the road trying to find additional investment money, correct?

A. Yes, sir.

Q. But when Mr. Munger and others were unsuccessful in raising that money, did SAIC eventually decide that it would discontinue investing money and trying to find outside investors?

A. Yes, they did.

Q. When did that happen?

A. That was in something like late June, early July of 2001.

Q. Did you still have money available at that time from what SAIC had already invested to continue developing at least a test beta?

A. Yes, sir. They -- they did not pull back any of the money. They let us keep what we had to continue development.

Q. And did you do that?

A. Yes, sir, we did.

Q. How was that beta progressing in the late summer of 2001?

A. I -- I was very pleased with it, and I told my management that I thought they would be pleased with how much progress we were making.

Q. I said that was in the late summer of 2001.

What effect did the events of September 11th, 2001, have on your team's ability to continue to work on trying to make a business out of your invention?

A. Well, the -- the 9/11 event really changed a lot of things. And for us, we always -- we had always been working on national security problems, and -- and, you know, that was kind of our -- felt like that was our mission in life.

And -- and we started thinking about, you know, what could we do to contribute to the -- you know, in this new -- with this new threat.

Q. And what -- what projects did you devote your time to?

A. I -- I ended up working on an unmanned aerial vehicle mission planning system, provided some support on the -- on the FBI counter-terrorism.

Q. Remind us what that FBI project was.

A. Yes, sir.

That was a -- it was an intelligence system to try to collect information from a lot of different sources, a lot of different databases, and try to identify what people were doing and where the next attacks might occur.

Q. And was that project for the FBI successful?

A. Yes, sir. I can't talk about the details, but there were specific attacks that were stopped because of that program, and there were lives saved.

Q. Let me show you a document, Dr. Short, that -- that I think you wrote. It's an e-mail, and it's Defendant's Exhibit 3257.

Do you recognize that document?

It's in the book in front of you. You can't see it very well on the screen.

A. Oh, it's hard to see on there.
Q. What is this e-mail?
A. I think that's the right one.
Oh, yes, sir, I recognize this.
Q. What is it?
A. This is an e-mail I sent in the November timeframe in 2005 to Gif and to Vic Larson.
Q. And what were you talking about?
A. This is -- I was trying to understand what SIP was all about. I had gotten a book and was reading on SIP.
Q. Let me direct you to the second sentence of your e-mail. You wrote to Mr. Munger and Mr. Larson -- that's Mr. Vic Larson, I guess, one of your co-inventors.
And you said: Still reading through the book, but I find myself losing the bubble on what distinguishes us from SIPs, SIP-S.
What did you mean by that sentence?
A. Yeah, that's an expression I use.
I believe I was looking at SIPS, which is secure SIP, in trying to figure out, okay, what distinguishes our technology from -- point of view of what features and capabilities do we provide that -- versus what SIPS provides. And at that point, I was

losing the bubble.

In other words, I was having trouble distinguishing the significant differences in terms of capabilities and features between the two.

Q. Were you referring to technical differences or business differences?

A. I -- I think ultimately, at this point, I was looking at potential market opportunities and, you know, from the point of view of what could we offer the market that was different.

Q. All right. Sometime around this time, Dr. Short, did you learn that Mr. Munger, because of some of the work he was doing, had begun to suspect that Microsoft was infringing your patents?

A. Yes, sir.

Q. What was your reaction?

A. I was -- it was kind of mixed feelings. I was -- I was surprised, but I was also gratified that a company like Microsoft actually recognized the significance of these ideas and these concepts.

And then I was also a little disheartened that, you know, because there was an emerging opportunity potentially for us to try to commercialize this -- this technology again. And it appeared that there were companies already using this technology. I

didn't see how we were going to be able to compete with that.

Q. Did you think that Microsoft's use of your invention would affect your abilities to introduce a product to the user?

A. Oh, yes, sir.

Q. How?

A. Well, we were -- we were really small and, you know, being able to -- to build and launch a product that Microsoft was already in that space doing, I thought would be extremely difficult and difficult to get people to invest in because of the potential of losing out to Microsoft.

Q. When did you learn that the company called VirnetX had been formed?

A. That was probably in -- it was in 2005, I believe.

Q. 2000 what?

A. 2005.

Q. Remember, speak up, please --

A. Yes, sir.

Q. -- so everybody can hear you.

Take a look at Defendant's Exhibit 3081.

What is this document?

A. This is -- this is a chain of e-mails.

Q. Is one of them an e-mail that you wrote to Mr. Vic Larson at SAIC and Mr. Gif Munger in January of 2006?

A. Yes, sir.

Q. And you're discussing VirnetX in this e-mail, correct?

A. Yes, sir.

Q. And one thing you wrote was that: As we discussed on Monday, if we don't have an IP infringement play, I don't see the play.

Do you remember writing that?

A. I do remember that, yes, sir.

Q. What did you mean by that?

A. Well, this goes back to what I -- what I just said, that -- and what I meant by infringement play was, if we can't defend our intellectual property, then we -- we can't keep people from competing with us using that intellectual property.

And so if we can't prove infringement and protect our property, I don't see how, from a business point of view, we could survive.

Q. And when you -- when you say in your answer, intellectual property that you needed to defend, you're referring to what?

A. Well, I'm referring to these patents, yes,

sir.

Q. When did you join VirnetX?

A. That was in 2007. I think April of 2007.

Q. And you'd been with your company, SAIC, how long at that time?

A. Over 10 years.

Q. And they had how many employees?

A. At that point, 60,000.

Q. 60,000?

A. Probably more. I'm not sure.

Q. And how many employees did VirnetX have?

A. 12.

Q. 12?

A. Yes, sir. Less than 12 at that point.

Q. At that point, less than 12?

A. Yes, sir.

Q. So, Dr. Short, after being at SAIC, a company with 60,000 employees for 10 years, why did you decide to leave there and join this company with less than 12 employees?

A. Before I came to SAIC, I had to convince myself that we were really going to try to do something real with this technology; in other words, we were going to try to develop, license, make a real business out of it.

And, you know, this -- this -- in some ways, it's like a child for me where I was involved in the original conception and development of it. And the fact that I became convinced that we actually had an opportunity here to make a business and help people with this technology, and that was exciting to me.

Q. What is your position at VirnetX?

A. I'm the Chief Science Officer.

Q. What are your responsibilities?

A. I'm -- I'm responsible for the design, directing the development, and I do a lot of the development on the -- on the Gabriel product.

Q. And tell us again, what stage of development is your Gabriel product in?

A. It's at the beta stage.

Q. Are you continuing to develop it?

A. Yes, sir.

Q. But, Dr. Short, do you believe that your Gabriel product can be successful in internet applications if Microsoft continues to infringe your patent?

MR. BOBROW: I need to object. It assumes that Microsoft, again, is infringing.

THE COURT: Overruled.

A. Can you repeat the question, sir?

Q. (By Mr. Cawley) Yes, sir.

Do you believe that your Gabriel product can be successful in internet applications if Microsoft continues to infringe your patent?

A. No, sir.

Q. Why not?

A. I don't believe that -- that -- number one, I don't believe we can compete with them, if they decide to compete head-to-head with us.

The other is, I think it's going to be difficult, if not impossible, to team with other companies who have to invest in this effort when they see the potential of having to compete against Microsoft.

Q. And finally, Dr. Short, in -- in developing products such as Gabriel, did you try to avoid infringing others' patents?

A. Yes, sir. We were really careful. If it comes to our attention that we need to license software and we need to license the capability, we do that.

Q. Thank you, Dr. Short.

MR. CAWLEY: I'll pass the witness.

THE COURT: All right. Cross-exam.

MR. BOBROW: Thank you, Your Honor.

Your Honor, may I approach the witness

with a notebook?

THE COURT: Yes, you may.

THE WITNESS: Excuse me.

CROSS-EXAMINATION

BY MR. BOBROW:

Q. Dr. Short, good morning.

A. Good morning.

Q. My name is Jerry Bobrow. I represent Microsoft. I have some questions for you this morning.

And I wanted to start, if I might, with some questions about what you believe that you invented, and I want to then take you back to around the year 2000 when you filed your patent applications, okay?

A. Okay. Yes, sir.

Q. So I believe that your first patent was filed in February of 2000, correct?

A. Yes, sir.

Q. Now, certainly by that time, there were a number of technologies that were already in existence for securing communications over the internet; is that fair?

A. Yes, sir.

Q. One of those technologies -- and you alluded to it a little bit -- is the technology that was called https, correct?

A. Yes, sir.

Q. And you've already told us, if we can keep all of these letters straight, what https stood for. And I think you said it was something like hypertext transfer protocol secure; is that right?

A. I believe that's right. I may not be exactly right.

Q. All right. And if I understand what you're saying, before your patents were filed, users of the internet, like the people in this courtroom, if they are at home or what-have-you, that they could use https to set up a secure connection on the internet; is that right?

A. Yes, sir.

Q. And one of the things that you could do to set up a secure connection on the internet before the year 2000, before you filed your patents, was you could be at your, say, home computer and you could type in something called a domain name; is that right?

A. Yes, sir.

Q. So I could have a web browser opening like Internet Explorer; I could type in www.amazon.com; and that would take me to a website, right?

A. Yes, sir.

Q. And with https, what I could do is type in

https:\\www.amazon.com, and that would take me to a secure page at Amazon, correct?

A. Yes, sir.

Q. And then I could conduct e-commerce. I could buy a book; I could buy whatever product that was being sold at Amazon, right?

A. Yes, sir.

Q. And I could do that securely, correct?

A. That's correct.

Q. The credit card information, any other information I needed to enter that was private to me would be secure over the internet from my computer to Amazon, because it was encrypted, right?

A. That's correct, yes, sir.

Q. And part of that connection, and one of the issues I wanted to ask you about, is that when I'm at home, to create that secure connection, all I have to do is type in https www.amazon.com and hit enter, and that connection was automatically created, right?

A. Yes, sir.

Q. And not just the connection but the secure connection was automatically created, right?

A. Yes, it was.

Q. Users didn't have to do anything else, correct?

A. That's correct.

Q. So from the user's standpoint before 2000, what I could do was type in what's called the domain name, hit enter, and have a secure, encrypted connection, right?

A. That's correct.

Q. And the technology doing that connection was something called SSL, right?

A. I believe that's correct, yes, sir.

Q. Secure socket layer, SSL; is that right?

A. Yes, sir.

Q. And all of that, from the user's perspective, was easy, wasn't it?

A. Yes, sir.

Q. It was fast?

A. Yes, sir.

Q. And it was, from the user's standpoint, fast, easy, and efficient and, frankly, user-friendly, wasn't it?

A. Yes, it was.

Q. And that whole system, https, that's not something that you invented or Mr. Munger invented or any of your co-inventors invented, is it?

A. That's correct.

Q. Now, if we might, I'd like to pull up from

that explanation you gave. Remember, you used some animations and some PowerPoints and the like?

MR. BOBROW: If we could pull up one of them.

Right. I think we need to dim the lights. I don't think we can see that.

Thank you very much.

Q. (By Mr. Bobrow) Now, Dr. Short, this is a still image from the presentation you gave in response to Plaintiff's counsel earlier today; is that right?

A. Yes, sir.

Q. And I want to make sure I understand the various elements of this, okay?

A. Yes.

Q. So if I've got this right, up in the upper left corner, I have what you're calling a remote user, right?

A. Yes, sir.

Q. The remote user, I think you even said it might be somebody at home, may be somebody at an airport, may be somebody at a hotel; this is somebody who is remote, correct?

A. Yes, sir.

Q. Seeking access to the internet, right?

A. Yes.

Q. And that remote user may -- in this example that you've illustrated, the idea here is that that remote user could use https to get to Acme, right?

A. Yes, sir.

Q. And I think what you're showing us and what you told us earlier is that on the internet what you do to communicate is you don't use physical envelopes, of course, but you use something that you call packets, right?

A. Yes, sir.

Q. And I think what you were saying was that an envelope and a packet were kind of similar in that they will have information on the outside of them, and they will have information on the inside of them, right?

A. Yes.

Q. When you were describing here how the https system works, what you were saying, I think, is that there's a source address and a destination address on the outside of the packet, right?

A. Yes, sir.

Q. And on the inside of the packet is the content, right? The payload it's sometimes called, I think, right?

A. Yes, sir.

Q. And what you're showing there is that the

https system would encrypt or scramble up the inner content of the packet, right?

A. Yes, sir.

Q. But the outer parts of the packet, the source address and the computer that was sending the message and the destination address of the computer that would receive the message, would be visible, correct?

A. Yes, sir.

Q. So if there was a hacker of the type you described earlier, somebody who, unfortunately in this day and age, may be pulling information off the internet -- that hacker would be able to see the source address and the destination address, right?

A. That's correct.

Q. And as a result of that, it would know which two computers were communicating with each other, correct?

A. Yes, sir.

Q. All right. Now, I understand from what you said that this automated system -- this easy automated system called https is something you didn't invent, right?

A. That's correct.

Q. There were a number of other elements involved in internet communication, secured internet

communication you didn't invent either, right?

A. I'm sure that's correct.

Q. The whole domain name system is something that you didn't invent, is it?

A. No, sir, we did not.

Q. The use of domain names was something you didn't invent, correct?

A. That's correct.

Q. Encryption is something that you didn't invent in these patents, correct?

A. That is correct.

Q. And another thing that you didn't invent related to secure communication were the actual VPNs themselves, correct?

A. That's correct.

Q. VPNs were already known prior to 2000 when you filed the patents, right?

A. Yes, sir.

Q. And they were known before September 1999 when you had the train ride that you described earlier, correct?

A. That's correct.

Q. By September of 1999, there were a number of different kinds of VPNs, weren't there?

A. I believe that's correct, yes, sir.

Q. One of them that you described and spent some time over there, when you were marking up on those large, white boards, that was a VPN that was called an IP SEC tunnel-mode VPN, right?

A. Yes, sir.

Q. All right. That was one VPN that was out there at the time prior to the filing of your patents and prior to the time that you had the idea that led to your patents, correct?

A. That's correct.

Q. But that wasn't the only one, was it?

A. That's correct. Yes, sir.

Q. There was also something that was available before those times that was called a PPTP VPN, PPTP VPN, right?

A. I understand that's true, yes, sir.

Q. And a PPTP VPN, and I think -- you were here for the opening statements, right?

A. I was, yes, sir.

Q. And so you heard something about PPTP VPNs in that context, right?

A. Yes, sir.

Q. All right. But that is your understanding that was a VPN that was available before the year 2000?

A. That's what I understand, yes, sir.

Q. And there was also a VPN that was called an L2TP, if I can just keep with the alphabet soup, an L2TP VPN that was also available before the time you filed your patents, right?

A. I'm not sure I'm familiar with L2TP. It sounds familiar, but I can't answer yes or no on that.

Q. Well, you mentioned that you did some research before the time that your patent was filed, right?

A. Yes, we did.

Q. You're not claiming your research in this field was comprehensive, was it?

A. Probably not, no, sir.

Q. So you're not saying there that L2TP didn't exist; you're just saying you don't know either way; is that right?

A. That's correct.

Q. Now, when you were talking about the IP tunnel VPN earlier and you had all the boards up over there, that was not saying how to configure a PPTP VPN, was it?

A. No, sir.

Q. None of those steps, none of those pages of bullet points and numbered paragraphs, none of that had to do with how you configure a PPTP VPN, right?

A. Yes, sir; that is true.

Q. And none of those steps that you described in

that long list of boards that we went through, describe the steps for how to implement an L2TP VPN, correct?

A. Well, I don't know how to configure it, so I don't know if any of those are relevant or not.

Q. But what the document described and what you said was that those were the steps for an IP SEC tunnel-mode VPN, not for any other VPN, right?

A. Yes, sir, that's true.

Q. Now, I'd like to pull up, if we might, another graphic that you used as part of your explanation of this process.

And I think, if I was listening and paying attention to what you were saying -- I was certainly doing my best, and I hope I didn't get it wrong -- so tell me, I believe this is a graphic of what you were describing as a basic VPN.

Did I get that right?

A. Yes. This was an example, sir.

Q. I understand.

And I -- I'm just trying to make sure that I'm not confusing this image with an https image.

So this is a VPN, right?

A. Yes.

Q. Okay. Thank you very much.

And what you've depicted here is a very

typical situation where, even before 2000, a user would want to use a VPN, correct?

A. That's correct.

Q. And what you're depicting here is, once again, the remote user up in the upper left-hand corner, okay? Is that right?

A. Yes, sir.

Q. And, again, this could be someone who's seeking what's called remote access, right?

A. Yes, sir.

Q. All right. So this person has a computer at the airport, at a hotel, maybe at home, one of those types of places where you're seeking remote access. And what you're trying to get to by the remote access is you're trying to get -- for information, you're trying to access information back at your company, right?

A. Yes, sir.

Q. So you want to get those resources that are at your company, but you're remote from your company, right?

A. Yes. Or send information.

Q. And so I think what you're depicting here is that here's this remote user. He or she is away from the Acme Company and wants to set up a VPN back into the Acme Company, correct?

A. Yes, sir.

Q. Now, with the scenario that's painted here with the remote user seeking remote access, that scenario, the common scenario for using a VPN, has absolutely nothing to do with the VPN configuration that you talked about with all those big poster boards when you were describing an IP SEC tunnel VPN, correct?

A. Can you repeat the question, please?

Q. I will. Sure.

A. Thank you.

Q. This scenario of creating a VPN by a remote access user has nothing to do with the VPN that you were describing when you were using those -- the white poster boards and the red ink and you were going through the steps to create that IP SEC tunnel VPN, correct?

A. I don't know if that's true or not, sir.

Q. All right. Well, you certainly read -- and if we can put it up -- Exhibit PX983.

Now, sir, I don't have those boards. Maybe they're over there, but what I'm showing you on that screen is an image of the document that you walked everybody in the courtroom through, to show all the different steps that are involved in creating an IP SEC tunnel VPN, right?

A. Yes, sir.

Q. With Windows 2000, right?
A. Yes, sir.
Q. All right. Now, this document is a Microsoft document, as you said, right?
A. Yes, sir.
Q. When was the first time you read this document?
A. I've never seen this document. An earlier version of this document, back in the 2000 timeframe.
Q. So not this version of it but an earlier version from 2000?
A. Yes, sir. I believe this is a revised version.
Q. And that version back then and this version now we're describing, again, this IP SEC tunnel-mode, right?
A. Yes, sir.
Q. Now, what I'd like you to do -- I'd like to direct your attention to the text that is underneath -- it's about the middle of the page, and there's a paragraph that begins: Windows 2000 IP SEC tunneling.

MR. BOBROW: Let's see how big we can make that.

Can you make that any bigger, Chris?

Thank you.

Q. (By Mr. Bobrow) So the first page of this document is not a page that you marked up for the ladies of the jury, correct?

A. Yes, sir.

Q. All right. But you did read this page to yourself, either back in 2000 or recently, right?

A. I'm sure I did, yes, sir.

Q. What this paragraph says at the start is that Windows 2000, the IP SEC tunneling is not supported for client remote access VPN use.

You see what I'm referring to there, right?

A. Yes. Yes, sir, because the NRFCs don't provide the access solution.

Q. Right.

So what this is saying to people who are reading the Microsoft information is that the IP SEC tunneling mode with Windows 2000 is not for use in the remote access VPN scenario, correct?

A. Yes, sir. Those two aren't.

Q. What it's saying instead is, don't use that remote -- don't use that IP SEC tunnel-mode VPN.

What this document says, does it not, is use a different VPN, correct?

A. Yes, sir.

Q. What it says to do is, instead of using the IP

SEC tunnel-mode VPN that you showed on these boards, is that instead to use an L2TP VPN, right?

A. Yes, sir.

Q. And what it adds is that there were several companies, including Microsoft and Cisco, who specifically developed the L2PT VPN for the purpose of providing client remote-access VPN connections, right?

A. Yes, sir.

Q. So what this document is saying is, forget the IP SEC VPN. Use the L2PT VPN when you want to have remote access of the type that you were describing in your graphics.

When you want to do that, use the L2PT VPN, correct?

A. Yes, sir.

Q. And one of the things that it further adds is that in Windows 2000, it says that client remote-access VPN connections are protected using an automatically generated IP SEC policy, correct?

A. Yes, sir.

Q. So the user isn't creating that policy. That policy is automatically created, right?

A. Yes, sir.

Q. Now, I noticed that as you were going through all of the steps describing the IP SEC tunnel VPN, I

wanted to through with you some of the other VPNs that were around at that time just so that we're all clear about what you were trying to demonstrate to us.

And -- and there was one technology that's been discussed -- you were here for at least part of it, because it was in the opening -- was a technology that was called Aventail.

Does that name ring a bell?

A. Yes, sir. Yes, sir.

Q. Now, that lengthy protocol of steps that you went through with all these pages for IP SEC tunnel mode, that was not describing how Aventail works, was it?

A. No -- not to my knowledge, sir. No.

Q. To your knowledge, Aventail did not use an IP SEC VPN, right?

A. I don't know one way or the other, sir.

Q. And so as far as you know, Aventail didn't use that technology, correct?

A. That's correct, sir.

Q. Now, I'd like you in your book, or you can simply look on the screen -- I want to direct your attention to Defendant's Exhibit 3121.

Now, I know you said you did some research back in the day when you were looking to secure

information, and you were looking at different VPN technologies, correct?

A. Yes, sir.

Q. And you certainly had done enough research to have seen a prior version of this Windows 2000 exhibit that we just looked at a moment ago, right?

A. Yes, sir.

Q. All right. So one of the things I wanted to find out, Dr. Short, was, I put in front of you this exhibit, which is called Microsoft Windows NT Server Operating System, a white paper, and then underneath it says Microsoft Virtual Private Networking Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet.

Do you see that?

A. Yes, sir.

Q. All right. And if you would turn the page --

MR. BOBROW: This is going to be hard for, I think, everybody to read, so could you blow that up, Chris? How do you like that for a copyright page?

Why don't we take a look, though, and blow that up if we can.

Q. (By Mr. Bobrow) And you'll see in the very upper left, that this document bears a copyright date of 1996.

Do you see that?

A. Yes, sir.

Q. And if you go to the next page, there was some information available to folks to look at about PPTP VPNs.

Do you see what I'm referring to?

A. Yes, sir.

Q. And in the upper left corner, it talks about virtual private networking, right?

A. Yes, sir.

Q. And it mentions the point-to-point tunneling protocol or PPTP, right?

A. Yes, sir.

Q. And you understand that back in this time in 1996, that was a technology that Microsoft was working on, PPTP VPN.

A. Yes, sir.

Q. And what this manual is telling people is that those PPTP VPNs were for remote users, if you look in the third line, right?

A. Yes, sir.

Q. This technology was about allowing remote users to connect securely using a VPN, right?

A. Yes, sir.

Q. And it describes those VPN connections using

PPTP as being easy-to-implement solutions for creating secure and encrypted communications across the internet.

Do you see that?

A. Yes, sir.

Q. All right. Now, if I direct your attention to Page -- and there are lots and lots of page numbers on these documents, so forgive me.

I need to direct your attention to a page that's called 3121.007. It's in the -- the page numbers are in the lower right corner. And it will be up on the screen, but feel free to look at it in your book, if you wish.

A. This is easier, actually.

Q. All right. And I wanted to first have you look at the top of the page where there's a figure, and that figure is describing some VPN connection scenarios using PPTP, correct?

A. Yes, sir.

Q. All right. And the scenario that is being painted here is one where you have remote users on the one hand trying to connect to corporate resources on the other hand, correct?

A. Yes, sir.

Q. And what this is saying is that back in 1996, you could use PPTP to connect remotely to corporate

resources using a VPN, correct?

A. Yes, sir.

Q. It describes doing that lower down on the page.

MR. BOBROW: If we could show that.

Q. (By Mr. Bobrow) This publication, Exhibit 3121, from 1996 describes doing that as being easy, easy implementation, correct?

A. Yes, sir.

Q. Now, if we go to Page 11, there's a -- the second paragraph from the top is called Making PPTP Easy to Use.

Do you see that?

A. Yes, sir.

Q. And that, once again, is describing that it is easy for clients and servers and for clients -- I'm sorry.

It says that ease of use has been built into VPN from its inception for both the server and client personal computer.

Do you see that?

A. Yes, sir.

Q. And right underneath that --

MR. BOBROW: If we can go down the page.

Q. (By Mr. Bobrow) -- it says that setting up the

VPN on Windows NT Server 4.0 is easy, correct?

A. Yes, sir.

Q. So certainly, Exhibit 3121 is describing and telling people that using PPTP VPN, it was easy to make a remote access connection securely to corporate resources.

That's what this is saying, isn't it?

A. Yes, sir.

Q. And finally, if you go to Page 3121.013, Page 13 --

MR. BOBROW: If we can highlight the bottom paragraph.

Q. (By Mr. Bobrow) -- this is, once again, talking about PPTP, correct?

A. Yes, sir.

Q. And creating VPN connections, correct?

A. Yes, sir.

Q. And at the bottom of this paragraph, it says that to further simplify use, both the ISP connection and the VPN connection can be set up and activated from one easy AutoDial phone book entry.

Do you see what I'm referring to there?

A. Yes, sir.

Q. And you were here when there was some mention of AutoDial in the courtroom, correct?

A. Yes, I was.

Q. All right. And what this is describing is how you can use AutoDial to easily create a VPN connection in that remote access VPN scenario, correct?

A. Yes, sir.

Q. And I take it that you understand that this kind of a VPN, when you're talking about remote access and the like, that this kind of a system is using the DNS infrastructure that was already in existence, correct?

A. That PPTP was using the -- I don't know one way or the other, sir.

Q. Well, let's take a look at Page 20, and you'll see, at the bottom of that page, there's a paragraph labeled summary.

Do you see that?

A. Yes, sir.

Q. And towards the bottom of that paragraph, in talking about PPTP VPNs, it says that the security, reliability, ease of use, and speed of PPTP-enabled Windows NT servers, combined with the DNS infrastructure provides significantly enhanced business-to-business communications across the internet.

Do you see that?

A. Yes, sir, I see that. I see that, yes, sir.

Q. So what this -- so what this is saying is that when you're using PPTP and you have remote access, that that's taking advantage of the DNS infrastructure to create secure communications across the internet, right?

A. Yes, sir.

Q. Okay. And that was in 1996, correct?

A. Yes, sir.

Q. That was three or maybe four years before you filed your patent application, right?

A. That's correct.

Q. Certainly, three years before you had the idea that led to your patent applications, correct?

A. That's correct.

Q. All right. Now, I wanted to shift subjects a bit, and I now wanted to ask you some questions about the demonstration that you were kind enough to show to us using the two computers that are over there, one that's in front of Mr. Munger and one that is on -- that was on that little easel or what-have-you over by the jurors.

You know what I'm talking about, right?

A. Yes, sir.

Q. And I think what you told us was that both of these computers in the courtroom were running what you're calling the Gabriel connection software; is that

right?

A. Yes, sir.

Q. And this is the software that you've been working on for several years, right?

A. That's correct.

Q. This technology, this software includes the patented technology that is the subject of your patents, right?

A. Yes, sir.

Q. Now, when you ran this demonstration in the courtroom, I trust that this was not the first time that you used the computer that is over by Mr. Cawley right now, was it?

A. No, sir.

Q. And this wasn't the first time that Mr. Munger used the computer that's in front of him, was it?

A. No, sir.

Q. I assume the two of you have communicated using these computers at various times over the last several years, right?

A. No, sir. Those were just set up specifically for this demonstration.

Q. Ah, okay. So -- so how old are those computers? How long have you had them?

A. The one over on the easel, maybe for a month,

and then this one, a couple of days now.

Q. Now, I trust that when you first got those computers and you plugged them into the wall and you pushed the power button, I assume those computers were not ready at that time to do VPN communication, correct?

A. That's correct.

Q. You had to configure the computers in various ways to do a VPN communication even using your invention, right?

A. Yes, sir. We had to download our software and install it.

Q. There are things that you need to install on the computer, aren't there?

A. That's correct.

Q. And there are things that you need to activate on the computer, aren't there?

A. Yes, sir.

Q. And that takes time, doesn't it?

A. Yes, sir.

Q. So the first time that you use something like this, and you create on your computer the various resources, as it were, that you needed to do a VPN, that takes time, right?

A. Yes, sir.

Q. You can't just click your fingers, click the

mouse once when you first power up the computers, and have your invention work; you need to do some work behind the scenes, right?

A. Yes, sir.

Q. All right. I'd like you, if you would, please, to take a look at Exhibit 3578. It's in your binder.

So I will apologize in advance for the font size. This is as big as we got it from VirnetX. And I hope you'll recognize this if we maybe blow up the top title, that what this document is called is the Gabriel Connection Technology Beta Version 3 User's Guide by Vic Larson from May of 2009.

Do I have that right?

A. Yes, sir. That's what it says.

Q. Now, just to get our bearings here, if we may, Vic Larson is actually Dr. Vic Larson, right?

A. Yes, sir.

Q. He's one of the coinventors on the patents that are involved in this suit, right?

A. Yes, sir.

Q. And you're familiar with this document from May of 2009, a little less than a year ago, I guess, right?

A. Yes, sir.

Q. This is a document that's, what, about 12 pages long?

A. Yes, sir.

Q. What this document is describing is how you install and set up the Gabriel connection software of the type that you demonstrated here today, correct?

A. Yes, sir.

Q. But this is just a version that existed about a year ago. That's what this document, 3578, is describing, right?

A. Yes, sir.

Q. What this document does in part -- and let's turn to the second page.

And if I got this right, what this is saying is that, essentially, if you are a user of this beta -- and I think we heard earlier what a beta is, right?

It's kind of like a test where you let people outside of the company use the software to see how well it's working and help -- I think it's called debug it, get the bugs out of the software?

A. Yes, sir.

Q. That's what's going on here, right?

Okay. So if I want to use this Gabriel software in the VirnetX beta test, use the software, I've got to go through all of these steps in order to be

able to set up a VPN on my computer, right?

A. Yes, sir.

Q. So if I took this computer over on our desk over here, I would have to walk through the steps in this manual before I could do a VPN of the type that you and Mr. Munger showed us about an hour ago, right?

A. I'm not sure you have to go through all these steps.

Q. Well, one of the things I'd have to do if I want to participate in a beta is, you told the folks who were participating that they had to register, correct?

A. Yes, sir.

Q. So that's on Page 2, right?

A. Yes, sir.

Q. And if you go down to the bottom, it looks like there's a screen where you have to type in -- the user has to type in all kinds of information before they can get your beta software so that they can create a VPN, right?

A. That's correct.

Q. User name, a first name, a last name, their e-mail, all kinds of information has to be put into the computer before they can use your software and connect using a VPN, right?

A. Yes, sir. This is being put into our

registry.

Q. Sure. And then --

A. Yes, sir. Sorry to interrupt you, sir.

Then the next page --

MR. BOBROW: If we can go there.

Q. (By Mr. Bobrow) -- it tells you how you download and install the software, right?

A. Yes, sir.

Q. So before that happens, before I download the software and install the software, there's no way that I could use Gabriel to do a VPN connection of the type that you and Mr. Munger showed us earlier, correct?

A. That's correct.

Q. So I've got to go through a downloading and installing process, correct?

A. Yes.

Q. That takes time, doesn't it?

A. Yes, sir.

Q. Then if I go to the next page, this is now a page that headed, Running the Gabriel Connector Software for the First Time.

Do you see what I'm referring to there?

A. Yes, sir.

Q. What this is referring to, it's talking about all kinds of issues that may come up after I download

and install the software but attempt for the first time to create a VPN connection using your software that includes your invention, right?

A. Yes, sir.

Q. All right. So what this manual is telling us about your Gabriel software is that it is not a situation where I can simply power up my computer and click and create a VPN; what I need to do is, in fact, install your software, download the software and take some steps to configure my computer so that I can communicate, right?

A. That's correct.

Q. All right. And those steps, at least in part, are laid out in a 12-page document that VirnetX created to describe how that process works, 12 pages long, right?

A. Yes, sir.

Q. Now, I'd like to shift gears and go to a subject that I mentioned just briefly earlier and that had to do with some software mentioned briefly here in Court already called Aventail.

You remember hearing about that from the opening statements, correct?

A. Yes, sir.

Q. Now, Aventail and the Aventail software, the

first time you heard about this software was not in opening statements, was it?

A. That's correct.

Q. Okay. You heard about Aventail back around the year 2000-2001, that timeframe, didn't you?

A. Probably 2001, but I'm not sure, sir.

Q. Back at that time, Aventail was one of the companies that was in the market trying to compete to sell software to perform and create secure connections on the internet, right?

A. Yes, sir.

Q. They were one of many companies out there that were trying to compete in this market, correct?

A. Yes, sir.

Q. Along with SAIC, correct?

A. Yes, sir.

Q. Now, in the -- I think you said it was in the 2001 timeframe, you not only learned about Aventail, but you also were aware of a company called ANX, weren't you?

A. Yes, sir.

Q. ANX was an SAIC company, right?

A. I believe that's correct, yes, sir.

Q. So ANX was essentially owned by the company that you and Mr. Munger worked for back in 2001,

correct?

A. Yes, I -- I believe that's correct.

Q. And what you learned back in 2001 was that ANX, this SAIC company, wanted to try some security software; they wanted to do a beta trial of some software, didn't they?

A. I'm not sure if they wanted a beta or if they were looking for a product that they could actually use, sir.

Q. And certainly, one of the things that you were trying to do, and I believe at the request of Dr. Beyster from SAIC, was to try to set up a beta trial of your software, what you were working on, would use your invention, you wanted to set that up at ANX, correct?

A. You're talking about our group now, sir?

Q. Your group, yes.

A. Yes, sir.

Q. So your group, Mr. Munger, yourself, Dr. Larson, your group at SAIC wanted to have ANX run your software, right, to do these automatic VPN connections, correct?

A. I believe there were discussions about that, sir. I wasn't involved.

Q. Well, I wanted to ask you about that, because

my understanding is, is that you actually were one of the people who briefed ANX about the technology; isn't that right?

A. I don't recall. It's possible.

Q. All right. Let me ask you to turn -- it's not in that book of exhibits, but if you'll close that book. Underneath it, there's a spiral-bound volume that has your deposition transcript.

Do you have that, sir?

A. Yes, sir.

Q. Let me ask you, please, to turn to the third tab.

A. (Complies.)

Q. Do you have that, sir?

A. Yes, sir.

Q. All right. Please turn to Page 111, if you would.

And just to remind everyone, sir, you were deposed in this case, meaning you had your deposition taken, right?

A. Yes, sir, that's correct.

Q. And of course, that deposition didn't happen in a courtroom; it happened in an attorney's office; but you were sworn to tell the truth when -- when you testified, right?

A. Oh, yes, sir.

Q. So it's testimony under oath just like here today, right?

A. Yes, sir.

Q. Now, if you'll look down at the bottom of Page 111, you'll see that there's a reference there at Line 21 down to Line 23, and it says there -- you were asked a question about a document that says: The straw that broke the camel's back was the loss of the ANX beta site as they decided to go with an Aventail solution.

Do you see that?

A. Yes, sir.

Q. And you recall, don't you, that during the middle of 2001, essentially, SAIC decided to no longer continue to seek commercial funding for your inventions, right, in the middle of 2001?

A. Yes, sir.

Q. All right. And so what this document is saying is that the straw that broke the camel's back, the reason for no more commercial funding, was that --

A. Yes, sir.

Q. -- Aventail got this beta site, right?

A. Yes, sir.

Q. And if you go down further, from Page 111 over to 112, you were asked a question: Do you recall an

effort by SAIC to set up a beta at ANX?

Do you see that?

A. Yes, sir.

Q. And at Page 112, your answer at Lines 2 and 3 was: I recall a briefing to the ANX program people about VirnetX, yeah. I recall that.

A. Yes, sir.

Q. Do you see that?

All right. So at the very least, at the very least, what you remember was that your team provided a briefing to --

A. That's --

Q. -- to ANX about your inventions; is that right?

A. Yes, sir. I do recall there was some briefing. I don't recall being at it.

Q. I see.

And the briefing took place -- there was a discussion about your software and technology and ANX decided against your technology in favor of Aventail; is that right?

A. Yes, sir. They -- which I thought was the right decision, sir.

Q. In 2001, and after you learned that ANX had decided to go with Aventail, you learned that SAIC

invested in Aventail in 2001, didn't you?

A. I don't recall when I learned about the investment, sir.

Q. Let me refresh your recollection, if I might. If you would turn -- and I'm sorry to have you turn to all these books, but turn back to that binder of exhibits and take a look at Exhibit 3256.

A. (Complies.)

MR. BOBROW: And if we highlight the top, please.

Q. (By Mr. Bobrow) You can see that, essentially, this is --

MR. BOBROW: Actually, Chris, the wrong one. If you can highlight the very top. Thank you. I'm sorry I wasn't clear on that.

Q. (By Mr. Bobrow) You'll see here that this is a message from Foley to Mr. Munger and others, including yourself, Bob Short, correct?

A. Yes, sir.

Q. And this was an e-mail that you received on September 28th, 2001, correct?

A. Yes, sir.

Q. This is about the SAIC/Aventail partnership, correct?

A. Yes, sir.

Q. And what was happening here was that somebody was forwarding to you and others an e-mail about the relationship and investment by SAIC in Aventail, correct?

A. Yes, sir, it looks like that.

Q. All right. And what you learned and what this document is saying is that SAIC and ANX were, essentially, partnering together to provide full extranet VPN services, correct?

That's one of the things you learned from this e-mail, right?

A. Yes, sir.

Q. And you also learned something about Aventail from this e-mail, correct?

A. Yes, sir.

Q. In that bottom paragraph, you learned that Aventail provides secure and authenticated access to a customer's critical software applications and thus makes these applications available to business partners and employees who are working remotely, right, working remotely off the customer's corporate network, correct?

A. Yes, sir.

Q. You also learned from this that Aventail provides that security by providing identity authentication, user authorization, and encryption

services, correct?

A. Yes, sir.

Q. You also learned that Aventail was being used by Fortune 100 companies, correct?

A. Yes, sir.

Q. Certainly, at this time in September of 2001, there were no Fortune 100 companies that were using your software or your inventions, correct?

A. That's correct.

Q. And to this day, you have not licensed that software or those patents to any Fortune 100 companies or anyone else for that matter, correct?

A. Not exactly, sir.

Q. Well, if we put aside the SafeNet license for which SAIC received no money, correct?

A. Yes, sir.

Q. Putting that aside, your patents have not been licensed by any Fortune 100 companies, correct?

A. That's correct, yes, sir.

Q. Now, in the courtroom here, we observed your demonstration of software here in 2010, the software you've been working on since you joined VirnetX in 2007, correct?

A. Yes, sir.

Q. Now, back in 2000 to 2001, in that timeframe,

you also demonstrated software that embodies your patents, that uses your patent to others, correct?

A. Yes, sir.

Q. There were any number of times that you and your colleagues would visit someone or someone would visit you, and what you would do is demonstrate the software, show how it works, show the creation of the VPN, much like we saw here, and in doing that, you were trying to interest others in either providing funding for you or helping you develop your inventions further or license your -- your patents, correct?

A. Yes, sir.

Q. And certainly, back in 2001, one of the things that you were trying to do was provide information to a number of government organizations to try to see whether they were interested in providing funding for you or using your inventions, correct?

A. Yes, sir.

Q. And so even after SAIC pulled the plug on its commercial, that is, its effort to get private businesses to fund your development -- and that -- that was not successful, was it?

A. No, sir.

Q. So after SAIC decided on that, one of the things that you did was you tried to get the government

interested in using your inventions, right?

A. Yes, sir. If you're talking about us as a group, that's correct, sir.

Q. One of the -- one of the government organizations that you tried to get interest from to use your patented ideas was a company called -- or an entity, I should say, called OSIS, O-S-I-S; is that right?

A. That doesn't ring a bell to me, sir, but it's possible.

Q. All right. Well, why don't we take a look at Exhibit 3347, and we'll see if that refreshes your recollection, okay?

THE COURT: Counsel, I don't know whether this is a good time, but let me just inquire how much longer you anticipate on cross-examination.

MR. BOBROW: I imagine perhaps another 15 to 20 minutes.

THE COURT: All right. I think we'll go ahead and stop at this point then and take our noon break. It's about ten after the hour.

So, Ladies of the Jury, we're going to recess for lunch, and I will remind you of your instructions not to discuss the case among yourselves or with anyone else.

We're going to recess until 1:30. That will give you an hour and 20 minutes today. So enjoy your lunch, have a nice break, and we'll see you back here at 1:30. We'll be in recess until then.

COURT SECURITY OFFICER: All rise.

(Lunch recess.)

* * * * *

CERTIFICATION

I HEREBY CERTIFY that the foregoing is a true and correct transcript from the stenographic notes of the proceedings in the above-entitled matter to the best of my ability.

/s/_____ _____
SUSAN SIMMONS, CSR Date
Official Court Reporter
State of Texas No.: 267
Expiration Date: 12/31/10

/s/_____ _____
JUDITH WERLINGER, CSR Date
Deputy Official Court Reporter
State of Texas No.: 731
Expiration Date: 12/31/10

EXHIBIT F4

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX	*	Civil Docket No.
	*	6:07-CV-80
VS.	*	Tyler, Texas
	*	
	*	March 9, 2010
MICROSOFT CORPORATION	*	1:30 P.M.

TRANSCRIPT OF JURY TRIAL
BEFORE THE HONORABLE JUDGE LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPEARANCES:

FOR THE PLAINTIFFS:
MR. DOUGLAS CAWLEY
MR. BRADLEY CALDWELL
MR. JASON D. CASSADY
MR. LUKE MCLEROY
McKool-Smith
300 Crescent Court
Suite 1500
Dallas, TX 75201

MR. ROBERT M. PARKER
Parker, Bunt & Ainsworth
100 East Ferguson
Suite 1114
Tyler, TX 75702

APPEARANCES CONTINUED ON NEXT PAGE:

COURT REPORTERS:
MS. SUSAN SIMMONS, CSR
Ms. Judith Werlinger, CSR
Official Court Reporters
100 East Houston, Suite 125
Marshall, TX 75670
903/935-3868

(Proceedings recorded by mechanical stenography, transcript produced on CAT system.)

APPEARANCES CONTINUED:

FOR THE DEFENDANT:
MR. MATTHEW POWERS
MR. JARED BOBROW
MR. PAUL EHRLICH
MR. THOMAS KING
MR. ROBERT GERRITY
Weil Gotshal & Manges
201 Redwood Shores Parkway
5th Floor
Redwood City, CA 94065

MS. ELIZABETH WEISWASSER
MR. TIM DeMASI
Weil Gotshal & Manges
767 Fifth Avenue
New York, NY 10153

MR. DANIEL BOOTH
Weil Gotshal & Manges
700 Louisiana
Suite 1600
Houston, TX 77002

MR. RICHARD SAYLES
MR. MARK STRACHAN
Sayles Werbner
1201 Elm Street
4400 Renaissance Tower
Dallas, TX 75270

MR. ERIC FINDLAY
Findlay Craft
6760 Old Jacksonville Highway
Suite 101
Tyler, TX 75703

* * * * * *

P R O C E E D I N G S

COURT SECURITY OFFICER: All rise.

All rise for the jury.

(Jury in.)

THE COURT: Please be seated.

All right. Counsel, you may proceed.

MR. BOBROW: Thank you, Your Honor.

ROBERT D. SHORT, III, Ph.D., PLAINTIFF'S WITNESS, PREVIOUSLY SWORN

CROSS-EXAMINATION (CONTINUED)

BY MR. BOBROW:

Q. Good afternoon, Mr. Short.

A. Good afternoon. Thank you.

Q. Welcome back.

I have just a few more questions for you on a couple of topics, okay?

A. Yes, sir.

Q. Thank you.

I think where we broke for lunch was I was asking you about some of the efforts that SAIC made after SAIC had decided to stop trying to seek funds from the commercial market in the summer of 2001.

Do you recall that?

A. Yes, sir.

Q. What I had asked you about was whether SAIC had made an approach to a government agency called OSIS in the summer of 2001.

Do you recall that?

A. Yes, sir.

Q. Let me please -- and I believe, sir, your

testimony may have been -- and forgive me if I've gotten this wrong -- that you weren't sure whether there was such an approach to OSIS; is that right?

A. Yes, sir. It was not a name that rang a bell in my head.

Q. Thank you.

All right. So what I'd like you to do, then, is take a look at the exhibit that I mentioned right before the break, and that's Exhibit 3347.

And, sir, Exhibit 3347 should also be on the screen in front of you. And it appears to be a presentation from SAIC to OSIS dated June 6th of 2001.

Do you see that?

A. Yes, sir.

Q. Do you see, for example, that Mr. Munger's name is listed on this presentation, right?

A. Yes, sir.

Q. And you see also that your name is listed on this presentation as well?

A. Yes, sir.

Q. And Mr. Zimmet as well?

A. Yes, sir. I don't recall that name.

Q. All right. So in all events, you and Mr. Munger were involved in this presentation to OSIS, correct?

A. Yes, sir, it appears so.
Q. And does this refresh your memory that you, indeed, were so involved?
A. Not really, but I believe that I probably was. My name is on there.
Q. Right. And OSIS, as you recall, was a government agency that was involved in intelligence, don't you?
A. I seem to recall that, yes, sir.
Q. And one of the things that you did when you went to OSIS in the summer of 2001 was you were trying to interest OSIS in your invention, right?
A. Yes, sir.
Q. You were hoping to get OSIS to help fund the continuing development of your invention, right?
A. Yes, sir.
Q. So one of the things that you had to do to get them interested in your invention was to describe it to them, right?
A. Yes, sir.
Q. And one of the things that you did on Page 3 -- if you'd take a look there, please, Page 003 at the top -- was you wanted to let OSIS know what the problem was that your invention was trying to deal with, right?

A. Yes, sir.

Q. You told them one of the things you were trying to address was the secure connectivity of road warriors, right?

A. Yes, sir.

Q. People on the road trying to access corporate resources from remote locations, correct?

A. Yes, sir.

Q. Now, what you did was you told them about the technology you were trying to get patents on; am I right?

A. Yes, sir.

Q. And if you take a look at Page 7 towards the bottom, you describe a situation where you have a client on the Wal-Mart LAN who wants to access services at Mattel using a secure link, and you go through a series of steps there.

Do you see what I'm referring to?

A. Yes, sir.

Q. And at the end of those steps which involve a gatekeeper and which involve entering a domain, a secure domain name with .scom in there into a browser, at the end of that, you get a VPN tunnel, right?

A. Yes, sir.

Q. And essentially in those steps, you're

describing your invention, right? The invention that brings us here into this courtroom?

A. I'm not sure if we were describing our invention or describing the prototype that we had developed.

Q. The prototype you developed to embody your inventions, right?

A. Yes, sir.

Q. All right. One of the things that you also did on Page 6 was you described for OSIS -- and it's probably a little hard to read because of the copy, but if you look at the box all the way over to the right-hand side, it says 280-plus patent claims pending.

Do you see that?

A. Yes, sir.

Q. So you're also telling OSIS that you were getting patents on the technology you're presenting to OSIS, correct?

A. Yes, sir.

Q. And after telling them all of this information about your inventions, what you did, on Page 9, was you asked OSIS to consider doing a beta trial of your technology, right?

A. Yes, sir.

Q. You describe on Page 9 some of the

possibilities for a beta trial, 45 days, 10 clients, available mid-July.

Do you see that?

A. Yes.

Q. That beta never happened with OSIS, did it?

A. No, sir.

Q. They rejected your approach to them, didn't they?

A. Yes, sir.

Q. Now, after June of 2001, as you had mentioned, we all do remember those tragic events of September 11th. And those events transpired. And I think you mentioned on direct examination that you were looking for ways that you could help to contribute in light of the effort that all of us needed to take to respond to that challenge, right?

A. Yes, sir.

Q. One of the things that you and Mr. Munger decided to try to do, in response to that challenge and those horrible events, was to approach government agencies to try to interest them in these inventions that are the subject of these patents, correct?

A. That's correct, sir.

Q. You had the idea, as did Mr. Munger, that the government at that time of 9/11 should be particularly

interested in internet security and in protecting the internet infrastructure that our country had come to depend on so much, right?

A. Yes, sir.

Q. So one of the things that you did was you approached a number of government agencies that were involved with security and infrastructure, correct?

A. Yes, sir, we did.

Q. One of those agencies was the -- was the FAA, right?

A. Yes.

Q. Federal Aviation Administration?

A. Yes, sir, I do recall it.

Q. Yes. And you approached the FAA, which, of course, is responsible for aviation, in September of 2001, just shortly after the events of September 11th, correct?

A. I think that's correct, yes, sir.

Q. And one of the things that you recognized and I think that OSIS recognized is that these horrible events could be used as an opportunity to get funding from the federal government to further develop and enhance the technology that you were working on as a way to get funding so that the FAA or others could use that technology, correct?

A. I'm not sure I would say it that way. We -- we believed that maybe our technology could help in improving security for the country.

Q. Indeed. And you learned at that time that the federal government was anxious to spend money on security in securing the internet, correct?

A. I believe there was an interest, yes, sir.

Q. And so why don't you take a look at Page 3525.

A. I'm sorry --

Q. I'm sorry. I said page. I meant Exhibit 3525.

A. 3525. Yes, sir.

Q. Thank you.

And do you see at the bottom of that first page that there is an e-mail from Dan Woolley to you and Mr. Munger?

Do you see that?

A. Yes, sir.

Q. And it says must read; see highlight paragraph.

Mr. Woolley, who was he at that time?

A. Let's see. What's the date here?

Q. September 18, 2001.

A. I don't recall what his role was. Earlier, he was leading the effort to help commercialize.

By September of 2001, I don't think he was doing that, serving that role anymore. I'm not sure what his role was at that point.

Q. Now, if you turn to the second page of this exhibit, please.

A. Uh-huh.

Q. You'll see that there is an article that was being forwarded to you by someone named Thomas Temin, from Government Computer News Staff Writer, dated September 17, 2001.

Do you see that?

A. Yes, sir.

Q. And what that tells you in the first paragraph is that federal technology managers have jammed the pedal to the metal on information security. The terrorist events of September 11 have seen to that.

Do you see what I'm referring to there?

A. Let me look here.

Yes, sir.

Q. All right. So what this article was telling you was that those responsible for spending money may very well be interested in spending money on internet security, information security, and the like, in light of those tragic events, correct?

A. Yes, sir.

Q. So then if we turn back to the prior page, the first page, it appears about the middle of the page that Mr. Munger, copying you and others, sent an e-mail to Michael Brown at FAA.

Do you see what I'm referring to there?

A. Yes, sir.

MR. BOBROW: And, Chris, if you would please go up above that to the text above that.

Q. (By Mr. Bobrow) It appears that Mr. Munger sent an e-mail that discusses your IP hopping research and also our latest work in Dynamic IP SEC VPNs.

You see what I'm referring to there?

A. Yes.

Q. And what you're referring to there is, again, part of the work that you were doing related to the inventions that bring us here into this courtroom, right? The Dynamic VPNs?

A. Yes, sir. The second part of that, the Dynamic IP SEC VPNs would be that, yes, sir.

Q. And if you look even further up the document, there's a mention in an e-mail from Mr. Munger to FAA and others, including yourself, from September 18th, wherein the first line of the e-mail, it talks about VirnetX's ISC.

Do you see that?