Bellcore

SPECIAL REPORT
SR-4717
ISSUE 1, JANUARY 1999

Voice Over Packet in Next Generation Networks: An Architectural Framework

Trademark Acknowledgments

CLASS is a service mark of Bellcore.

Prepared by:

Voice Networks:
Design and Engineering

For ordering information, see the References Section of this document.

SPECIAL REPORT
NOTICE OF DISCLAIMER

This Special Report (SR) is published by Bellcore to inform the industry of Bellcore's Voice Over Packet (VOP) Initiative.

Bellcore reserves the right to revise this document for any reason, including but not limited to, conformity with standards promulgated by various agencies, utilization of advances in the state of the technical arts, or the reflection of changes in the design of any equipment, techniques, or procedures described or referred to herein.

Bellcore specifically advises the reader that this SR does not directly or indirectly address any Year-2000 ("Y2K") issues that might be raised by the services, systems, equipment, specifications, descriptions, or interfaces addressed or referred to herein. As an example, and not a limitation, neither this SR nor Bellcore is directly or indirectly assessing or determining whether specific services, systems, or equipment, individually or together, in their current form, or as they may be implemented, modified, or augmented in the future, will accurately process dates and date-related data within or between the twentieth and twenty-first centuries, in either direction, including elapsed time, time difference, and/or leap year calculations.

BELLCORE MAKES NO REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT TO THE SUFFICIENCY, ACCURACY, OR UTILITY OF ANY INFORMATION OR OPINION CONTAINED HEREIN. BELLCORE EXPRESSLY ADVISES THAT ANY USE OF OR RELIANCE UPON SAID INFORMATION OR OPINION IS AT THE RISK OF THE USER AND THAT BELLCORE SHALL NOT BE LIABLE FOR ANY DAMAGE OR INJURY INCURRED BY ANY PERSON ARISING OUT OF THE SUFFICIENCY, ACCURACY, OR UTILITY OF ANY INFORMATION OR OPINION CONTAINED HEREIN.

This document is not to be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by Bellcore to purchase any product, whether or not it provides the described characteristics.

Readers are specifically advised that each LEC/IXC may have requirements or specifications different from the generic descriptions herein. Therefore, any vendors or manufacturers of products should communicate directly with a LEC/IXC to ascertain that company's needs, specifications and actual requirements.

Nothing contained herein shall be construed as conferring by implication, estoppel or otherwise any license or right under any patent, whether or not the use of any information herein necessarily employs an invention of any existing or later issued patent.

Bellcore does not recommend products and nothing contained herein is intended as a recommendation of any product to anyone.

If further information is required, please contact:

Anindo Bagchi
Bellcore
331 Newman Springs Road
Red Bank, NJ 07701

For general information about this or any other Bellcore documents, please contact:

Bellcore Customer Service
8 Corporate Place, Room 3A-184
Piscataway, NJ 08854

1-800-521-2673 (U.S. and Canada)
(732) 699-5800 (All Others)

Voice Over Packet in Next Generation Networks: An Architectural Framework

Contents

List of Figures

List of Tables

1. Introduction and Background

1.1. Motivation for Voice Over Packet

Various industry experts have published numerous papers with forecasts of the amount of voice traffic that will be transmitted over alternative networks, such as the Internet, and public and private Internet Protocol (IP) networks. Their published forecasts seem to support just about every point of view, from the wildly optimistic view to the rather conservative view, with a variance of over 100% for 2002 and 2003. A composite of forecasts by these industry experts suggests that a likely scenario for the penetration rate of Voice Over Packet (VOP) traffic by 2003 is in the vicinity of 10% of the voice traffic. In addition, 25% of the Virtual Private Network (VPN) and other private network traffic is expected to migrate to public packet based IP networks by 2002. This growth forecast would differ significantly for the diverse segments of the industry over this timeframe. For example, it is likely that the growth for VOP traffic in the long haul and backbones network would be higher than in the Local Exchange Carrier (LEC) market.

VOP transports calls on packet-based data networks. There are numerous business drivers for offering VOP. A key motivation for some early adapters has been to take advantage of the inequities in telecommunications tariffs. This allows service providers to take advantage of unresolved regulatory issues that enable them to avoid paying access charges. However, it is anticipated that these arbitrage opportunities would not be available beyond the next couple of years.

Another motivation is that VOP provides the opportunity for additional revenues for service providers that have data network with spare capacity, which can be used for voice calls. Many service providers such as Interexchange Carriers (IXCs), Competitive Local Exchange Carriers (CLECs), and alternate access providers, have already deployed high capacity digital networks to key enterprise sites. The same scenario is true in many other countries, where International Carriers have bypassed the incumbent's Public Switched Telephone Networks (PSTN) to selected large business sites. These same high-speed networks, which were originally used for data, can be utilized using VOP for long distance and international voice calls.

VOP would allow carriers to take advantage of savings as a result of the consolidation of voice and data networks. Today, many large carriers have parallel networks for transporting voice and data. While the existing circuit-switched network is mainly used for voice calls, newer packet-based networks are being deployed to handle data transport. However, maintaining two parallel networks is inherently expensive. The VOP technology presents carriers with an opportunity to migrate all information transport, i.e., voice, data, fax, image, and video, onto a single medium. There is the likelihood of significant cost reductions on transport, switching, on site cabling and equipment, and administration and management, with the single VOP network for both voice and data communications. Given the much higher growth in data traffic, carriers are being forced to make investments to upgrade their packet networks. VOP would allow the carrier to use the same packet network to handle the growth in its voice traffic, initially in the backbone network. For newer carriers who do not have their own infrastructure, the economics are even more compelling. Given the faster growth in data traffic, the carrier

is likely to deploy a packet network to handle its data traffic – VOP would allow the carrier to use the same network for voice.

Over the longer term, arguably the most significant motivation is that VOP provides carriers with the potential for new service offerings. Such newer services, most of which are still in the conceptual stage, could take advantage of both voice and data offerings. In addition, packet networks offer a more "open" environment (for example, using IP, the Internet Protocol) with a greater flexibility for service creation and customization than the relatively "closed" telephony environment. Using IP, the Application Programming Interfaces (APIs) are open and available to any developer or in-house development group, to create custom services for each enterprise. Large businesses, such as banks, government, transportation companies, hi-tech, and healthcare concerns, who are likely to be a carrier's key customers, would be able to create and deploy custom telecommunications services to meet their unique requirements. This is in contrast with traditional telephony networks where there are few open APIs. A big gain from using VOP is the efficiency and better service that can be provided to traveling employees when VOP is combined with other packet-network operations. For example, a traveling employee can connect his or her notebook computer to the public Internet or a corporate Intranet to obtain information, access data bases, and send/receive e-mail. However, on the same call he or she can also use the speaker and microphone built into his or her notebook PC to check voice mail, and make voice calls through his or her office Private Branch Exchange (PBX).

In addition to all the above, there are studies that suggest that there are cost advantages of VOP. There are analyses that show that VOP offers cost advantages for both switching and transport. Some Bellcore studies suggest that the combined infrastructure and operations cost savings could be on the order of 30-50%. However, such analyses depend on the specific assumptions used, and are often based on market forecasts and assumptions that may be arguable, or not applicable to a particular situation. The cost savings potential of VOP are realistic, but need to be quantified on a case-by-case basis in order to develop a sound business case for migration to VOP.

1.2. VOP Solutions for the Service Provider's Networks

The technology which enables VOP is not really new. Technologies such as voice packetization, data detection, and silence suppression have been in use for about twenty years as a means of improving the trunking efficiencies of international submarine cable systems and other transport systems, with a relatively high cost of bandwidth and low flexibility in system bandwidth upgrade. What is new is that, (1) signal processing technology has advanced enough to allow these systems to be implemented on single chip digital signal processors and personal computers, and (2) protocols have been developed which standardize means for packetized voice to be transmitted and controlled over ordinary data networks, based on the Internet Protocol stack. Many of the initial VOP solutions are based on the H.323 family of standards, which is published by the ITU-T. H.323 itself, and is really an umbrella systems recommendation that calls on many other standards for support. However, existing standards do not address all the needs of a carrier wanting to deploy VOP. For example, H.323 does not address guaranteed Quality of Service (QOS); and it is generally acknowledged that in order to have acceptable voice quality using VOP over wide area networks, some control over such parameters as packet latency and packet loss is required.

VOP solutions that are considered for wide deployment in public networks may have to demonstrate suitability from several different perspectives. The VOP solution would have to provide necessary reliability and security that is expected in public networks. It would also be critical for the VOP solution to be scaleable (lack of scaleability is one of the inadequacies of initial VOP solutions). In addition, the following issues will be important:

- *Interoperability*

  The VOP solution deployed in the network would have to interwork with not only other VOP networks, but would also have to interwork with the legacy PSTN for support of end-to-end voice calls and other narrowband services.

- *Voice Quality*

  The VOP network would have to offer voice quality that is comparable to that which is offered by the PSTN.

- *Telephony Features and Services*

  The VOP network would have to be able to support the suite of telephony features and services that are offered by the typical PSTN. This would, in many cases, imply that the VOP network would be able to interact with the Common Channel Signaling (CCS) network and Service Control Points (SCPs) in the PSTN. In addition, the VOP network would need the framework to support new services.

- *Accounting and Settlements*

  The VOP network would have to provide necessary capabilities for billing and accounting management. In many cases, this will imply the ability to interact with legacy billing systems.

- *Network Management*

  The VOP network would need to support the necessary operations and network management capabilities expected in public networks. This will imply that the elements of the VOP architecture have built-in capabilities to support operations and network management. These capabilities would have to be integrated into an overall operations architecture.

1.3. Purpose and Scope of Document

This Special Report (SR) provides a comprehensive framework for the support of voice and other narrowband services over packet-based networks. The VOP solution that is discussed in this SR places significant emphasis on the issues that are important for the solution to be widely deployed in public networks. The goal is to develop a solution that provides a framework for a VOP network that has parity with the PSTN in terms of features and services, their quality, and reliability. The framework supports necessary capabilities for billing. A significant focus of this SR is on operations and network management.

In particular, the SR provides Bellcore's current views on the following:

- Network technologies and architectures that may be used to support voice and other narrowband services on packet-based networks (i.e., VOP networks) in the next one to three years

- Services supported by VOP networks
- Functional requirements for the likely components of VOP networks
- Architectures for the operations and management of VOP networks
- Related issues and challenges, including the migration strategies for circuit-switched networks, for first-generation packet-based voice networks, and for wireless networks to the VOP network discussed in this SR.

While it is understood that the VOP network would support additional services that are currently not offered on the PSTN, this SR does not seek to define such services. The focus of this SR is on ensuring the support of PSTN services on packet-based networks.

The VOP network is recognized in this SR as a component of the Next Generation Networks (NGN). However, NGN has many features and characteristics that are beyond the scope of the VOP network as discussed in this SR. The SR discusses the relationship of VOP to NGN, and discusses an evolution strategy for going beyond this VOP solution towards NGN.

A significant need for VOP networks is that they interoperate with other VOP networks and with the PSTN. One approach towards interoperability is through the development of Generic Requirements (GRs). Towards that end, this SR provides a roadmap for GRs for VOP and for its related operations and network management capabilities.

1.4. Document Organization

The subsequent sections of this document are organized as follows:

- Section 2 presents an overview of the current industry and standards activities on VOP, and discusses the need for VOP Generic Requirements.
- Section 3 identifies characteristics of a VOP network, such as network services, network capabilities, as well as its relationship with the Next Generation Network (NGN).
- Section 4 describes the high-level VOP architecture framework, together with illustration of the call flows and identification of GRs needed for VOP.
- Section 5 discusses the functionality of the significant components of a VOP network.
- Section 6 presents the Operations and Maintenance framework for VOP and the major issues involved.
- Section 7 discusses the migration strategies for various existing networks towards the VOP network discussed in this document, and the migration beyond VOP and towards NGN.

2. Current Industry Status

Numerous disparate industry efforts have been announced to address Voice over Packet (VOP). There are relationships and similarities among the service, technology, and network aspects of these initiatives. However, no one initiative is addressing the overall service, technology, and network aspects of VOP; nor does the collection of initiatives address all aspects of VOP to assure interoperability and interconnection among VOP networks, and to existing telecommunications networks.

This section provides a summary of the activities of network operators and suppliers, including network infrastructure plans, VOP service offerings, equipment characteristics (both existing and planned), and standards and developments. Finally, this section identifies areas which may require additional specification to assure interoperability and interconnection among VOP networks and between VOP networks and existing telecommunications networks.

2.1. Network Operators

All types of network operators have announced plans for VOP, but they have different motivations. VOP was first offered by IP Telephony Gateway Service Providers in the international arena to offer customers a cost-effective alternative to international toll charges. However, many other network operators have also announced plans for providing voice services over packet networks. Following are some examples:

- *Interexchange Carriers*

  Sprint, AT&T and MCI Worldcom all have announced VOP initiatives. Their motivation is mainly to gain network and operational efficiencies through consolidated core network infrastructures in the short term. In some cases, the IXC's VOP initiative is directly tied to a strategy for entering the local exchange service market. In the long term, they hope to offer new, multimedia services that capitalize on the common infrastructure planned for all telecommunication services. Their goals are not new – ATM, a packet technology, was designed to integrate all services. It is just that now the vision is becoming a reality.

- *Local Exchange Carriers*

  Many LECs are also assessing VOP technology. Some of their motivations are the same as for interexchange carriers. They also see the growth of data transported on their networks, and want to introduce more efficient ways of carrying that data. Some LECs have the additional motivation that they wish to use VOP as a vehicle for economical entry into the long-distance market.

- *New Facilities Based Carriers*

  New market entrants, i.e., Qwest and Level 3, have announced plans to deploy a single network infrastructure based on packet technologies. They plan to avoid deploying "legacy" voice infrastructures, which they hope will save them capital as well as operating expenses. In some cases, these new entrants seem to be regarding VOP as a technology which can help them offer voice services over a network optimized for data, thus bringing in new revenues, providing a use for initial excess capacity, and, perhaps, increasing the possibility of data networking sales by packaging data and voice into an attractive bundle.

- *Internet Service Providers*

  ISPs have data networks and see voice as just another application that can ride over their network and generate some revenue.

- *Wide Area Network Service Providers*

  Some network operators provide data WAN services, such as frame relay, to enterprise customers. These network operators are upgrading their services to support voice capabilities.

- *Cable Operators*

  Cable operators are considering VOP technology as part of their strategy for offering voice services over their cable infrastructure. Videotron of Canada has announced plans to deploy voice services over a packet infrastructure. Recently, AT&T also announced that it will be implementing Voice over IP on their TCI cable infrastructure, pending shareholder approval of the AT&T/TCI merger.

Figure 2-1 is a useful illustration for understanding goals and strategies of various network operators. It shows the paths that network operators can take in deploying technology. They can proceed in two directions, (1) deployment to gain network efficiency, or (2) deployment to develop new service capabilities.

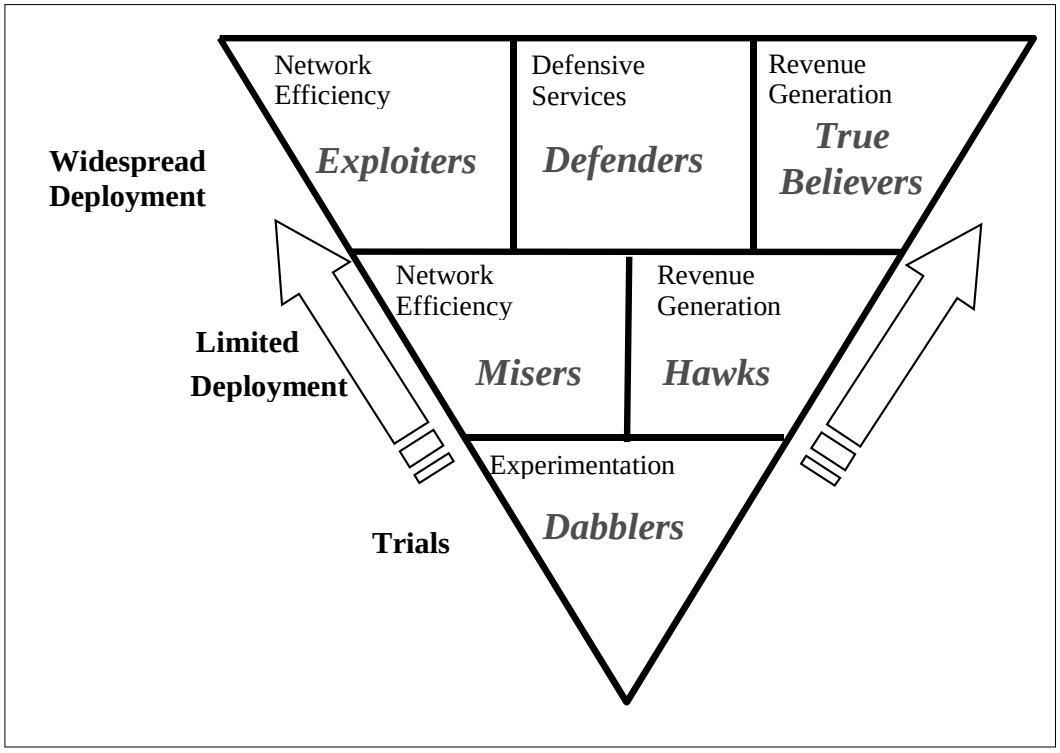

Figure 2-1 Technology Deployment Strategies

Most network operators today are in the initial stage of experimenting with VOP technology. This is partially due to the fact that first generation products do not lend themselves to large-scale deployment. It is expected that this will change in the next few years.

The following subsections review the network operator categories, and review announced plans and strategies of operators in the categories.

2.1.1. Interexchange Carriers and Local Exchange Carriers

Many traditional carriers are at least assessing VOP technology. Many are considering consolidating their backbone transport networks supporting different data services onto a common packet backbone. Others are going beyond that. One example is Sprint with its ION initiative. This initiative is intended to provide business and, ultimately, residential customers bundled access to a variety of network services, including voice via an ATM network. For residential service, call processing and supplementary services will be handled by software on servers. Additional lines will be accessible at any time by establishing new virtual circuits to the call-processing server. Sprint appears to be on the revenue generation path towards becoming a True Believer.

Many Local Exchange Carriers are examining the efficiencies that can be gained by replacing tandem switches with core packet backbones as a first step in transitioning to VOP. Their motivation is cost savings through network efficiencies. Within the next year, it is likely that limited deployment will begin moving these carriers along the Hawk path.

Additionally, Bell Atlantic is taking a defensive position by announcing that it will terminate VOIP calls from the ITXC consortium of VOIP gateway providers.

2.1.2. New Facilities Based Carriers

New facilities based carriers such as Qwest and Level 3 have deployed significant fiber-network capacity and have been talking about deploying a purely IP-based network. Level 3, in particular, has been working on developing standards for the support of VOIP networks, having initiated the Technical Advisory Committee (TAC) that prepared the IPDC proposals for controlling media gateways. These companies can be categorized as Exploiters, i.e., eager to plan and deploy a streamlined, efficient network.

2.1.3. Internet Service Providers

Internet Service Providers (ISPs) are generally assessing VOP at this time. A few have introduced VOIP service as part of a Virtual Private Network (VPN) service. This includes providing tie line replacement for corporations. This service allows companies to connect their PBX systems through a packet network, rather than through private line service, thereby saving substantial amounts of money.

As can be seen in the supplier section, equipment is available for ISPs to upgrade their remote access servers to support VOIP. It is likely that more ISPs will enter the market for VOP services in the near future as Hawks, developing new revenue opportunities on existing infrastructure.

2.1.4. Wide Area Network Service Providers

WAN service providers provide interconnectivity of corporate sites for data transport and Local Area Network (LAN) interconnection. As equipment becomes available, it is a

relatively simple task to add VOP services allowing for interconnection of PBX systems. An example is Equant's Integrated Voice and Data Service built on top of their Frame Relay Service offering. Similar to ISPs, it is likely that more WAN service providers will enter the market for VOP services in the near future as Hawks, developing new revenue opportunities on existing infrastructure.

2.1.5. Cable Operators

For several years , Cable Operators have been experimenting with supporting voice services over their cable infrastructure. They anticipate that VOP will allow them to realize this goal without the need to purchase circuit-switched-based equipment. Just recently, TCI (and AT&T) have announced plans for implementing VOIP using Cisco equipment over their cable plant. Videotron of Canada made a similar announcement earlier in 1998. More and more cable operators are likely to plan voice service deployment using packet technology as a way to generate more revenue, and defend against local exchange company plans to offer broadband access. Their strategies will either be hawk or defensive, depending upon the nature of their market.

2.1.6. Internet Protocol Telephony Gateway Service Providers

IP Telephony Gateway Service Providers are typically Hawks, who saw an excellent revenue opportunity, due to the current high cost of international toll calls. These companies often offer 50% or greater discounts from traditional rates. They typically own very little infrastructure, other than the gateways they have deployed. Several have developed consortia to increase the scope of their services. Over time, as international settlement rates drop, these companies will have to evolve to offer more services.

2.2. Supplier Segment

VOP equipment suppliers can be placed in three broad categories:

1. New VOP Equipment Manufacturers, such as VocalTec and Vienna Systems, who make gateway products used primarily by gateway service providers and enterprises
2. Data Equipment Manufacturers, such as Ascend and Cisco, who have introduced VOP to existing products, but have broader carrier scale plans
3. Traditional Telecommunication Carrier Equipment Manufacturers and Software Developers, such as Nortel, Lucent and Bellcore, that are developing carrier-scale products with interoperability capabilities with existing telecommunications infrastructures.

The following subsections describe the types of products that each category of supplier has available and is planning. Interoperability is a key issue for VOP equipment. Different suppliers' equipment and software may not interoperate with each other and may not interoperate transparently with the traditional telecommunications network.

2.2.1. New VOP Equipment Manufacturers

VocalTec was the first company to introduce commercial software for voice communication between PCs over the Internet when they introduced the Internet Phone in 1995. They and others then expanded their product lines to include gateway products that allowed PSTN users to make a basic telephone call to a gateway. Once connected to

the gateway, the user is authenticated and indicates the actual destination of the call much like in a calling card call. The call is completed via packet transport between the originating gateway and a terminating gateway, or a PC.

While the original gateway systems introduced were proprietary implementations, manufacturers now seem to be moving towards using a subset of the ITU-T Recommendation H.323 series. Some, however, use other protocols such as SIP, a specification from the Internet Engineering Task Force (IETF), or continue to use proprietary protocols. The products rely on signaling and control between the gateways. Interworking with SS7 is not typically available, but is in the plans of some of these manufacturers.

Because these products rely on two-stage dialing in the public arena, they typically do not provide many services. Instead a user would receive services via their local circuit switch. Because there is no interworking with SS7, features such as calling number delivery will not work correctly.

These products are not designed for large-scale deployment. Typical gateways have approximately 96 ports. They have been widely used for trials and by gateway service providers for small, targeted deployment. Increasingly, the focus of this class of suppliers has been on enterprise for intra-enterprise communications between sites. It should be noted that even gateways that are based on the same specifications (e.g., ITU-T Recommendation H.323) may not interoperate. However, there is recent industry activity that is attempting to resolve such interoperability issues.

2.2.2. Data Equipment Manufacturers

Initial offerings of data equipment manufacturers have been in the form of new interface cards on existing remote access server products. Remote access servers are used for dial-up access to data networks. Manufacturers such as Ascend and Cisco have introduced cards that can be placed in these servers to enable them to act like gateways. Since existing access server products typically implement modems for dial-up access using Digital Signal Processors (DSPs), a typical upgrade provides a new set of DSP code which turns the processor into a voice compression coder, and provides other signaling and control functions. Such products are mainly of interest to Internet Service Providers (ISPs) who own hundreds of Remote Access Servers. With this upgrade, ISPs can start providing voice services via their packet infrastructure. These products typically are based on ITU-T Recommendation H.323, rely on two-stage dialing, and have no SS7 interworking functionality.

Data equipment manufacturers have more extensive plans than apparent from their current product offering. Most are concentrating on capabilities needed for carrier class systems. These include the ability to provide appropriate Quality of Service(QOS), and to interoperate with the existing telecommunications infrastructure. Data equipment manufacturers are also developing large-scale, high-performance backbone equipment that can carry millions of calls, as well as data traffic, over a packet backbone. SS7 interworking capabilities are envisioned for late 1999 by many suppliers.

2.2.3. Traditional Telecommunications Suppliers

Traditional telecommunications suppliers, such as Nortel and Lucent, entered the market with products designed to compete with those of the start-ups – small-scale, standalone gateways. They are evolving, however, to carrier-scale solutions based on their Class 5 office products. These carrier-scale products attempt to allow for seamless integration with traditional telecommunication networks, while allowing voice traffic to be transported via a packet network. However, products from different manufacturers may not interoperate with each other. In several cases, traditional telecomm suppliers are also offering a solution similar to those described in the previous two sections.

Bellcore, a traditional supplier in the OSS arena, has started in a new direction with the announcement of initiatives with Sprint and Le Group Videotron Ltee. Bellcore is supplying software to these initiatives that will allow these network operators to provide Class 5 office functionality via a server-based Call Agent on a packet network.

2.3. Standards and Forum Segment

Numerous standards and forums are developing service, signaling, operations, and architecture specifications related to VOP. The primary organizations include the Internet Engineering Task Force (IETF), International Telecommunication Union (ITU), European Telecommunications Standards Institute (ETSI), and the ATM Forum. The activities of these organizations serve as excellent building blocks for the development of requirements to ensure interoperability between equipment and networks. However, there are many open issues for further study and specification.

For example, most of these standards bodies have not specifically addressed the issue of operations for a VOP network. A number of the standards bodies and industry forums have begun the process that will lead to standardization of aspects of VOP operations by organizing projects and activities to study questions regarding VOP operations. This includes IETF, ITU, ETSI/TIPHON, and the TeleManagement Forum.

The current lack of standard, consistent, open, and interoperable VOP operations requires users (both service providers and suppliers) to determine interim solutions that can fill in the gaps, and integrate across standards that are currently established. These solutions should allow the user to attempt to avoid the shortfalls of existing solutions, and to evolve their VOP operations as standardized, integrated, and open VOP operations solutions mature. At minimum, it is important to monitor the standards and forum activities to understand how emerging standards can be used as part of the VOP operations solution.

This section summarizes the activities in the various organizations. The number and variety of standards, as well as options within the standards, point to a need for requirements to support development of equipment that is interoperable and still provide the functionality needed to support both advanced and traditional services. Interoperability with the PSTN is also a critical need that is not yet well-addressed by the standards organizations.

2.3.1. IETF

Following are several working groups within the IETF that are addressing various service, signaling, operations, and architecture aspects of VOIP:

- *IP Telephony Working Group*

  The IPTEL working group has the following two major initiatives:

  1. To develop a call processing syntax that can be used during call establishment for call handling, i.e., a call processing server can arrange for the call to be terminated elsewhere, have a message sent back to the originating server that the called party is busy, or drop the call completely (among other possibilities). This working group is developing syntax to allow the called party to provide input to what happens and for servers to communicate with each other. In addition to the syntax, the group will produce a service model framework describing the services that can be enabled using the call processing syntax.

  2. To develop a gateway attribute distribution protocol that will provide for a common way to distribute gateway attributes (e.g., PSTN connectivity, supported codecs, etc.), so that gateways can be selected during call establishment based on a variety of criteria.

- *Media Gateway Control Working Group*

  The primary purpose of the MEGACO working group is to develop an informational RFC detailing the architecture and requirements for controlling Media Gateways from external control elements, such as a media gateway controller. A media gateway is a network element that provides conversion between the information carried on telephone circuits and data packets carried over the Internet or over other packet networks. This working group will neither work on media gateway controller to media gateway controller protocols, nor on media gateway to media gateway protocols. This is the group where the Media Gateway Control Protocol (MGCP) is being described.

- *Multiparty Multimedia Session Control Working Group*

  The primary purpose of the MMUSIC working group is to develop Internet standards track protocols to support Internet teleconferencing sessions. MMUSIC's focus is on supporting the loosely-controlled conferences that are pervasive on the MBone today. However, the working group also intends to ensure that its protocols are general enough to be used in managing tightly-controlled sessions. To date, MMUSIC has drafted the Session Description Protocol (SDP) and Session Announcement Protocol (SAP); SAP Security, the Real-Time Stream Protocol (RTSP); Session Initiation Protocol (SIP); and Simple Conference Control Protocol (SCCP).

- *PSTN/Internet Interfaces*

  The PINT Working Group addresses connection arrangements through which Internet applications can request and enrich PSTN (Public Switched Telephone Network) telephony services. An example of such services is a Web-based Yellow Pages service with the ability to initiate PSTN calls between customers and suppliers. They are developing a standards track RFC that specifies a service support transfer protocol between Internet applications or servers and PSTN Intelligent Network Service Nodes (or any other node that implement the Service Control Function). The protocol under development is known as the "PINT Profile for SIP and SDP", and is based on the SIP and SDP protocols defined for multimedia conferencing. They also plan to develop a standards track RFC for a relevant MIB to support the service management protocol between Internet applications and the PSTN Service Management System.

- *Signaling Transport*

  The SIGTRAN Working Group addresses the transport of packet-based PSTN signaling over IP Networks, taking into account functional and performance requirements of signaling. For interworking with PSTN, IP networks will need to transport signaling such as Q.931 or SS7 ISUP messages between IP nodes such as a Signaling Gateway and Media Gateway Controller or Media Gateway. The group is making use of existing IETF QOS and security technology.

- IETF Operations and Management Area Working Groups address various operations issues associated with the Internet. These Working Groups are primarily focused on defining and standardizing SNMP MIBs and their associated managed objects. While the effort of these Working Groups is useful to VOP operations, it is not specific to VOP operations. Following is a listing of the working groups within the IETF Operations and Management Area whose work may be applicable to VOP networks:
  - Distributed Management Working Group
  - Entity MIB Working Group
  - SNMP Agent Extensibility Working Group
  - Physical Topology MIB Working Group
  - Routing Policy System Working Group
  - Remote Network Monitoring Working Group
  - Remote Authentication Dial-In User Service (RADIUS) Working Group
  - Roaming Operations
  - Ethernet Interfaces and Hub MIB
  - Bridge MIB
  - MBONE Deployment
  - Uninterruptible Power Supply
  - Guidelines and Requirements for Security Incident Reporting Equipment
  - Next Generation Transition
  - ADSL
  - SNMPv3 Working Group
  - Benchmarking Methodology Working Group.

2.3.2. ITU-T

The ITU-T develops international standards for use in telephony networks. The ITU-T TSAG has instructed all Study Groups to address IP technologies in their areas of responsibility. Study Group 13 has been assigned as the Lead Study Group responsible for IP related subjects in which a new project has been started, the "IP and Telecommunications Networks Inter-relationship" project (I.1). Additionally, guidelines have been established for collaboration with IETF.

2.3.2.1. Study Group 4

Study Group 4, “Telecommunication Management Network (TMN) and Network Maintenance”, is responsible for TMN studies and for other studies relating to maintenance of networks, including their constituent parts. The Study Group has submitted a proposal for a project regarding integrated management of telecom and IP-based networks, which includes a TMN architecture for managing IP networks,

integrated management of mixed circuit switched and IP networks, information models (at the NE, network, and service level) for managing IP network. The output of this project would include a discussion paper on TMN evolution for IP and mixed networks, a TMN architecture for IP networks, and extensions to ITU-T Recommendations M.3400 and M.3200 to include IP network management.

Additionally, other IP-based protocols have been submitted to ITU Study Group 4 for use in the management of telecommunications networks. Specifically, these are SNMP (Simple Network Management Protocol) and CORBA (Common Object Request Broker Architecture). CORBA has been "determined" by ITU Study Group 4 in June 1998 as a TMN protocol at the X-interface of the TMN, and is up for approval in March 1999 by Study Group 4. SNMP was recently contributed as a candidate for an additional TMN protocol at the Q3 interface to ITU Study Group 4, and discussions are ongoing.

2.3.2.2. Study Group 11

Study Group 11, “Signaling Requirements and Protocols,” is responsible for studies relating to signaling requirements and protocols for telephone, narrowband ISDN, Broadband ISDN, Universal Personal Telecommunications (UPT), mobile, and multimedia communications.

The technical work of this Study is organized into 24 “Questions.” Question 5/11 specifies the overall IN requirements for service aspects, network aspects, and management aspects for IN Capability Sets. Question 22/11 specifies the IN Application Protocol requirements to support the service aspects, network aspects, and management aspects identified by Question 5/11. Both of these Questions are addressing Intelligent Network aspects of PSTN – Internet Interworking (PINT) and Voice over IP (in the context of IN support for TIPHON). In addition, Study Group 11 will also develop specifications for the transport of SS7 protocols over an IP network.

2.3.2.3. Study Group 13

Study Group 13, “General network aspects,” is responsible for studies relating to future telecommunications network aspects and the initial studies of the impact of new system concepts and innovative technologies on telecommunication networks, including Broadband ISDN and Global Information Infrastructure (GII).

The technical work of this Study is organized into 29 “Questions.” Recently, a project description on IP (Internet Protocol) and Telecommunications Interrelationships was developed by Study Group 13. This project was initiated because of the large growth of IP data traffic on telecommunications networks worldwide. The project states that seamless interworking between IP based networks and telecommunications networks, and interoperability of their respective applications/services is essential to meet new business requirements. The primary objective of the project is to identify the issues relative to IP and telecommunications interoperability. The scope of the project has been defined as follows:

1. Access to IP based networks using the following telecommunications facilities:
    - Interworking Between IP and Telecommunications networks, such as PSTN, N-ISDN, B-ISDN, digital mobile networks, packet switched data networks, WAN/MANs

- Transport for IP Networks
  - IP over ATM
  - IP over SDH
  - IP over Optical.
- Integration of ATM and IP networking
- Signaling and routing
- Application interworking
- Future architectures
- Coordination within ITU and with other key standards and industry bodies.

This consolidated project concerning IP and Telecommunications networks is a good start by the ITU to manage the work needed to integrate IP with existing telecommunication network standards. It is important that such a project is able to identify the work components and minimize any duplication of work within the ITU-T.

2.3.2.4. Study Group 16

Study Group 16, "Multimedia Services and Systems," is responsible for studies relating to multimedia services definition and multimedia systems, including the associated terminals, modems, protocols and signal processing. The technical work of the SG is organized into 23 "Questions." Question 13/16 addresses Packet Switched Multimedia Systems and Terminals. This question is responsible for multimedia systems and terminals using packet-switched networks. Although initially focused on LANs, the scope of this Question addresses packet-switched environments of any geographic size, reflecting the importance of support over the Internet and other wide-area packet-switched networks.

The trend within this Question is to attempt to focus on the multimedia system operation, independent of the details of the supporting network service. This reflects the following two factors concerning the key system document for which this Question is responsible (H.323):

1. ITU-T Recommendation H.323 has been receiving more industry attention recently than the systems recommendations for other network environments. It can be expected to have a more well-developed set of capabilities and greater product availability in the future, given limited vendor development resources.
2. Since the non-QOS LAN environment, for which H.323 was designed, offers the least in the way of network service guarantees, its system requirements must compensate for lack of QOS. An H.323 system that can operate in a non-QOS packet environment should be able to operate in a circuit-switched or QOS packet switched environment as well, with few modifications. In addition, H.323 has been adopted by the ETSI TIPHON project as part of its approach for standardizing Internet telephony.

2.3.3. ETSI

ETSI is building upon ITU-T Recommendation H.323 to address interoperability between existing telecommunications networks and IP-based networks for voice communications. ETSI has started a standardization effort referred to as

"Telecommunications and Internet Protocol Harmonization Over Network (TIPHON)" to address real-time voice communication and related voiceband communication over IP-based networks. The objective of this project is to support a market that combines telecommunications and Internet technologies to enable communication over IP-based networks to work with existing Switched Circuit Networks (SCN), which include the PSTN, ISDN, GSM, and Private Integrated Services Network (PISN). The standardization effort covers interoperability between the two networks, and not on the actual individual network itself.

The following scenarios are being examined:

- **Scenario 1**: communication between IP network-based users and SCN-based users, in which the call set-up is originated by the IP network user
- **Scenario 2**: communication between IP network-based users and SCN-based users, in which the call set-up is originated by the SCN based user
- **Scenario 3**: communication between SCN-based users, using IP based networks for the connection/trunking between the involved users.
- **Scenario 4**: communication between IP network based users, using SCN for the connection/trunking between the involved users.

The TIPHON project begins to address a number of issues in the interworking between IP-based networks and SCNs. These issues include numbering and addressing, accounting and billing (with Call Detail Records described), and resource and control management (through the use of Media Gateway Control Protocol, or MGCP). Other issues have been identified by TIPHON as topics that require further study, such as Operations, Administration, Maintenance, and Provisioning (OAM&P), as well as further study of MGCP.

2.3.4. ATM Forum

The principal work areas for the ATM Forum VTOA Trunking WG are focused on the use of ATM Adaptation Layer Type 2 (AAL2) for trunking connections interworking between broadband and narrowband networks.

The AAL 2 trunking objective is to specify an efficient transport mechanism to carry voice, voice-band data, circuit switched data, frame mode data, and fax traffic. Its application would be for the interconnection of PBXs, private networks, or enterprise networks. A major roadblock for the group has been on agreeing to a common compression algorithm. If agreement cannot be reached, the specification cannot go forward.

While ATM Forum is currently working on the development of standards for providing voice services directly over ATM, the ATM Forum has not yet begun work on the operations of a Voice-over-ATM network.

2.3.5. Multiservice Switching Forum

The Multiservice Switching Forum, which was formed in late 1998, is an open membership organization committed to accelerating the development and deployment of ATM-capable, multiservice switching systems and networks by carriers and service providers. Through its Implementation Agreements, the MSForum seeks to enable an

open and modular switching system architecture that separates control and network intelligence from switching and media adaptation functions. Such an architecture will enable carriers to deploy open switching systems with components from multiple vendors, allowing them to optimize functionality, performance, and price. This will accelerate deployment of next generation networks supporting advanced, integrated broadband communications services.

The services that a multiservice switching system will support include voice, video, private line, and data services (e.g., Asynchronous Transfer Mode [ATM], Frame Relay, and Internet Protocol [IP] services). Such systems may support a broad range of access technologies, including traditional Time Division Multiplexed (TDM) access lines, Digital Subscriber Line (xDSL), wireless data, and cable modems.

The MSForum is focussing on protocols and interfaces used within switching systems. It intends to leverage the agreements and standards created by the ATM Forum, IETF, ITU, Frame Relay Forum, Bellcore Generic Requirements process, and other industry associations.

The three initial working groups of the MSForum are focused on System Architecture, Switch Control, and Voice Control. The founding members of the forum have proposed provisional Implementation Agreements describing the architecture of a Multiservice Switching System and the Virtual Switch Interface (VSI) for Switch Control.

2.3.6. T1A1 (Reliability, Performance)

The Performance and Signal Processing Technical Subcommittee (T1A1) focuses on the following two main areas:

1. Performance of networks and services at carrier-to-carrier and carrier-to-customer interfaces, with due consideration of end-to-end performance and the performance of customer systems

2. Signal Processing for the transport and integration of voice, audio, data, image and video signals, with due consideration of interaction with telecommunications networks; the integration of inputs and outputs between information processing and multimedia systems and telecommunication networks; and techniques for assessing the performance and impact of such signal processing on telecommunication networks.

The following efforts are related to VOP:

- T1A1.2 has developed Technical Report No. 55 that addresses the reliability and survivability aspects of interactions between the Internet and the Public Telecommunications Network (PTN). The primary focus of this work is on the use of the PTN to access the public Internet. At a later stage, T1A1.2 intends to explore the reliability implications of carrying voice over the Internet.

- T1A1.7, the WG on Signal Performance and Network Performance for Voiceband Services Processing has been investigating voice and voiceband data performance issues of transport over non-PSTN networks, including IP-based networks, which may interconnect with the PSTN. The WG has also developed Technical Report No. 56 which recognizes that voice communications are increasingly becoming a

significant source of traffic between the Internet and the PTN, and provides a set of principles for improving end-to-end transmission performance.

2.3.7. Internet Traffic Engineering Solutions Forum

The ITESF provides an industry framework for management of Internet traffic through understanding, developing and promoting the architectural, technical and operations solutions that lead to data off-load strategies, and deployment of services and products to effectively alleviate PSTN congestion. Correspondingly, as most solutions require "internetworking" with IP architectures and emerging services (e.g., voice and fax over IP), the ITESF expanded its scope in May of 1998 to involve IP performance topics. The ITESF desires to promote dialogue among carrier, supplier and ISP forum participants to stimulate exchange of knowledge and ideas that impact the technical and business decisions affecting deployment solutions. Bellcore coordinates and chairs the ITESF meetings. In addition, through ITESF discussions, Bellcore seeks to influence the industry on technical capabilities architectural solutions via publication of white papers. Bellcore has published a white paper on "Architectural Alternatives to Internet Congestion using SS7 and IN Capabilities" generated from discussions and presentations at the ITESF.

2.3.8. Wireless/CDMA (IMT-2000)

Several types of VOP technology have already been standardized and deployed for certain portions of wireless networks. The IS-95 CDMA air interface carries voice in packet mode over the air. Current wireless network standards (IS-634) support voice connections in packet mode over ATM for soft handoff.

The ITU is addressing future wireless systems through its work on IMT-2000 Related work on Third Generation Wireless (3G) standards is being pursued in TR-45 and ETSI (where it is known as UMTS). Most of the focus in 3G standards is on-air interfaces; and most current work on network architecture is in IMT-2000 and UMTS standards. The IMT-2000 service set includes voice, data, and multimedia sessions; and several of the leading air interface candidates are CDMA based, so the development of a packet-based core network using VOP technology to support voice services is the almost inevitable result.

2.3.9. TeleManagement Forum

The TeleManagement Forum, formally known as the NMF, established an IP Task Group at a "Birds of a Feather" meeting during the TeleManagement World held in Dallas in October of 1998. The objective of the IP Task Group is the creation of multi-vendor, multi-technology solutions for network management of faults of Internet services deployed using IP and IP/ATM technologies. The logistics and schedule for this task group, though, is currently unknown.

2.3.10. Multimedia Cable Network System

The MCNS is a consortium of cable operators to develop specifications for cable networks. MCNS has produced a set of specifications known as the Data-Over-Cable Service Interface Specifications (DOCSIS). DOCSIS provides a reference architecture

and interfaces to permit data, including voice over packet, to be transmitted over a cable network, terminating on an Integrated Telephony Cable Modem (ITCM) at the customer premises. The ITCM provides cable, Internet, and telephony access for the customer. As part of the DOCSIS, SNMPv1 MIBs have been developed to support data interfaces, operations support interfaces, RF interfaces, and security interfaces mainly between an EMS and the various subtending cable modems. Additionally, as part of the DOCSIS reference architecture, business processes (e.g., Service Delivery, Service Assurance, Billing, etc.) and hypothetical scenarios (e.g., System Setup, Enrollment, System Administration, and Problem Handling) are addressed, at least in part. Further work is required in various areas of the DOCSIS.

2.3.11. Ordering and Billing Forum

The OBF is an Alliance for Telecommunications Industry Solutions (ATIS) Carrier Liaison Committee (CLC) sponsored committee. The OBF defines Business requirements and data elements for LEC and Access services ordering. There is no indication that this group is addressing VOP issues, but there are guidelines that are being developed (such as the Local Service Ordering Guidelines (LSOG) and Access Service Ordering Guidelines (ASOG)) that can be applicable to VOP operations.

2.4. Need for Generic Requirements

The preceding sections on industry status paint the picture of a dynamic, emerging industry. Recognizing the many business opportunities and technical challenges, multiple suppliers, service providers, and industry groups are energetically tackling various aspects of VOP. This Special Report, and the Generic Requirements (GRs) that will follow it, a part of a program that can make a substantial contribution to the success of service providers and suppliers.

For service providers evolving existing networks to support VOP, this program, consisting of this SR and subsequent GRs, will provide a migration from current systems, maximizing reuse of assets already in place. For service providers deploying new networks, it will provide a basis for interconnection and interoperability with existing infrastructure, maximizing the ubiquity and utility of the new service. For all service providers, this program will promote carrier-grade performance and scalability, two attributes critical to sustained commercial viability. The added benefit to service providers of widely accepted GRs is the availability of compatible solutions from multiple suppliers, resulting in faster time to market and lower costs.

For suppliers of VOP technologies, this program offers a significant reduction of the risks of developing new and enhanced products. This risk reduction flows from the better definition of customer requirements inherent in GRs, and from the commonality of requirements among multiple customers.

This GR program is intended to build on the strength of existing standards projects, and to facilitate the innovation of service providers and suppliers. The GRs will provide an end-to-end view of service capabilities and a comprehensive view of network elements, which is essential to consistency, interoperability, scalability, manageability, and reliability. The GRs will provide added value through the following activities:

1. Integrating multiple standards applicable to a given network element or service capability

2. Defining specifics of the interpretation of a standard which are necessary to assure consistent and interoperable implementations
3. Including additional recommendations regarding functionality not addressed by standards
4. Addressing both the networking and the operations functionality of VOP technology.

Bellcore has established a strong record of accomplishment in developing GRs that provide these benefits to industry. Bellcore GRs have assisted service providers in planning their networks, and in purchasing equipment for interconnection within those networks. Moreover, suppliers have benefited from Bellcore's GRs in designing their products to meet the needs of their customers. The wide-spread utilization of Bellcore GRs is evident from the FCC's Network Reliability Council (NRC) 1996 survey that found that Bellcore GRs were the most widely-used reference on network reliability and integrity within the industry.

Bellcore GRs provide timely, high-quality implementable solutions that customers can consider. To achieve this, Bellcore provides leadership and the technical and editorial resources to produce GRs that satisfy deliverable milestones that have been contracted with customers.

The Bellcore GR process has been attractive to customers because it provides customers with an opportunity to accomplish the following:

- Shape the direction of work related to technologies and services that can potentially increase revenues or reduce the costs of service or product planning, implementation or operations
- Have early access to requirements information that can be factored into service or product planning and improve time-to-market
- Influence the technical content of the GR document
- Have a decision-making role in resolving any technical disputes
- Work with other industry leaders to discuss goals and solutions
- Receive a pre-publication copy of the GR before it is generally available to the public and then receive a final publication copy of the GR as soon as it can be distributed.

An added value of GR development is that companies that fund GR development work are granted a license to copy GR text for use internally, including majority affiliates, and to incorporate GR text in their product and service specifications. This feature is important to customers in communicating in the global economy and in reducing the costs associated with documenting the features and characteristics of products and services.

3. Characteristics of VOP Networks

The section describes characteristics of VOP networks from the following perspectives:

- Target customers for VOP services (see Section 3.1)
- Types of calls that VOP networks can handle (see Section 3.2)
- Types of VOP services that can be offered (see Section 3.3)
- Impacts Customer Premises Equipment (CPE) may have in the deployment and consumer acceptance of VOP services (see Section 3.4)
- VOP network attributes and capabilities required to support these services (see Section 3.5)
- Types of business agreements that might exist between VOP service providers and their customers (see Section 3.6)
- Regulatory and policy issues that may need to be addressed by VOP service providers (see Section 3.7)
- Characteristics of VOP networks and how they relate to those envisioned for Next Generation Networks (see Section 3.8).

In addressing the topics above, the overall purpose of this section is to provide a foundation for the remaining sections of this document.

This section follows an overall philosophy to focus primarily on replicating the voice and other narrow-band services currently offered via the public switched telephone network (PSTN). This means achieving service parity (and in many cases, transparency to the end-user) via seamless inter-working with the PSTN in the initial VOP networks.

It is recognized, however, that a driving motivation for VOP networks is the rapid deployment of many new and innovative services, including multi-media services. Therefore, a key requirement of the VOP networks discussed in this document is to complement and/or support the deployment of these new services.

3.1. Target Customers and Markets for VOP Services

The target customers for VOP services include both retail and wholesale markets. For the most part this section will focus on retail services.

Target retail customers for VOP services are expected to include the following:

- Business customers (e.g., for Long Distance, 800, Centrex, and ISDN PRI Services)
- Residential customers (e.g., for Long Distance, CLASS and BRI Services)
  - Subscribed customers
  - Casual users (e.g., those who use alternate interexchange carriers, such as by dialing 101XXXX on a per-call basis, or those who dial 1-800 access on a per-call basis).
  - Wireless customers (e.g. cellular, PCS, and fixed wireless services).

Certain services might only be offered to residential customers, while others may only be offered to business customers. For example, residential customers may not have access to service management capabilities. Similarly, business customers behind private branch exchanges (PBXs) may not need access to a network-provided Call Forwarding feature.

In addition to supporting retail service offerings, VOP networks may be used to provide wholesale network services to other service providers. For example, one provider could sell operator services on a wholesale basis to another service provider that does not have its own. Or, one provider could wholesale its toll-free services to another provider for the latter to resell to its customers.

3.1.1. Customer Perspective

Consideration of retail and wholesale customers' perspectives is critical to the implementation of VOP networks and services.

The following assumptions generally apply to VOP services:

- Customers will want their existing telephone and computer equipment to continue to work.
- Customers will want their current services to continue to work, and work at least as well as they do now
- Customers will want the same type of interface, or better, than they have now.

Potential customer motivations for using VOP services may include the following:

- To save money – the use of VOP services may represent cost savings to the customer. In fact, certain customers may be willing to live with less (or different) quality and/or functionality in return for reduced prices or other benefits. Also, some providers may be able to implement services more cost-effectively via a wholesale arrangement with a VOP provider than they could themselves.
- Because it is "cool" – so that individuals can brag to their friends and associates that they have the latest technology. Similarly, companies can enhance their image as a "high-tech" company by employing VOP capabilities.
- For convenient access to new services - (e.g., it facilitates "push to talk" features or enables integrated services such as Internet Call Waiting to work more efficiently, as well as to support other integrated media services).
- Because their service provider is not giving them a choice (i.e., the service provider is using VOP to reduce their own costs and, in fact, the customer may not even be aware that VOP technology is being used).

3.2. Types of VOP Calls Supported

In this document, it is assumed that calls can be established between the following types of end-users:

- VOP network subscriber-to-VOP network subscriber

- VOP network subscriber-to-PSTN/ISDN subscriber (and *vice versa*)
- PSTN/ISDN subscriber-to-VOP network subscriber
- PSTN/ISDN subscriber-to-PSTN/ISDN, via a VOP network.

A "VOP network subscriber" is loosely defined as a customer who subscribes to services provided by a VOP network. The interface to such a subscriber may or may not be packet-based. The types of calls that can be established include voice calls, circuit switched data calls (perhaps via circuit emulation), and packet switched calls.

3.3. VOP Services

This section provides an overview of the possible scope and nature of VOP service deployment. As mentioned earlier, the initial goal is to replicate the voice and other narrow-band services currently offered via the PSTN.

3.3.1. Scope of VOP Services

The scope of VOP services addressed in this document includes the following types of voice services currently offered via the Public Switched Telephone Network (PSTN):

- Plain Old Telephone Service (POTS)
- Mobile telephone service
- 800/888/877 and other toll-free services
- 900 and other Information Services
- Custom Calling Features
- CLASS^{SM} Features
- Centrex Features (Line-Side Interface) and other Basic Business Group (BBG) services
- ISDN BRI Services (Line-Side Interface)
- ISDN PRI Services (Trunk-Side Interface)
- Advanced Intelligent Network (AIN) Features
- Voice Messaging Features
- Operator Services, both manual and automated (e.g., alternate billing, Directory Assistance, operator assistance)
- Repair
- E-911.

3.3.2. Features and Services Supported by a VOP Network

This section lists specific existing voice and other narrow-band retail features and services that may need to be supported by a VOP network. Sections 3.3.2.1and 3.3.2.2 address residential and business features and services, respectively. Some features operate independently of a call and these features are discussed in the context of call independent features. Section 3.3.2.4 addresses Advanced Intelligent Network (AIN) features that may need to be supported by a VOP network.

It is assumed that a VOP network supports analog line terminations as well as ISDN line terminations. The services to be provided for these lines should be consistent, to the extent feasible, with those provided in today's circuit switched network. It is assumed, for example, that "busy" is defined as in today's PSTN/ISDN networks for access lines. In accordance with those definitions of busy, "busy-related" features (e.g., call forwarding on busy) will be expected to operate as they do today.

For each service listed below, there is a designation provided in square brackets [ ] of either "I" or "II", to indicate, for illustrative purposes, how a VOP Service Provider might establish service deployment priorities. I denotes a higher priority than II. In some cases, this might be a reflection of the current market penetration of the service; in another instance, it might indicate a regulatory requirement; in still others it may reflect the relative level of technical complexity required to support the service or feature. *This designation does not constitute a Bellcore recommendation.* Depending on the nature of the VOP service provider, it may elect to offer different subsets of VOP services, or follow a different deployment strategy.

High-level definitions of each of the services listed below can be found in Appendix A.

Descriptions of capabilities and functions needed to support these services are provided in Section 3.5 and in Appendix B.

3.3.2.1. Services Provided to Residential Customers

3.3.2.1.1. Basic Features

- Dial Tone [I]
- Feature Group D Dialing [I]
- Call Completion (Local, intraLATA Toll, interLATA, International) [I]
- Access to Toll-Free Numbers [I]
- Access to E-911 Service [I]
- Operator Assistance for Call Completion and other assistance (0, 00, or Equivalent) [I]
- Access to Repair (611 or Equivalent) [I]
- Local Number Portability (LNP) [I]
- Automated Alternate Billing and Pre-Pay Services [II]
- Access to Directory Assistance (411 or Equivalent) [II].

3.3.2.1.2. Custom Calling Features

- Call Waiting [I]
- Call Forwarding on Busy Line (CFB) [I]
- Call Forwarding on No Answer (CFDA) [I]
- Speed Dialing [II]
- Three-Way Calling [II].

3.3.2.1.3. CLASS Features

- Calling Number Delivery [I]
- Calling Name Delivery [I]
- Distinctive Ringing / Call Waiting (DR/CW) [I]
- Calling Number/Name Presentation Restriction [I]
- Automatic Callback (AC) [I]
- Automatic Recall (AR) [I]
- Caller Identity Delivery on Call Waiting (CIDCW) [I]
- Call Waiting Deluxe (CWD) [I] a service best supported by ADSI CPE
- Anonymous Call Rejection (ACR) [I]
- Outside Area Calling Alerting (OCAA) [II]
- Call Screening [II]
- Selective Call Forwarding [II]
- Selective Call Acceptance [II]
- Selective Call Rejection [II]
- Bulk Calling Line ID (BCLID) [II]
- Remote Call Forwarding [II].

3.3.2.1.4. Other Features

- NPA Split Management [I]
- Network-Based Voice Mail [I]
- Visual Message Waiting Indicator (VMWI) [I]
- “Teen Line” [I]
- Multi -Party Lines [II]
- Outgoing Call Restriction / Customized Code Restriction [II]
- Voice-Activated Dialing [II]
- ISDN Flexible Call Management [II]
- ISDN Additional Call Offering Service [I].

3.3.2.1.5. Call-Independent Services

Call-independent services are features that can be invoked without the establishment of a call. This includes the ability to turn features on and off, and to create/maintain screening lists, such as the following:

- VMWI [I]
- Cancel Call Waiting [I]
- Customer Originated Trace (COT) [I]
- Call Forwarding Variable (CFV) [II]
- Ring Control [II]
- Screening List Editing [II]
- Visual Screening List Editing [II] an ADSI-based service.

ISDN-specific call-independent services include the following:

- ISDN Parameter Downloading (helps automate the terminal setup process) [I]

- ISDN Inspect (allows the user to determine the meaning of certain keys on the terminal) [II].

Because of the nature of the signaling capabilities available to ISDN lines, ISDN terminals, as defined by National ISDN, generally are required to identify themselves with the network through a process called terminal initialization. It is expected that the VOP network will support terminal initialization. In addition, the VOP network is expected to support the Auto-SPID capability, which helps decrease the human user involvement in the terminal initialization procedure.

3.3.2.2. Services Provided to Business Customers

Business customers should be provided with many of the same services suggested for residential customers, at least the Basic Features of Section 3.3.2.1.1, plus the services listed below.

3.3.2.2.1. Services Offered to Businesses by Network Service Providers

- Toll-free service (wholesale or retail, e.g., 800/888/ Inward Wide Area Telecommunications Service - INWATS) [I]
- Outward Wide Area Telecommunications Service (OUTWATS) [II]
- Basic Business Group (BBG) Features including Centrex features and private network access [II]
- PBX Network Services [II].

3.3.2.2.2. Centrex Features

- Custom Calling Centrex Features [II]
- CLASS Centrex Features [II]
- Extension Dialing [II]
- Call Transfer [II]
- Call Pickup [II]
- Conference Calling – Six-Way Station Controlled [II]
- Series Completion [II]
- Multi-Line Hunt Group [II]
- Attendant Features [II].

3.3.2.2.3. Private Virtual Networks

- Private Virtual Networking (PVN) features [II].

3.3.2.2.4. ISDN PRI

Ninety percent of PBXs have call-associated-signaling trunk interfaces to the end-office. In general, it is assumed that the CPE served by the ISDN PRI Trunk is a PBX, although it does not have to be limited to a PBX. Since PBXs already provide a number of capabilities and services to the end users that they serve, not all services provided to analog lines and ISDN BRIs are offered via ISDN PRIs.

It is assumed that a National ISDN PRI is used for this trunking interface. On this interface the following services, at a minimum, need to be supported by the VOP network:

- Calling Number/Redirecting Number Reception [I]
- Calling Number/Redirecting Number Delivery [I]
- Calling Name/Redirecting Name Delivery [I]
- Call-by-Call Service Selection [II]
- PRI Two B-Channel Transfer [II]
- PRI-based Private Networking Features [II].

The above listed features require support by the VOP network.

In addition, it is assumed that the VOP network will provide tones and announcements for originated calls under certain conditions. The PBX is expected to provide certain tones and announcements to its end-users. These include dial tone, recall dial tone, audible ringing, and busy tone.

3.3.2.3. Voice Services Provided to Mobile Telephone Customers

3.3.2.3.1. Basic Features

- Call Completion (Local, Toll, Long Distance, International) [I]
- Call Delivery while Roaming [I]
- Incoming Call Barring [I]
- Outgoing Call Barring [I]
- Access to Toll-Free Numbers [I]
- Access to 911 Service [I]
- Operator Assistance for Call Completion (0, 00, or Equivalent) [I]
- Repair (611 or Equivalent) [I]
- Local Number Portability (LNP) [I]
- Automated Alternate Billing and Pre-Pay Services [I]
- Directory Assistance (411 or Equivalent) [II].

3.3.2.3.2. Custom Calling Features

- Call Waiting [I]
- Call Forwarding on Busy Line (CFB) [I]
- Call Forwarding on No Answer (CFDA) [I]
- Call Forwarding Default [I]
- Three-Way Calling [II].
- Call Hold [II]
- Call Transfer [II].

3.3.2.3.3. CLASS Features

- Calling Number Delivery [I]
- Calling Name Delivery [I]

- Distinctive Ringing / Call Waiting (DR/CW) [I]
- Calling Number/Name Presentation Restriction [I]
- Automatic Callback (AC) [II]
- Automatic Recall (AR) [II]
- Caller Identity Delivery on Call Waiting (CIDCW) [I]
- Call Waiting Deluxe (CWD) [I]
- Anonymous Call Rejection (ACR) [I]
- Outside Area Calling Alerting (OCAA) [II]
- Call Screening [II]
- Selective Call Forwarding [II]
- Selective Call Acceptance [II]
- Selective Call Rejection [II]
- Password Call Acceptance [II]
- Subscriber PIN Access [I]
- Subscriber PIN Intercept [I].

3.3.2.3.4. Other Features

- NPA Split Management [I]
- Network-Based Voice Mail [I]
- Message Waiting Indicator (MWI) [I]
- Voice-Activated Dialing [I]
- Dispatch Group [II]
- Calling Party Pays [II]
- Mobile Access Hunting [II]
- Priority Access and Channel Assignment [II].

3.3.2.3.5. Call-Independent Services

Call-independent services are services that can be invoked without the establishment of a call. This includes the ability to turn features on and off, and to create/maintain screening lists, such as the following:

- Over the Air Activation [I]
- Cancel Call Waiting [I]
- Customer Originated Trace (COT) [II]
- Call Forwarding Variable (CFV) [II]
- Screening List Editing [II]
- Visual Screening List Editing [II].

3.3.2.4. AIN Features

Completing an AIN service typically requires the telephone network to perform a sequence of events organized by sophisticated software. This process involves a series of rapid interactions between elements of the AIN network, especially between the SSP and SCP. An additional AIN network element may be involved with some services. AIN services that may need to be supported by a VOP network include the following:

- Area-Wide Networking [II]
- Call Center Management [II]

- Calling Name Delivery [II]
- Calling Party/Paging Party Pays [II]
- Centrex Extend [II]
- Customer Location Alternate Routing [II]
- Do Not Disturb [II]
- Follow Me Service [II]
- Government Emergency Telephone Service (GETS) [II]
- Intelligent Redirect [II]
- Network Switch Alternate Routing [II]
- Outgoing Call Restriction [II]
- Prime Number [II]
- Remote Access Forwarding [II]
- Selective Call Acceptance [II]
- Virtual Private Network [II]
- Work at Home [II]
- 500 Access Service [II].

3.4. Role of CPE

The type of Customer Premises Equipment (CPE) and access method employed by the end user may greatly impact the nature and availability of VOP services. For example, placing even a simple VOP phone call can be markedly different for the end user, depending on whether they are using a traditional telephone or a PC.

It is imperative that VOP services can be accessed from current CPE (e.g., the ability to place a long distance or international call that employs VOP from a traditional 2500 set).

The use of PCs and other advanced CPE will not only help make VOP technology transparent to the end user, but will also facilitate the use of advanced services such as Unified Messaging.

In general, advantages of VOP might be as follows:

- Cumbersome dialing arrangements for some PSTN-based vertical voice services might be avoided by using advanced, IP-compatible CPE or mobile terminal (MT).
- Services which are impacted or limited by the alternate voice/data nature of the analog telephone network (Call Waiting and Caller ID on Call Waiting) might be re-designed to benefit from simultaneous voice/data.
- Service integration with emerging IP-based services, such as Unified Messaging and Web-based directory services, is made much easier and can also take Computer-Telephony Integration to new levels of efficiency and convenience.
- Voice service usage will become more aligned with emerging “point-and-click” and “click-to-talk” service management and support capabilities.

The following types of CPE are assumed to be available for use in conjunction with VOP services:

- Standard corded and cordless telephone sets (e.g., 2500 sets)

- Type I Analog CPE (i.e., compatible with Caller ID and Visual Message Waiting Indicator services)
- Type II Analog CPE (i.e., includes Type I functionality and is also compatible with Calling Identity Delivery on Call Waiting services)
- Type III Analog CPE (i.e., includes Type II functionality and is also compatible with the Analog Display Services Interface (ADSI))
- ISDN sets (must support terminal initialization)
- PBXs (with ISDN or analog interfaces), including those sets behind the PBX
- IP PBXs
- IP Phones
- Set-top Boxes (Cable Equipment)
- Wireless handsets (both analog and digital)
- PCs, both directly connected (e.g., via ADSL or other Digital Subscriber Lines – collectively referred to as xDSL - or cable modem) and those behind routers/LANs
- Message Storage and Retrieval (MSR) Systems.

3.5. Network Aspects

This section describes the network aspects of VOP networks.

3.5.1. Required Attributes of a VOP Architecture

Any VOP network architecture is assumed to possess the following attributes:

- *Cost-effective* – implementable and manageable at a cost that allows the service provider to achieve the desirable rate of return on investment
- *Realizable in the next one to two years* – technically and practically implementable in the stated time frame
- *Provides required Quality of Service (QOS)* – support required levels of quality of service
- *Scalable* – grows gracefully from small implementations to larger deployments
- *Inter-operates with existing networks* – backward compatible with existing voice and data networks
- *Open (interfaces)* – based on an open architecture and open interfaces to other networks and to CPE
- *Reliable* – provides the required level of reliability
- *Secure* – assures privacy of customers' information and able to withstand "attacks"
- *Evolvable* – offers one or more migration paths to networks capable of supporting more advanced, multi-media, broadband services.

3.5.2. Network Interconnections Required

A VOP network will need to interconnect and inter-work with several different types of networks, including existing circuit-switched telephony networks, existing data networks, and broadband networks. Specific interworking scenarios are as follows:

- VOP network-to-PSTN/ISDN

  This includes interworking such as Multi-frequency (MF) operator services signaling, MF 911 calls, SS7 ISUP signal transport, and SS7 TCAP queries.

- VOP network-to-Internet
- VOP network-to-ATM network
- VOP network-to-Frame Relay network
- VOP network-to-other VOP network.

3.5.3. Capabilities to be Supported by VOP Network

This section identifies some of the key capabilities that will need to be provided and/or supported by the VOP network in order to enable the services discussed earlier. These capabilities will impact the functional requirements of the elements of the VOP network to be discussed in Section 5. A more detailed description of these capabilities and more examples from existing networks are found in Appendix B.

3.5.3.1. Originating Services/Capabilities

This section provides a list and high-level definition of originating end network call processing capabilities, and services capabilities upon which services depend.

3.5.3.1.1. Call Originating Capabilities

On an originating call basis, the VOP capabilities that are to be provided include the following:

- *Ability to Access Intelligent Network Services*

  This is the ability during the originating end call processing for the network to activate Intelligent Network (IN) service processing when one or more defined IN trigger conditions are encountered.

- *Ability to Access Originating End Vertical Network Services*

  This is the ability to modify any of the call processing capabilities defined below with installed and activated originating end vertical service capabilities. These vertical service features are distinct from the IN services discussed above, but may interact with the IN services to perform a service for an end user. Originating end network capabilities that support the service specific processing are mentioned in Section 3.5.3.1.2.

- *Ability to Scan for and Detect an Origination Attempt Signal or Message*

  This is the ability for the network, when an access interface is idle, to scan for and detect the occurrence of a signal or message from an entity requesting originating end

call processing by the network (e.g., the network receives an off-hook indication from an idle non-ISDN line).

- *The Ability to Verify the Authority of a User to Place a Call*

  This is the ability to verify the authority of a calling entity (e.g., user CPE or incoming trunk) to continue to place the call with the given properties (e.g., line restrictions).

- *The Ability to Provide Call Denial Indication*

  If call placement is denied, the network must provide an ability to send a denial indication to the calling entity, and wait to detect call abandonment, or to time out then return to idle.

- *The Ability to Detect Call Abandonment*

  This is the ability to, at any time during the originating call setup processing, to detect that the calling entity has abandoned the call before it has been answered, and to return to idle.

- *Ability to Request and Receive Call Control or Call Processing Information*

  This ability enables the network to send an indication to the calling entity that the network is ready to receive the service request, along with the ability to collect further information about the request from the calling entity.

- *Ability to Analyze and Act On Collected Call Control or Call Processing Information*

  This is the ability of the network to analyze call control or processing information collected from the calling entity, and to decide how to further treat the call (e.g., route it or activate a vertical service feature).

- *Ability to Route the Call*

  This is the ability of the network to route a call to a destination network interface or node designated by the calling entity (e.g., to a destination CPE). For wireless networks, this includes the ability to locate and route calls to roaming subscribers.

- *Provision of Network Busy Indication*

  This is the ability of the network to send to the calling entity an indication that it is unable to route the cal (e.g., to send a “fast busy” signal). The network should then provide Call Abandon or Call Placement Denial processing.

- *Ability to Derive Information Needed for Call Setup*

  This is the ability of the network to derive additional information needed by the terminating end to complete call setup beyond what was received from the calling entity, including all originating caller information (e.g., Calling Party ID).

- *Ability to Send Call to Terminating End Call Processing*

  This is the ability of the network to send an indication of the desire to setup a call to the terminating end call processing, and to pass collected or derived call information to the appropriate terminating end capabilities.

- *Ability to Receive and Respond to Call Progress from Terminating End Call Processing*

  This is the ability of the network to receive and act on call progress indications from the terminating end call processing, informing the originating entity as needed.

- *Provision of Active Call Capabilities*

  This is the ability of the network to provide for voice transmission within the expected performance levels, and for detection of indications of activation of mid-call vertical services, or of caller or called entity disconnection.

- *Provision of Call Release Capabilities*

  This is the ability of the network originating end to respond to an indication of calling entity disconnection (e.g., detection of on-hook), or called entity disconnection (e.g., on-hook), or reconnection (e.g., off-hook) to clear or restore the active call. Other network controls may also cause call release.

3.5.3.1.2. Originating End Service-Support Capabilities

This section presents a list and high-level description of generic originating end capabilities intended to support known vertical services, such as the following:

- *Provide Vertical Service Feature Activation/Deactivation Indication*

  This is the ability for the network to provide the calling entity with a service-specific indication that an originating end vertical service feature has been activated or deactivated.

- *Record, Store, and Play Audible Announcements*

  This is the ability to record audible announcements, including voice messages and standard network signals and tones (e.g., Call Progress Announcements such as Intercept announcements). This also comprises the ability to store these announcements such that they may be accessed and played to end users under control of a particular originating end capability.

- *Voice Response*

  The originating end must support voice response capabilities (e.g. for Voice Activated Dialing).

- *PSTN Supervisory and Address Signals*

  The originating end must support all PSTN line and trunk supervisory and address signals, including caller-generated signals such as DTMF, and operator services tones and signals.

- *Call Progress Tones*

  Generation of PSTN Call Progress Tones, such as audible ringing, needs to be supported, and receipt of an indication from the terminating end that these tones need to be generated needs to be supported.

- *Communicate via SS7 Protocols*

  This is the ability to communicate via Signaling System 7 (SS7) ISDN User Part (ISDNUP) and Transaction Capabilities Access Part (TCAP) data communications

protocols over Common Channel Signaling (CCS) links with CCS entities such as PSTN SSP switching systems, and SCPs, including Line Information Databases (LIDBs), or other AIN databases.

- *Call Hold*

  This capability allows the network to separate, but not clear, a call from a controlling end entity in order for this entity (such as an end user via a CPE) to initiate a new call, retrieve another already held call, or possibly join two calls to form a three-way call.

- *Call Retrieve*

  This ability allows the network to retrieve a held call. The held call may also be joined with another call and the entity.

- *Outgoing Memory Slot Administration*

  This is the ability to enter and store the last number "dialed", which is needed for PSTN Automatic Callback service (*66).

- *Determination of Calling Party Identity*

  These are the specific abilities to determine calling party identity and privacy choice from the calling entity to support Caller ID services, to allow the calling entity to modify their default privacy choice on a per-call basis, and to be able to convey these to the terminating end.

- *Provide Automatic Identified Outward Dialing*

  With the AIOD feature, the Private Branch Exchange (PBX) provides the local switch with the identification of the PBX originating line (or attendant) for charge recording purposes. The AIOD information is forwarded to the switch over a dedicated data link.

- *Provide Billing Data*

  This is the ability of the originating end to track and store (i.e., collect and record) appropriate Automatic Message Accounting (AMA) data for use in billing the call.

- *Provide Operator Services Signals*

  This is the ability of the network to generate and send to the calling entity various signals or messages pertinent to operator services or Alternate Billing Services (ABS) during call origination.

3.5.3.2. Terminating Services/Capabilities

This section provides a list and high-level definition of terminating end network call processing capabilities, and services capabilities upon which services depend. On a terminating basis, the capabilities that are to be provided include call terminating capabilities and terminating end service-support capabilities.

3.5.3.2.1. Call Terminating Capabilities

On a call-terminating basis, the capabilities that are to be provided include the following:

- *Ability to Access Intelligent Network Services*

This is the ability during the terminating end call processing for the network to activate Intelligent Network (IN) service processing.

- *Ability to Access terminating End Vertical Network Services*

  This is the ability to modify any of the call processing capabilities defined below with terminating end vertical service capabilities. Activation of these capabilities may result in different network responses and indications. These vertical service features are distinct from the IN Services discussed above, but may interact with the IN services to perform a service for an end user.

- *Ability to Scan for and Detect a Termination Attempt Signal or Message*

  This is the ability for the network to scan for and detect a request for terminating end call processing and to receive collected or derived call information.

- *Ability to Authorize Call Termination*

  This is the ability of the network terminating end to verify its authority to route this call to the terminating entity.

- *The Ability to Detect Call Abandonment*

  This is the ability to detect that the calling entity has abandoned the call before it has been answered by the called entity.

- *Ability to Select Facility for Call Presentation*

  This is the ability of the network terminating end to check the busy/idle status of the called entity and to indicate the status to the originating end.

- *Ability to Present the Call to and Alert the Called Entity*

  This is the ability for the network terminating end to alert the called entity about the incoming call, and to detect when the terminating entity has accepted, answered or rejected the call, or when the calling entity has abandoned the call.

- *Provision of Active Call Capabilities*

  This is the ability of the network to provide for voice transmission within the expected performance levels, and for detection of mid-call vertical service activation.

- *Provision of Call Release Capabilities*

  This is the ability of the network terminating end to respond to an indication of calling entity disconnection, or called entity disconnection or reconnection, to clear or restore the active call. Other network controls may also cause call release.

3.5.3.2.2. Terminating End Service-Support Capabilities

This section presents a list and high-level description of generic terminating end capabilities intended to support known vertical services.

- *Conference Bridge*

  This capability allows a terminating end network conference call service, or multiway calling service, in which several calls are completed each to a port of the network conference bridge. Once each call is active on the bridge, all callers can communicate with each other through the bridge.

- *Record, Store, and Play Audible Announcements*

  This is the ability for the terminating end to record audible announcements, including voice messages and standard network signals and tones. This also comprises the ability to store these announcements such that they may be accessed and played to end users.

- *Voice Response*

  The terminating end must support voice response capabilities, e.g., for Voice Activated Network Control (VANC) services.

- *Call Progress Tones*

  Generation of PSTN Call Progress Tones, such as audible ringing, by the terminating end (or reception from another network), transmission from the terminating end to the originating end of the network, and their regeneration by the originating end to a calling entity, needs to be supported.

- *Communicate via SS7 Protocols*

  This is the ability to communicate via Signaling System 7 (SS7) ISDNUP and TCAP data communications protocols over Common Channel Signaling (CCS) links with CCS entities such as PSTN SSP switching systems, and SCPs, including Line Information Databases (LIDBs), or other AIN databases.

- *Distinctive Alerting*

  This is the ability for the terminating end to generate distinctive alerting indications (e.g., Distinctive Ringing) to serve as notification to called parties of special events.

- *Transmit Calling Party Identification to Terminating Entity Being Alerted*

  This is the ability to send the Calling Party Number and Name information to the terminating entity being alerted.

- *Call Waiting Alerting*

  This is the ability to provide a unique notification (audible for analog lines) to a terminating entity, such as an end user already engaged on a call, that another call is waiting. The call waiting service typically allows the called party to use call hold and retrieve capabilities to alternate between the held and active call.

- *Caller Identity Delivery on Call Waiting Alerting*

  CIDCW is the ability to transmit the CPE Alerting Signal (CAS) of the CLASS CIDCW feature, as well as non-ISDN Calling Party Identification to the Terminating Entity being alerted.

- *Direct Inward Dialing*

  DID is the terminating end network capability to support the special signaling protocol for DID trunks to a PBX.

- *Call Hold*

  This ability allows a terminating end network to separate a call from a terminating entity such as a called CPE. The separated call is not cleared.

- *Call Retrieve*

  This ability allows a terminating end network to retrieve a held call.

- *Incoming Memory Slot Administration*

  This is the ability to enter and store the number of the last incoming call, which is needed for PSTN Automatic Recall service (*69) or Customer Originated Trace service.

- *Call Forwarding*

  This is the ability to redirect or reroute the incoming call when requested by a vertical service to the destination indicated by the service.

- *Billing*

  This is the ability of the terminating end to track and pass to the originating end Billing feature, on request, appropriate active call data, typically called Automatic Message Accounting (AMA) data, for use in billing the call.

- *Operator/Attendant Barge-in, Busy Verification, or Emergency Override Support*

  This is the ability of the terminating end to provide the special means for operator or attendant features to determine the busy versus idle condition of a called line and to connect to the selected line.

3.5.3.3. Network Services/Capabilities

This section lists and briefly defines network capabilities that are independent of call processing. Communications and other capabilities in support of Operations are not explicitly considered in this section, but are addressed in later sections. Local Number Portability support is covered in Section 3.7.7.

- *Communicate via SS7 Protocols*

  This is the ability to communicate via Signaling System 7 (SS7) ISDNUP (ISUP) and TCAP communications protocols over Common Channel Signaling (CCS) links with CCS entities such as PSTN SSP switching systems, and SCPs, as well as to communicate with Billing systems and provide equal access to long distance providers.

- *Communication with Billing Systems*

  This is the ability of the network to communicate collected billing records to billing systems for processing.

- *Screening List Editing*

  This is the ability to edit various service-specific databases stored on the network.

- *ISDN Customer Station Rearrangement*

  This is the ability to support movement of an ISDN station from one network port to another.

- *Message Service Notification*

  This is the ability for the network to communicate with a message service such that the message service host directs the network to route a standard notification of new messages waiting to the subscriber.

3.6. Business Aspects

This section focuses on the provision of voice and narrow-band services to business and residential customers who have contractual or other business relationships with the providers of the services. It also addresses the wholesale provision of connectivity services by a network provider to other services providers. The architectures described enable the participation of third parties in the execution of services, including those involving supplementary features.

The providers of the VOP services are assumed to be business entities who own and operate the packet-based networks and associated systems that support the services, or resellers of such services. The architectures described in this SR apply to networks owned by a single business entity, as well as networks comprised of components owned by multiple entities.

A proposed business model for VOP services is shown in Figure 3-1.

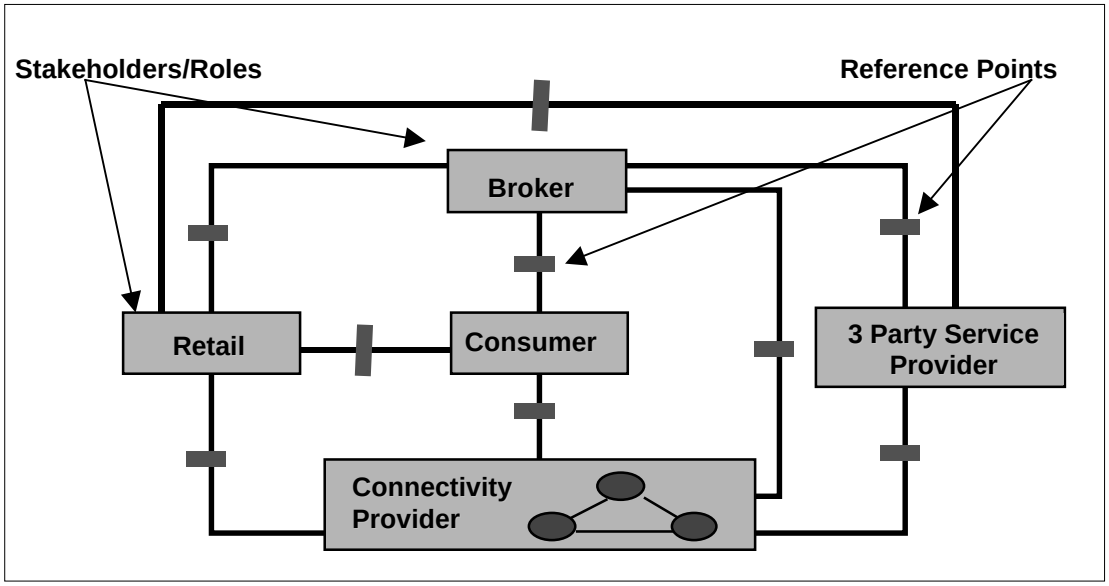

Figure 3-1 Business Model for VOP Services

There are five roles that one or more business entities could assume: Consumer, Retailer, 3rd-Party Service Provider, Connectivity Provider, and Broker. In many cases, the same entity will assume multiple roles. Briefly, these roles are defined as follows:

1. *Consumer* - typically the ultimate user/consumer of services
2. *Retailer* - provides retail services (primarily) to consumers
3. *Third-Party Service Provider* - provides "wholesale" services (primarily) to retailers

4. *Connectivity Provider* - provides basic connectivity services using a packet-based network
5. *Broker* - manages information on services and stakeholders; matches "consuming" stakeholders with "providing" stakeholders.

The reference points represent the relationships among the stakeholders, e.g., business relationships and operational interfaces. For example, the third-party service provider and the connectivity provider will have service level agreements that will specify the revenue sharing and the operational metrics for the quality of service and network performance. There will also be physical and operational interfaces between their respective network elements and systems.

The VOP architectures described in this SR can support the roles of each of the stakeholders identified in the above business model.

Possible connectivity service providers include the following:
- ILECs
- CLECs
- ISPs
- IXCs
- Wireless providers
- Hub providers.

Possible service retailers include the following:
- ILECs
- CLECs
- ISPs
- IXCs
- Wireless providers.

Possible brokers include the following:
- Non-facilities-based resellers.

Possible third-party service providers include the following:
- Content providers
- Directory service providers
- Hub providers
- Management services providers (e.g., call center providers).

The above business model is specific to the support of services by VOP networks and service providers. A separate business model applies to the relationships between equipment suppliers and network and service providers.

3.7. Regulatory/Public Policy Aspects (U.S.)

This section addresses regulatory and policy aspects of VOP networks and service providers in the United States. Regulations and public policy impose special requirements on carrier networks. While many of these requirements have traditionally

applied to Incumbent Local Exchange Carriers (ILECS), several of them can be expected to apply to new entrants, as well. Some of the issues expected to impact VOP networks and service providers are highlighted in the following sub-sections.

3.7.1. Communications Assistance for Law Enforcement Act

CALEA defines wiretapping capabilities that Telecommunications Service Providers (TSPs) operating in the U.S. are required to provide to law enforcement agencies. In particular, TSPs must provide real-time access to all addressing, signaling, and other call-identifying information, as well as the content of each communications session to or from a subject under surveillance. CALEA requirements will have significant ramifications for future network architectures, especially those based on digital transmission, packet switching, and advanced signaling mechanisms, such as VOP networks.

CALEA requirements have not been widely implemented. Although the likelihood is that these will be incorporated into the network in the near future, they are not addressed in this document.

3.7.2. Privacy and Federal/State Legislation

Whatever the final outcome of the surveillance capabilities provided under CALEA, those capabilities are intended for use under Court authorization. Other FCC and State regulatory rules, which relate more generally to privacy, have been implemented in the interests of both the calling party and called party.

VOP service providers could be expected to comply with existing Federal and State rules associated with issues such as passing of Calling Party Number (CPN), user control of CPN presentation status, and the functionality of CPN-based features—rules which could vary from State to State. Flexibility to accommodate State-to-State variances from the FCC's baseline rules could be anticipated.

3.7.3. E-911

Access to Enhanced-911 emergency services will need to be supported by VOP networks. This includes being able to route an E-911 call to the correct Public Safety Answering Point (PSAP) for the determination of the calling party's physical location, including location of a wireless user.

3.7.4. Universal Service

VOP service providers may be required to support universal service, depending on several factors, including the nature of the VOP service provider (e.g., ILEC vs. CLEC) and characteristics of a particular serving area (e.g., whether or not the area can be served by other service providers).

While a VOP service provider is not obligated to support universal service, they may have to contribute to a universal service fund. In this case, this obligation is not expected to impact the requirements on the architecture and network requirements.

Support for Universal Service is not expected to impact the requirements on the architecture and network requirements, except for those for quality of service and

network performance. There may also be additional physical and operational interfaces in the network if Universal Service is supported.

3.7.5. Equal Access

It is likely that VOP service providers offering local telephony services will be required to support equal access to any and all long-distance carriers. This will have impacts on the requirements placed on the elements of the VOP architecture.

3.7.6. Unbundling

The FCC has been identifying requirements for network unbundling, including unbundling of local loops, transport and switching resources, signaling and control elements, operator services and directory assistance facilities, and operations support systems.

If network unbundling occurs, a requirement to unbundle VOP network capabilities would be most likely for ILECs who are offering VOP services through their traditional regulated company. This could significantly impact how they design their VOP network.

Although other VOP service providers may be required to unbundle their networks at some point in the future, it is not assumed to be immediate issue in the current design of their VOP networks.

3.7.7. Local Number Portability

As a result of the Telecommunications Act of 1996 and the advent of Competitive Local Exchange Carriers, local telephony service providers are required to support service provider Local Number Portability (LNP). This allows end customers to change their local service providers without having to change their directory numbers.

VOP service providers will be required to support LNP. Initially, the VOP network may be able to use the LNP functionality in the incumbent LEC's network via the appropriate business arrangements. However, the VOP service provider's initial customer may demand portable local numbers, and LNP capability may be needed in the VOP network at service inception., At some point it may be desirable and/or necessary to deploy LNP functionality in the VOP network. This could have a significant impact on the functionality of the elements of the VOP architecture.

3.7.8. Numbering Plans

Inter-working and translation among alternative addressing and numbering schemes (e.g., IP addresses to NANP directory numbers) will be required. Numbering and addressing plans that have to be considered include ITU-T Recommendation E.164 numbers, NANP numbers, Private Numbering Plan (ISO/IEC 11579) numbers, and IP addresses.

It is assumed that the VOP network will support both fixed IP Addresses and dynamically assigned IP Addresses. However, in the interest of limiting the scope of the functionality, the functionality to use dynamically allocated IP addresses is not explored in this SR. A

subsequent version of the SR will explore services using dynamically allocated IP addresses and the functionality needed to support them in the network.

The VOP network will require support of number pooling for conservation of NANP NPA-NXX codes. In addition, the VOP network will have to provide support of NANP expansion schemes, when approved by the Industry Numbering Committee (INC). However, these issues are also not explored in this SR and will be considered at a later stage.

3.8. Relationship of VOP Networks to Next Generation Networks

A VOP network can be thought of as an interim step toward a Next Generation Network (NGN). A definition of an NGN and the similarities and differences between VOP networks and NGNs are discussed in the following paragraphs.

3.8.1. What is a Next Generation Network?

An NGN is loosely defined to be a packet-based network that employs new control, management, and signaling techniques to provide *all* types of services, from basic, narrow-band voice telephony services to advanced broadband, multi-media services. Hence, the concept of an NGN encompasses VOP networks but is broader in scope. From an evolutionary perspective, a VOP network may evolve to an NGN.

3.8.2. What are the Drivers for NGNs?

Today's PSTN has been engineered to efficiently support voice telephony traffic and services. However, Internet traffic, and data traffic in general, are growing rapidly, and the trend is expected to continue. The volume of data traffic carried on public and private circuit-switched networks has surpassed (or soon will surpass) the volume of voice traffic. This suggests that, going forward, it will be more efficient to engineer and operate networks optimized to handle data traffic. Packet-based transport and switching technologies are logical choices for such networks. The implication is that, in the future, voice traffic should be handled as data in a packetized fashion.

As data traffic continues to grow, users of network services are increasingly seeking value-added, multi-faceted communications capabilities, from unified messaging to complete service and terminal mobility. Users are also seeking higher communications bandwidths and greater control over that bandwidth. An NGN is envisioned as a network that will be able to satisfy these demanding user needs, while promoting innovation, enabling new services and revenue streams, and reducing management costs and time to market.

Additional drivers for NGN include the following:

- Continued deregulation of the telecommunications industry
- Increasing competition among service providers
- Entry of new industry participants
- Convergence of computing and telecommunications
- Rapid evolution of computing and communications technologies.

As a result of these drivers, networks are expected to evolve from today's voice-dominated circuit-switched networks to broadband, packet-based networks. Figure 3-2 highlights the nature of this transition.

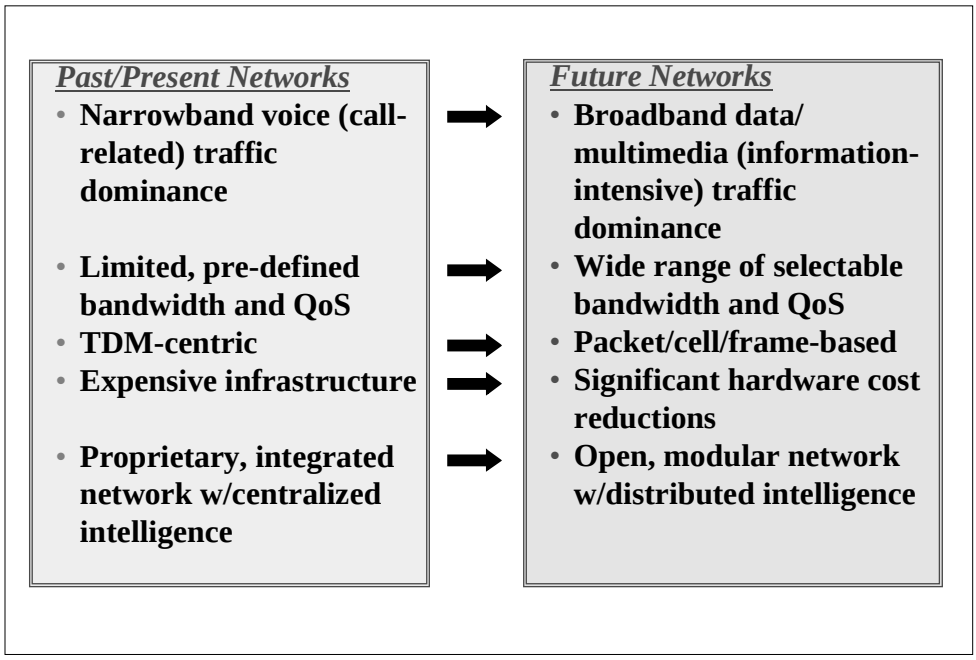

Figure 3-2 Networks in Transition

3.8.3. What are the Key Attributes of an NGN?

Elaborating on the key characteristics of an NGN, an NGN is assumed to provide the following:

- Support narrowband and broadband services
- Support simple as well as complex services
- Support service sessions with various degrees of complexity (e.g., suspendable, augmentable, rearrangeable, non-communications related, proxy controlled, etc.)
- Support multiple types of session topologies (e.g., point-to-point, point-to-multipoint, multipoint-to-multipoint)
- Provide all services over an integrated interface to a customer's premises
- Support all services on a single, integrated network
- Route, switch, and transport all information as packet data
- Employ packet technology for transporting user and network information
- Utilize service and resource control mechanisms that are separate from the routing, switching, and transport resources of the network

- Support existing and new access technologies
- Complement the capabilities of both simple and sophisticated CPE
- Provide high reliability
- Support open interfaces to users and to other service providers.

One area where NGNs will significantly differ from present networks is service control and signaling. Today's service control environments are very complex and increasingly difficult to manage. Quite simply, there are just too many protocols, too many types of systems, and too many types of required expertise and skill sets. To handle this heterogeneity, a smorgasbord of interworking or mediation devices are required. This frequently leads to high costs and difficulty in introducing new services to market. Components in today's environments are also very difficult to reuse, extend, and unbundle, and are becoming "out of synch" with emerging CPE and computing trends. Similarly, today's environments do not adequately support third-party software development and innovation. These limitations, together with the need to support increasingly complex services and session types, point to a need for a new service control paradigm for NGNs.

In an NGN, service control, including connection control, will be logically (and probably physically) separate from the underlying transport, routing, and switching functions of the network. The overall progression of service control – from simple circuit switched networks, through Advanced Intelligent Networks (AIN), to NGN – is summarized in Figure 3-3.

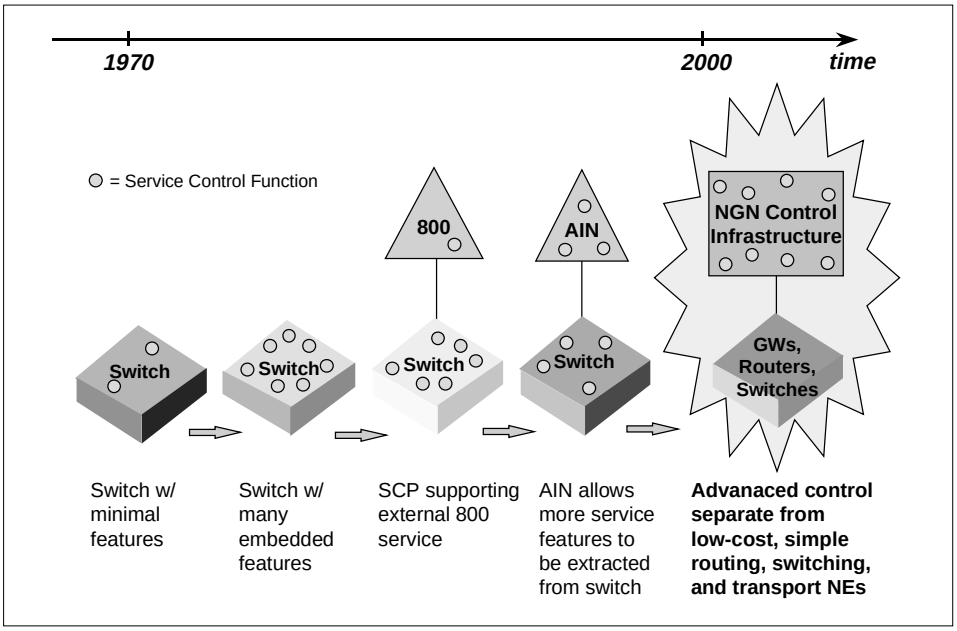

Figure 3-3 The Progression of Service Control

Another key attribute of NGN service control will be the use of distributed-object computing technologies, including Telecommunication Information Networking Architecture (TINA) and object-oriented middleware, such as Common Object Request

Broker Architecture (CORBA). In general, service control functions will be implemented as *application objects*, which will execute in *a distributed processing environment* based on distributed-object middleware. Objects executing on different computing platforms will communicate via an *inter-node communications network* based on IP and/or ATM. (The middleware and inter-node communications network together are roughly equivalent to a signaling network in today's environment.) This Next Generation control and signaling environment is depicted in Figure 3-4.

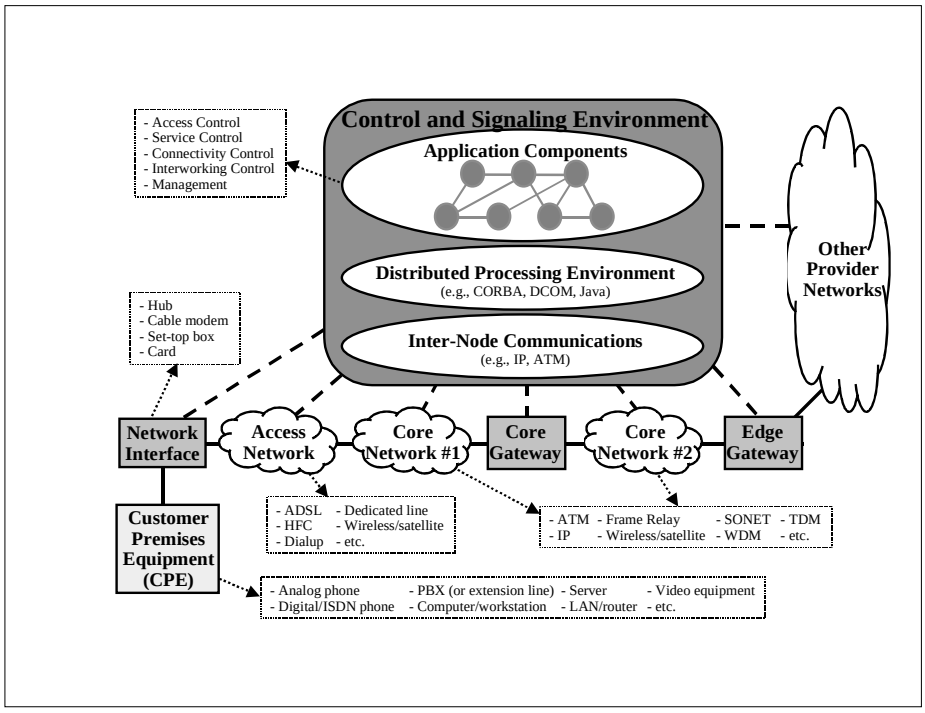

Figure 3-4 Next Generation Control and Signaling Environment

In a VOP network, service and connection control will also be separate from the underlying media gateways, routers, and switches. However, a VOP network is not as likely to employ formal, distributed object computing techniques as an NGN will. Also, in an NGN, control functions will be more specialized, resulting in a greater number of different, re-usable application objects. For example, in a VOP network, control will be divided into: (1) *Service Control* functions, such as those supporting supplementary features; and (2) *Call Control* functions, which support the basic set up and release of connections between communicating parties. In contrast, an NGN control architecture will consist of the following distinct functional groupings:

1. *Service Factory* – responsible for dynamically instantiating components to support service sessions.
2. *Session Management* – responsible for managing access, service, and communications sessions.
3. *Connectivity Management* – responsible for managing on-net to on-net and on-net to off-net connectivity across the underlying packet network (which may consist of multiple layer networks) and interworking gateways.

4. *Interworking Management* – responsible for managing interworking with the existing PSTN service architecture (e.g., via ISUP and TCAP). This includes control of lower layer gateway devices.
5. *Service Control/Support* – responsible for providing value-added capabilities to service sessions (e.g., supplementary features).
6. *Management Agent* – responsible for communicating fault, configuration, accounting, performance, and security information to management systems.

These separations of concerns are critical to an NGN being able to support advanced, multi-media, multi-party service sessions.

The NGN service control architecture is graphically depicted in Figure 3-5.

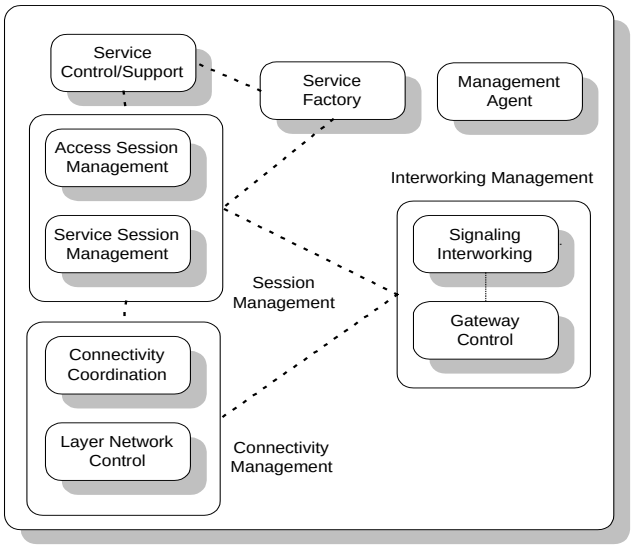

Figure 3-5 Next Generation Service Control Architecture

3.8.4. What are the Similarities and Differences between a VOP Network and an NGN?

Several of the differences and similarities between VOP and NGN have already been identified. These and others are summarized in Table 3-1.

Table 3-1 VOP Networks vis-à-vis NGNs

VOP Network	NGN
• Primarily narrow-band services (voice and data)	• Narrow-band and broadband services (voice, data, video)
• Simple services	• Simple and complex services (e.g., public network computing)
• Simple service sessions	• Multiple types of service sessions (e.g., multi-party, multiple service sessions per access session)
• Simple session topologies	• Multiple types of session topologies
• Integrated interfaces to users	• Integrated interfaces to users
• Integrated network	• Integrated network
• Packet-based switching and transport	• Packet-based switching and transport
• Control separate from the routing, switching, and transport	• Control separate from the routing, switching, and transport
• Service feature control separate from connection control	• Service feature control separate from service session management, which is separate from connection control

3.8.5. Evolution of a VOP Network to a Next Generation Network

From the preceding discussion, it is evident that a VOP network has much in common with an NGN. The NGN concept, however, encompasses a broader scope, particularly in terms of the numbers and types of services it is assumed to support. One can therefore envision that a network originally deployed as a VOP network could evolve to become an NGN. At a minimum, such an evolution would require:

- Augmenting the core transport and switching infrastructure and the access technologies to support broadband bandwidths
- Enhancing the service control infrastructure to support increasingly complicated services and service sessions.

4. Technology and Architecture Framework

4.1. Key Technology Considerations in Industry

This section discusses potential technologies that could be used in the deployment of VOP networks and services. The discussion offers several alternatives in key technologies areas and provides a brief analysis supporting the possible inclusion in the VOP architecture presented in Section 4.2. The analysis provided should be considered only in the context of VOP. The analysis does not extend to general fitness for other applications. The areas considered are by no means complete, but have been selected to consider those areas generally considered to be instrumental, and perhaps controversial, for the development of a VOP approach.

The following areas are considered:

- *Broadband Wireline Access:* The broadband wireline technology transporting analog, digital or IP voice traffic from the customer interface to network interface that provides access to the IP network
- *Wireless Access:* The wireless technology transporting analog, digital or IP voice traffic from the customer interface to network interface that provides access to the IP network
- *Data Transport:* The core technologies used to transport VOP packets within a provider's network
- *Packet Technologies:* The packet technology that is used to carry encoded voice traffic
- *VOP Protocols:* The protocols used for the encoding, signaling and control of VOP calls
- *Service and Network Management:* The technologies used to manage the VOP network and services.

4.1.1. Comparison and Trade-Off for Technology Choices

4.1.1.1. Data Transport

This section considers the various transport mechanisms that could be chosen to support one or more VOP techniques. For example, ATM can support Voice over ATM, Voice over IP and Voice over Frame Relay. The discussion of these packet alternatives is deferred until the next section.

4.1.1.1.1. Asynchronous Transfer Mode Transport

Advantages

ATM can handle voice traffic, as well as data traffic on the same network, with carrier-grade service quality. ATM has a several built-in techniques for ensuring a high grade of service. ATM uses short, fixed length cells that means voice traffic will not wait for long

packets to be transmitted. Thus, the transit delay is minimal. ATM also has traffic management techniques, such as admission controls and traffic policing that help ensure delay sensitive traffic gets through. ATM also has performance objectives for equipment that supports end-to-end performance objectives. All of these techniques support Quality of Service (QOS) in ATM equipment in a way that guarantees acceptable performance.

ATM can support IP, frame relay and cell relay services over the same platform. ATM offers the best integration of different services across switching, transport, and operations domains. ATM was developed, in part, because of its ability to simultaneously handle diverse applications. ATM supports connections that carry constant bit rate traffic as well as connections that carry variable bit rate traffic. In addition, ATM supports the flexible allocation of the access line bandwidth to logical connections supported across an interface. ATM also allows multiple services to be managed on a single network platform.

ATM can transport any of the candidate VOP formats. Because ATM can carry IP and frame relay traffic, it can support Voice over IP and Voice over Frame Relay, as well as Voice over ATM traffic.

Disadvantages

ATM adds an additional transport layer for IP or frame relay traffic. After packets or frames are created, they are encapsulated in ATM cells. Frame relay can also be translated into native ATM transport. Besides the overhead of both packets and cells, there are protocol procedures required to emulate the required IP or frame relay service. When the traffic is native ATM traffic (e.g., voice packetized directly into ATM cells), there is no additional transport layer.

ATM equipment tends to be more expensive than frame-based equipment. Putting traffic into cells is one reason for the equipment cost difference. Another reason is that ATM is more complex because it supports multiple services through explicit QOS support and traffic management. However, these are precisely the elements that may be needed in frame-based technologies to support voice and other real-time services, so the advantage may be less persistent.

ATM is a less mature technology than IP or SONET. ATM is a newer technology than either SONET or IP. Consequently, interoperable products, with the features necessary for voice support, have yet to reach the market. For basic PVC connections supporting some QOS categories, ATM technology is mature and interoperable. Other capabilities, such as AAL2 and SVC services, are in the early stages of deployment and interoperability testing.

Analysis

ATM is a worthwhile technology for the support of next generation voice networks. Support for voice service was designed in from the start, though the completion of that task is still work-in-progress. ATM can support many services well, including the transport of data, so it is an attractive choice for next generation networks. Though ATM is not strictly efficient from an overhead viewpoint, the ability to gain overall network efficiencies and manageability have led many enterprises and network providers to use ATM in their networks for IP and frame relay traffic transport.

4.1.1.1.2. Internet Protocol Transport

Advantages

IP is widely deployed. Almost all computers and a significant part of the data communications equipment are IP-aware. Much of the communications Research and Development (R&D) funds are directed at IP standards, products and services, so that even more of the communications infrastructure will use IP in some capacity.

IP can run over any transport technology. IP itself was designed to be independent of the underlying transport mechanism, although connectionless protocols tend to work easier with the IP toolbox of routing and address resolution mechanisms. IP can work with wireline or wireless, narrowband or broadband, or almost any other conceivable medium. A performance and financial benefit of this aspect is that IP can leverage advances in hardware performance and innovation more easily than most technologies. Recent examples have included 100 Mb and 1000 Mb ethernet, giga-routers and frame switching.

IP is a proven technology for data transport. The technology has been around for many years. It has been deployed, tested and enhanced. Network managers are comfortable and familiar with IP technology.

IP implementations are interoperable. The Internet is a testimony to the interoperability of equipment manufactured, deployed and managed by disparate organizations.

Disadvantages

Real-time support is incomplete and, consequently, performance is inconsistent. As the standards review indicated, IP is still lacking a proven set of real-time capabilities. Some elements, such as RTP, are mature, but most are still in the RFC process or waiting for the first vendor implementations. For some functions, the IETF is standardizing multiple approaches that have different degrees of usefulness in carrier networks. Several interim approaches can be used to manage performance. One approach is to use the conventional mechanisms (such as priorities, over-provisioning, and packet size control) to give a good, but not assured, level of performance. Another approach is to use an underlying ATM network for real-time support.

End-to-end management of performance in an IP network or internetwork is difficult. In a pure connectionless network with dynamic routing, control of performance is difficult due to the dynamic nature route calculation, selection and reconfiguration. Policy routing is at an embryonic stage. Also, in networks of multiple providers, there is no prescribed method of allocating impairments or other performance degradations.

IP can only support the Voice over IP approach among the VOP alternatives. IP does not carry ATM cells or frame relay traffic.

Analysis

IP is an essential part of next generation networks. If VOIP is selected as the basis for a voice offering, then IP transport has an essential, though not necessarily exclusive, role in near term VOP networks. The lack of mature IP techniques for supporting QOS will require special care in designing the IP-based VOP networks.

4.1.1.1.3. SONET/SDH Transport

Advantages

SONET/SDH networks can provide a high degree of reliability and survivability to network failures. SONET/SDH systems provide automatic protection mechanisms that can recover from failures, including cable cuts, in less than 60 ms.

SONET/SDH provides a rich set of network management and operations capabilities. These capabilities allow providers to operate the network cost effectively and to provide improved service and network management capabilities to customers. SONET/SDH provides a rich set of network management and performance information.

SONET/SDH is a proven technology deployed throughout the world. SONET/SDH is standards-based technology that facilitates interoperability between equipment from multiple manufacturers. SONET/SDH interfaces are becoming increasingly deployed on a range of data communications products including routers and ATM switches.

SONET/SDH is a scalable network. SONET/SDH supports transmission systems from 155 Mbps to 10 Gbps (based on current standards and products). SONET/SDH's flexibility allows it to transport a range of embedded services (e.g., T1/E1 and T3/E3), as well as new ATM and IP services.

Disadvantages

SONET/SDH can be more costly than some other transport methods (e.g., WDM). The additional cost associated with SONET/SDH comes from the additional layer of multiplexing. This layer of multiplexing is associated with the basic capabilities used by providers in today's high-speed networks. In the future, it may be more cost effective to deploy an ATM switch and IP router based network with high-speed interfaces than to deploy separate SONET/SDH multiplexers. These switches and routers could be connected directly to WDM elements.

SONET/SDH requires packet-networking elements (e.g., routers or ATM switches) to support VOP transport. SONET/SDH is an element in a solution, but is not a complete networking solution. Potential solutions include IP over PPP/SONET (SDH) and ATM over SONET (SDH).

Analysis

SONET/SDH is an element of the complex set of options regarding how to best build high-capacity, reliable networks using ATM, routing, SONET/SDH and WDM capabilities. Its combination of interoperability, reliability and manageability make it the default transport element for use with ATM and IP in provider networks.

4.1.1.1.4. Wavelength Division Multiplexing Transport

Advantages

WDM technology can dramatically increase the bandwidth capacity of fiber facilities. For example, a 16-channel WDM system can increase the bandwidth capacity of fiber facilities by 16 times. In the future 100 channel WDM systems will become available and higher capacity systems will likely follow.

WDM technology can reduce transport costs compared to single channel SONET/SDH systems. This is particularly true for long distance networks. In these networks WDM can realize significant cost savings in terms of reduced costs for laying fiber and in reduced costs for SONET/SDH regenerators. The rapid development of WDM equipment may provide opportunities for interconnecting backbone ATM switches and routers directly to the WDM equipment, bypassing separate SONET/SDH network elements. This can potentially save significant costs.

Disadvantages

WDM equipment is still relatively new and standards are immature or undeveloped for many of the capabilities. This results in vendor-proprietary implementations. Key examples include: standardization of specific wavelengths and physical parameters to be supported on particular WDM products (e.g., 16 channel STM-16 WDM), protection mechanisms, operations functions, operations communications protocols, information models and management systems.

WDM requires packet-networking elements (e.g., routers or ATM switches) to support VOP transport. WDM is an element in a solution, but is not a complete networking solution. Potential solutions include IP over WDM and ATM over WDM.

Analysis

WDM is an element of the complex set of options regarding how to best build high-capacity, reliable networks using ATM, routing, SONET/SDH and WDM capabilities. WDM is gaining ground now and will be a significant technology as various WDM capabilities are standardized.

4.1.1.1.5. Summary of Data Transport

Many combinations of technologies can be used to build transport networks to support VOP and most can be successful under the right set of circumstances. Some providers have strong views on networking technologies and are willing to take significant financial risks to innovate. The recommendation of this report is that transport technologies or architectures not be specified or standardized. Instead, the recommended course is to specify the required performance required of a VOP network and allow the provider to choose and manage a set of technologies that will meet the performance requirements.

4.1.1.2. Packet Technologies

This section discusses the relative merits of three packet technologies (ATM, IP and frame relay) to serve as the basis of voice transport. In particular, the choice of a packet technology means that encoded voice information will be placed in packets of that type and the associated packet procedures will used. A distinction is being made between the packet technology used and the underlying data transport. This section will discuss the merits of using IP (i.e., Voice over IP), but the data transport used to carry IP packets could be a routers, ATM or frame relay, or a combination of data transport for a given Voice over IP call.

4.1.1.2.1. ATM

Advantages

The direct use of ATM is the most efficient way to carry voice traffic by packet technology. Voice over ATM does not require encapsulation or mapping of packets into ATM cells; it places the voice samples directly into ATM cells. The overhead of an ATM cell (five octets) is small compared to other packet formats. In addition, if VOP is to be carried over an ATM network, Voice over ATM is undoubtedly the most efficient mechanism.

Voice over ATM can take direct advantage of the real-time capabilities of an ATM network. Reliable, proven mechanisms for the support of QOS are already built into ATM networks. No special mechanisms are required for provisioning, requesting or using the appropriate real-time capabilities.

ATM technology is being developed simultaneously as a public network technology and a LAN technology. There is generally a high degree of compatibility between the public ATM network and equipment that customers may be purchasing for their own private networking needs. This can lead to relatively seamless transport of ATM voice traffic from private to public networks.

ATM is data transport technology used in ADSL broadband access. ADSL will be one of the most important means of access to premium services. Voice over ATM would be an efficient way to use the built-in ATM transport.

Disadvantages

ATM voice traffic can only be transported over an ATM network. ATM traffic (of any type) can only be carried over ATM technology. This will limit the available transport options, though there are numerous vendors of ATM equipment. Since Voice over ATM is tied to the transport technology, it will inherit most of the advantages and disadvantages of ATM transport.

Voice over ATM is a less mature technology than IP or frame relay. Support for voice over AAL5 is now being standardized, with completion of the standard expected in 1999. However, SVC deployment by carriers is lagging and call control standards for voice telephony are incomplete. Unlike IP, there is no standard way for a user to set up a voice connection over ATM.

Analysis

Voice over ATM uses the services of the ATM transport layer directly. Because of this, the approach is efficient and there are no special concerns regarding the quality of the voice service. Support for voice service was designed in from the start, though the completion of that task is still work-in-progress.

4.1.1.2.2. Internet Protocol

Advantages

IP is ubiquitous. There is a large installed base of equipment capable of providing Voice over IP. Almost all computers are IP-aware and a significant portion of the PC consumer population is Internet-aware. This is in contrast to other forms of communications where

the cost and logistics of distributing and educating users on the new technology can be formidable.

Through Browser technology, IP has become user-friendly. The advent of the browser has brought the use of IP to the masses in a form that is largely transparent to them. With a set of cookbook instructions, a user can configure the dialer and browser for basic Internet access and services. Users like the interface and consider doing business on the Internet a form of entertainment. This has already been a benefit to IP telephony, since the technology was publicized and distributed over the Internet. Though any voice technology can benefit from the Web, IP telephony stands to gain more than most.

Voice over IP has significant industry momentum. Enormous resources from equipment vendors, service providers and academic sources are being focused on the Internet and IP telephony in particular. Products and services are being announced at a rapid pace. And working groups in the standards organizations are being spawned to address each open area of concern.

Voice over IP runs over IP. Though obvious, this means that it inherits the advantages of IP transport, including wide deployment and the ability to run over almost any transport technology, including ATM and SONET.

Disadvantages

Voice over IP inherits the disadvantages of IP. As described in the transport section, real-time performance support and management are not complete.

IP packet overhead is large. The IP packet headers are relatively efficient for most data traffic. However, for small packets, such as those carrying voice traffic, the overhead is relatively large. Overall bandwidth efficiencies come from the compression of the voice signal, not from the use of IP.

Analysis

IP has tremendous momentum in investment, deployment and experience. The enthusiasm for IP telephony is high among users and vendors alike. IP telephony can work well today in a lightly loaded network. In the future, IP telephony could work well in commercially loaded networks spanning the globe. But large networks will require successful efforts to develop real-time capabilities.

4.1.1.2.3. Frame Relay

Advantages

Frame relay technology leverages existing corporate networks. With frame relay, fewer physical interfaces and circuits are required, thus lowering both the cost of the enterprise network and the carrier network infrastructure, as well as lowering operations costs by requiring fewer physical elements to be maintained. Because of these cost advantages, frame relay is widely deployed in corporate WANs. Voice traffic can be easily added using voice-capable FRADs.

Technology to support frame relay service is widely available, including private networking equipment and public network platforms. This widespread availability leads to a competitive supplier market and relatively straightforward interworking of public and private network solutions.

Frame relay uses a very simple protocol. The frame relay protocol can be simple because of high quality transmission links in the public backbone, so that packets are rarely damaged in the network. The simplicity of frame relay leads to lower cost end-user equipment, low overhead and efficient transport of traffic, including voice traffic.

Disadvantages

Frame relay is not a general-purpose access protocol. Frame Relay is an enterprise networking protocol and there has been no move to use it as an access protocol for mass-market application. Unlike ATM, the industry has not embraced frame relay as a basis for the next generation of broadband access. Further, frame relay is generally used on point-to-point basis. The adoption of frame relay SVC, a necessary component of a general VOP offering, is lagging.

Real-time service support is lacking. Some vendors have proprietary support that mimics ATM traffic classes, but the support is not as robust as ATM for real-time traffic. Efforts are underway in the Frame Relay Forum to improve real-time support.

Analysis

Frame relay is unquestionably an attractive WAN service for data and will remain so. Frame relay provides a useful role in transporting voice in private frame relay network settings. However, the development of voice services on frame relay does not have the broad industry support that is necessary to create a robust technology basis for the next generation of networks. Frame relay voice services will likely expand when voice technology developed for ATM and IP can be leveraged. Voice over frame relay will not be considered further in this report.

4.1.1.2.4. Summary of Packet Technologies

Voice over IP has significant market momentum and interest that justifies further consideration in the VOP architecture and requirements efforts. Voice over ATM has promise from technical and market perspectives. If possible, the VOP architecture and requirements should support both approaches. Where simultaneous support is not possible, the first priority for the development of requirements should go to Voice over IP.

4.1.1.3. VOP Protocols

4.1.1.3.1. ITU-T Recommendation H.323

Advantages

H.323 is a stable standard that has been implemented in interoperable products. The first version of H.323 was approved in 1996. Version 2 of the standard has recently been released. H.323, and the associated protocols, are complete in that a full implementation of a voice network (or even a multimedia network) can be built using H.323.

H.323 is widely supported in existing Voice over IP products. After the first wave of proprietary products proved there was a market for Voice over IP, vendors migrated quickly to H.323, the only stable standard available. Today, nearly all voice over IP gateway and gatekeeper products support, or plan to support, H.323.

H.323 has rich set of communications capabilities. Because H.323 was designed for multimedia conferencing sessions, it has capabilities that potentially could be used to support new services.

Disadvantages

H.323 is a heavyweight protocol. H.323 was originally conceived as a protocol to support multimedia and conferencing sessions over LANs. In that context, the signaling had to be rich to support many media types and their varied needs for connections. Also, signaling over a LAN need not be lean since bandwidth and set-up times were not so serious as in wide area networks. A point-to-point, voice connection is a particularly degenerate case of a multimedia call. H.323 consequently has much protocol machinery that will never be used of voice services, as we know them today. The ITU has recently undertaken an activity to create a lighter version of H.323 for telephony.

The scalability is questionable. H.323 uses some techniques that limit its ability to grow to larger networks. For example, the H.323 gatekeeper maintains TCP sessions with the gateways. Also, services are largely implemented in the gateways, which could be difficult to upgrade for new services in a large network.

Analysis

H.323 has helped expand the market for Voice over IP by moving the technology away from proprietary implementations. It is doubtful whether H.323 can scale up to be the core technology of the voice networks of telephony providers.

4.1.1.3.2. IETF SIP/SAP/SDP

SIP is an application layer designed to support multimedia multicast (or point-to-point) connections in an IP environment.

Advantages

SIP performs well. SIP uses UDP so that the delays and overhead associated TCP sessions are eliminated. Also, SIP has a simpler structure and signaling protocol. A call setup using SIP may require only 25% of the time required when using H.323.

SIP provides unique capabilities. For example, one of its key applications is personal mobility. A person is identified by a name. Name mapping to locations and call redirection are integral parts of SIP. This allows end users to originate and receive calls and access subscribed telecommunications services on any terminal in any location.

Disadvantages

SIP is most appropriate for an IP environment. The development of SIP used the IP paradigm, which in some instances may be difficult to implement in a carrier environment. For example, SIP uses e-mail like addresses (e.g., hschulzrinne@cu.edu), though a gateway to the PSTN could use phonenum@gateway.

SIP is not a mature technology. SIP has not progressed through the IETF yet so there are no vendor products. Though most vendors of VOP products already offer H.323 products, SIP implementations are expected after a stable standard is in place.

Analysis
SIP is a streamlined protocol that could compete with H.323 for the next generation of IP-enabled voice applications and devices.

4.1.1.3.3. IETF MGCP

MGCP is a fusion of SGCP and IPDC, all of which are members of *distributed control protocols*. MGCP enables external control and management of data communications equipment operating at the edge of emerging multi-service packet networks. The edge devices are called "media gateways." The software programs that control the media gateways are known as "call agents" or "media gateway controllers." Examples of media gateway devices include voice over IP gateways, voice over ATM gateways, modem banks, cable modems and set-top boxes, soft PBXs, and circuit cross connects.

Advantages
MGCP can support both Voice over IP and Voice over ATM. MGCP is designed to control communications in a more technology independent way than are H.323 and SIP. MGCP is only concerned with the control, not the transport, of the calls. The transport functions are left to the media gateways that MGCP controls and those gateways could use IP or ATM.

MGCP uses a centralized service implementation. With MGCP, service functionality is centralized in a Call Agent, allowing for re-use of SS7 capabilities and the simpler introduction of new services.

MGCP should have good performance characteristics. One reason is that MGCP is UDP-based so TCP sessions do not have to be maintained and the delays associated with TCP are reduced. Also, MGCP uses simpler signaling. Analysis of call flows with and without supplementary services has shown that generally calls established using MGCP can be established more quickly than with H.323 because there are fewer transactions.

MGCP supports simpler gateways. With MGCP, the Call Agent implements complex signaling procedures, call models and AIN services while the gateways concentrate on a single task, the translation of audio signals into packets.

Disadvantages
MGCP is a new technology. MGCP has not progressed through the IETF, and has not been standardized. There are no implementations, although several companies have announced the development of MGCP products and the future deployment of networks based on MGCP control. In addition, several companies have working implementations of its predecessor, SGCP.

Analysis
MGCP is a good candidate for VOP signaling and control. It is designed specifically to support voice service in a way that is well suited to a voice provider environment. MGCP reflects the requirements emerging from the experience of the early carrier adopters of VOP technology.

4.1.1.3.4. VOP Signaling and Control Protocols Summary

MGCP is the best candidate for the signaling and control of VOP networks. It is efficient and is intended provide a standardized way to interwork with the signaling systems of the worldwide PSTN. H.323 and SIP can provide support for IP-enabled communications devices; both protocols will interwork with MGCP call agents.

4.2. Architecture for Voice Over Packets

The focus of discussion in this section is on the functional architecture of VOP networks. As such, the key functional elements in the VOP network are defined in the section. In addition, the relevant interfaces that have to be defined for these functional elements to interact with each other are also identified. However, the specification of the functional elements and the interfaces should not imply any specific physical implementation. Various suppliers should be able to develop functional elements within a single node and communicate with the relevant elements in other nodes. This architecture framework does not endorse any particular physical architecture.

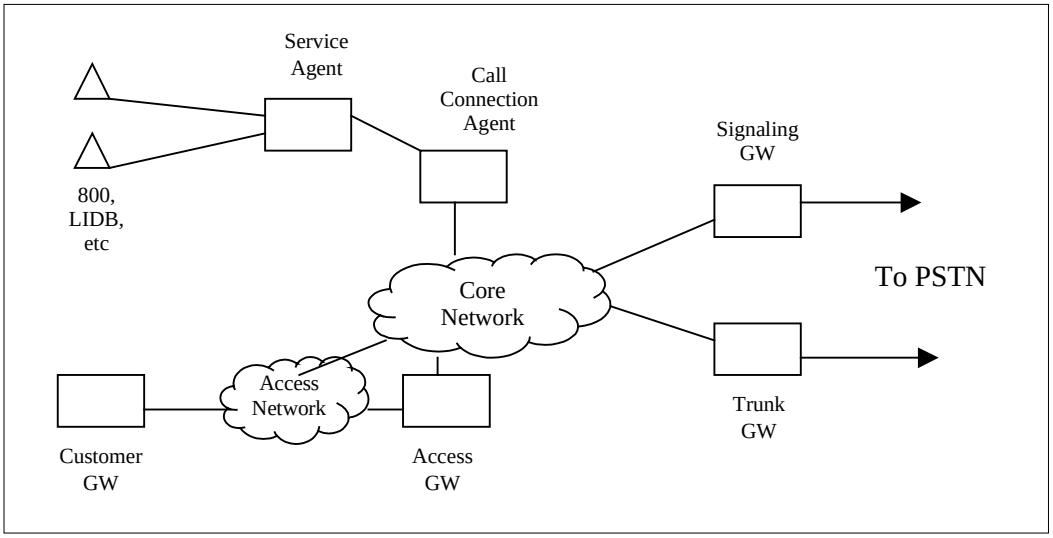

Figure 4-1 Key Elements in VOP Network

4.2.1. Key Functional Elements for VOP

Figure 4-1 shows the main functional elements in the VOP architecture. The key functional elements shown in the figure are described subsequently. In addition, the architecture relies on a Core Network and an Access Network for providing the necessary connectivity and transport. The Core Network is the packet transport network that provides connectivity to the functional elements in the VOP network. Discussions on the attributes of the Core Network are included in Section 5 along with the functional requirements of the key elements of the architecture. The Access Network represents the local loop network of the VOP. There are various ways of offering access to the VOP network. The Access Network could be based on the existing copper plant of Local Exchange Carriers or could use other technical options such as Hybrid Fiber-Coax

(HFC), Digital Subscriber Loop (xDSL), etc. Some of these newer options for accessing VOP network are discussed later in this section.

The key functional elements (FEs) in this architecture are as follows:

- *Access Gateway (AG)*

  An AG supports the line side interface to the VOP network. Traditional phones and PBXs currently used for the PSTN can access the VOP network through this FE. As such this FE provides functions such as packetization, echo control, etc. It is associated with a specific Call Connection Agent (CCA) that provides the necessary call control instructions. On receiving the appropriate commands from the CCA, the AG also provides functions such as audible ringing, power ringing, miscellaneous tones, etc. It is assumed that the AG has the functionality to set up a transport connection through the core network when instructed by the CCA.

- *Customer Gateway (CG)*

  A CG provides access to the network to some of the non-traditional CPEs that could have an associated IP address, such as IP-phones, personal computers, etc. Although a CG provides many of the functions associated with the AG, this FE is associated with a particular customer (business or residence). The CG is associated with a specific CCA that provides the necessary call control instructions. Calls originating in the CG would by-pass the AG and go directly into the core network.

- *Trunk Gateway (TG)*

  A TG supports a trunk side interface to the PSTN. The TG terminates circuit-switched trunks in the PSTN and virtual circuits in the packet network (the core network) and, as such, provides functions such as packetization. Even though a TG terminates trunks in the PSTN, this FE does not provide the resource management functions for trunks that it terminates. However, the TG has the capability to set up and manage transport connections through the core network when instructed by the CCA. It is associated with a specific CCA that provides it with the necessary call control instructions.

- *Signaling Gateway (SG)*

  An SG interconnect the VOP network to the PSTN signaling network. An SG terminates SS7 links from the PSTN CCS networks and thus provides the MTP Level 1 and Level 2 functionality. An SG communicates with the CCA to support the end to end signaling for calls with the PSTN. Each SG is associated with a specific CCA.

- *Call Connection Agent (CCA)*

  A CCA provides much of the necessary call processing functionality to support voice on the packet network. A CCA processes messages received from various other FEs to manage call states. A CCA communicates with other CCAs to setup and manage an end to end call. Although each gateway (AG, CG, SG and TG) is associated with a specific CCA, a CCA would typically interact with several gateways. A CCA instructs gateways with call control commands. A CCA interacts with the Billing Servers to generate usage measurements and billing data, such as Call Data Records (CDRs), for billing.

- *Service Agent (SA)*

  An SA supports supplementary services and generates TCAP messages to interact with Service Control Points for vertical services (Intelligent network services) such as 800 and LNP. It is initially envisioned that there would be a single SA for the entire VOP network that would interact with and through multiple CCAs.

The above list provides a very high-level view of the key functional elements involved in the typical call in the VOP network. One of the key issues going forward would be the allocation of specific functionality to different functional elements – much of which is defined in Section 5. However, a more comprehensive view of the VOP architecture is shown in Figure 4-2. In addition to the FEs described above and shown in Figure 4-1, Figure 4-2 shows the various user devices (e.g., IP-phones, traditional phones, etc.) that could be used to initiate a voice call on the VOP network, and some other FEs that are also important in the network. The additional FEs include the following:

- *Domain Name Server (DNS)*

  A DNS is used to translate IP names to routable addresses.

- *Routing and Translation Server (RTS)*

  An RTS is used by the Call Connection Agents during a call setup to determine the CCA and gateways (CG, TG, SG or AG) associated with a particular called number.

- *Billing Agent (BA)*

  A BA supports much of the billing functionality needed in the VOP network. It collects the necessary usage measurements from the CCAs and processes them for use by downstream billing systems.

- *Voice Feature Servers*

  Voice Feature Servers are special purpose servers that support various voice features and services. Examples include Announcement Servers, Interactive Voice Response Units, etc. In addition the Announcement Server would also be used as part of call processing to generate necessary tones and announcements.

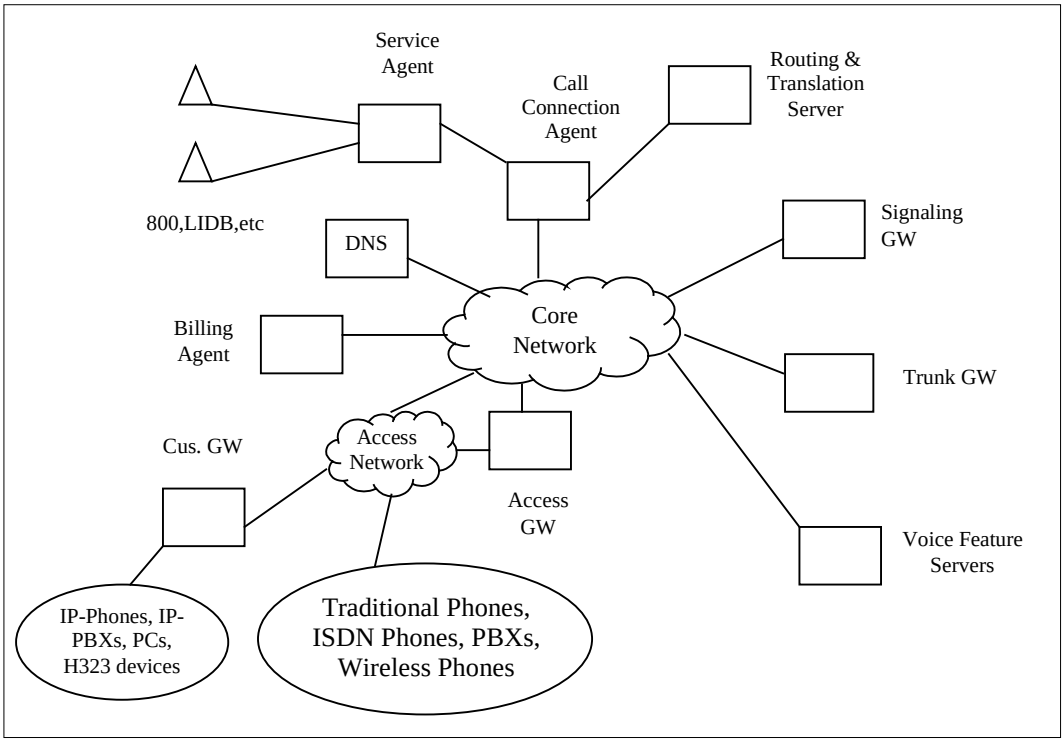

Figure 4-2 VOP Network with Additional Elements and CPE Examples

4.2.2. Interfaces and Protocols for VOP

Figure 4-3 presents key interfaces in VOP Architecture.

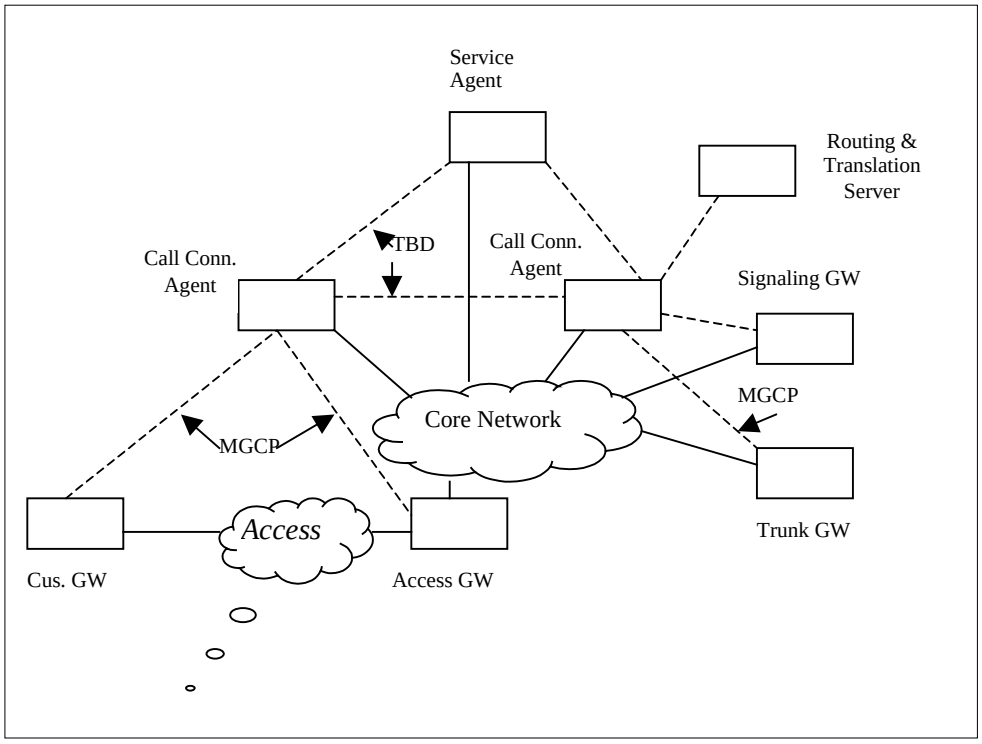

Figure 4-3 Key Interfaces in VOP Architecture

- *Interface between Customer Gateway and Call Connection Agent*

  MGCP could be used for this interface. Currently there are attempts to standardize MGCP. MGCP in its current form can be used for regular call setup. However, it remains to be investigated whether MGCP can be used to handle the numerous error conditions that are associated with existing call setups. It may be necessary to incorporate additional features in MGCP to use it to synchronize successive messages and to provide timestamps to messages when needed.

- *Interface between Access Gateway and Call Connection Agent*

  MGCP could also be used for this interface. However, it remains to be seen whether MGCP in its current form can support the necessary signaling functions associated with ISDN services. There is a possibility that either MGCP would have to be enhanced or some other signaling mechanism would have to be considered for communications over this interface.

- *Interface between Trunk Gateway and Call Connection Agent*

  MGCP could also be used for this interface. However it may be necessary to incorporate additional sequencing, timestamping features in MGCP to enable the CCA to remotely manage the trunk resources in a TG.

- *Interface between Signaling Gateway and Call Connection Agent*

  This interface could be based on a relatively small set of primitives (as yet to be defined) that could be used to send information received at the SG to the CCA and vice-versa.

- *Interface between two Call Connection Agents involved in a call*

  This interface will have to be defined, potentially based on an enhancement of ISUP or BISUP. Although either ISUP or BISUP would seem to be a natural protocol for use on this interface, there may need to be some enhancements needed to support the additional states associated with the separation of the gateway needs from the Call Connection Agents.

- *Interface between Call Connection Agent and Service Agent*

  This interface will have to be defined, potentially based on TCAP.

- *Interface between Call Connection Agent and Routing/Translation Server*

  This interface will have to be defined.

- *Interface between Call Connection Agent and Billing Agent*

  This interface will have to be defined.

4.2.3. Interconnection to PSTN

Figure 4-4 presents an example interconnection of the VOP network to the PSTN. Such an interconnection would be used to interconnect the VOP network to the network of an incumbent LEC or to IXCs. The key network elements involved in the interconnection are the Signaling Gateway (SG) and the Trunk Gateway (TG). The SG provides the interconnection to the PSTN signaling network and thus interconnects to STPs in the PSTN. Such an interconnection could be using A-links or using B/D links if pairs of SGs are interconnected to an STP pair for added reliability. However, the likelihood is that the VOP network will interconnect to the PSTN signaling network using A-links, due to the simplicity of this option. The interconnection to the PSTN signaling network also provides access to the PSTN SCPs (for services such as 800), since it is anticipated that initially the VOP network may not have its own SCPs.

The TG provides the trunk-side interface by interconnecting with the PSTN tandem.

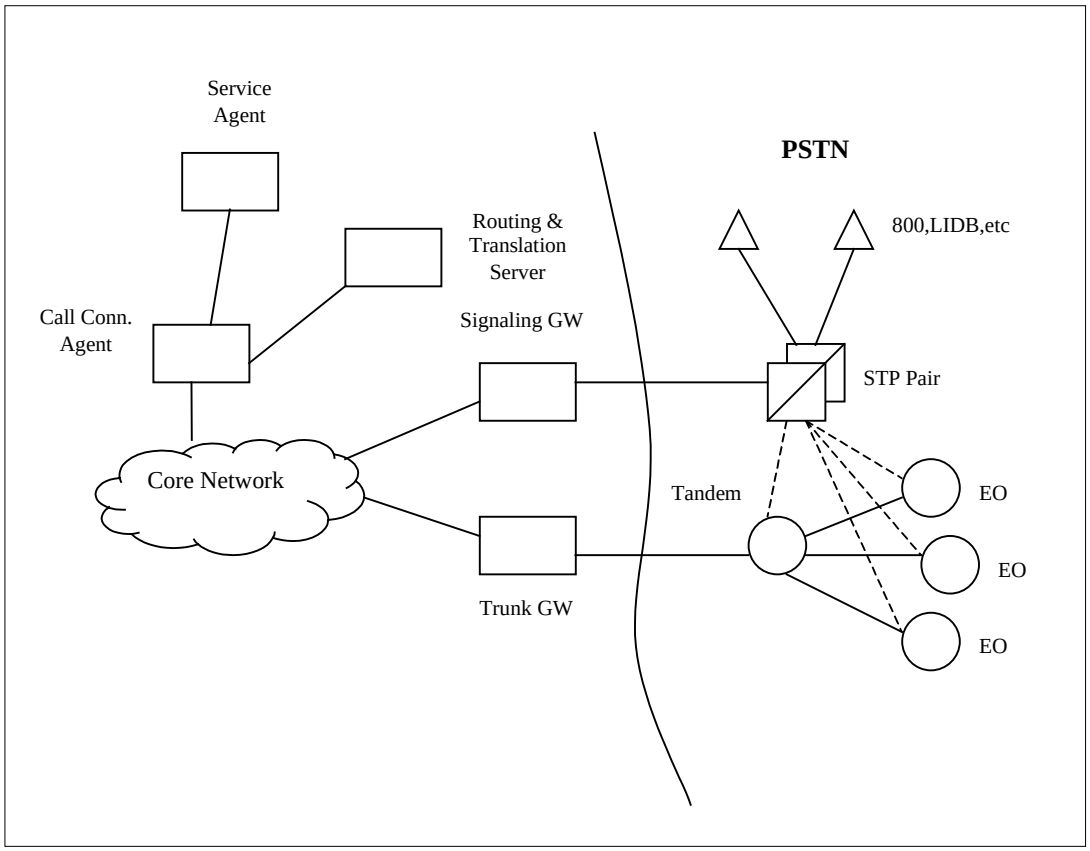

Figure 4-4 Interconnection to PSTN

4.2.4. Key Access Options for VOP Network

4.2.4.1. Digital Subscriber Loop Technologies (xDSL)

Figure 4-5 presents VOP Architecture with xDSL.

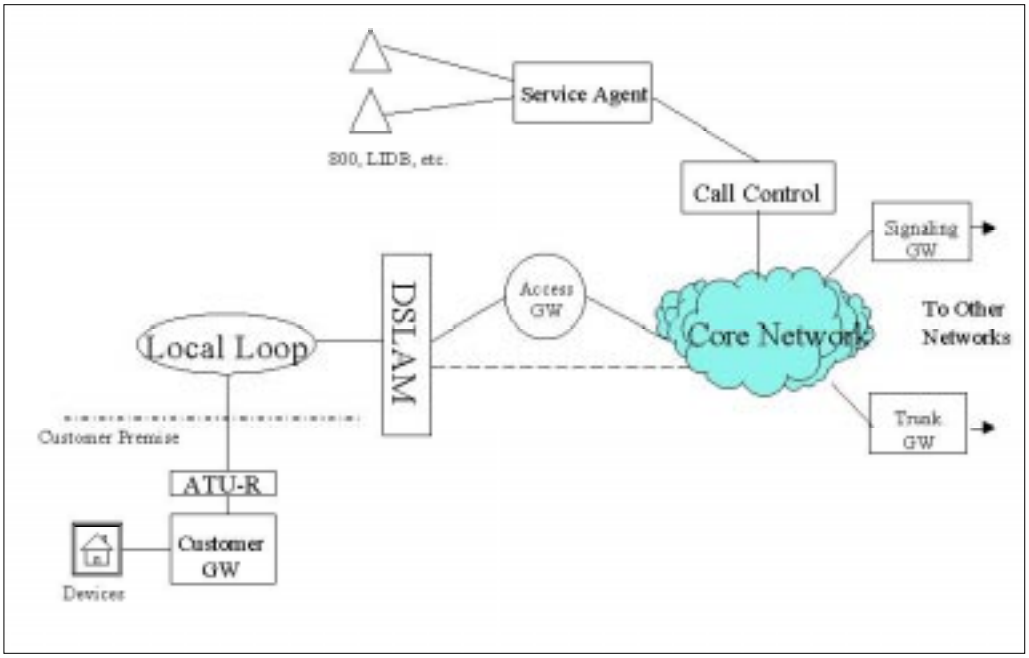

Figure 4-5 VOP Architecture with xDSL

4.2.4.1.1. Description

xDSL can provide high speed data transport over copper twisted pair. xDSL comes in a variety of flavors with different upstream and downstream bandwidths. There is a trade off between the bit rate that can be transported and the range of the system. Some examples are presented in Table 4-1.

Table 4-1 Differences Between Bit Rate and System Range

Technology	Downstream	Upstream	Range
ADSL	1 to 8 Mbps	128 to 640 Kbps	< 5.5 Kms
VDSL	13 to 52 Mbps	1 to 4 Mbps	1/3 to 1.3 Kms
SDSL*	784 Kbps	784 Kbps	4 Kms
HDSL *(2 pair)	1.544/2.048 Mbps	1.544/2.048 Mbps	4 Kms
RADSL	128 Kbps to 8 Mbps	128 to 640 Kbps	< 5.5 Kms

**Note HDSL and SDSL do not support POTS on the same loop.*

A DSLAM (Digital Subscriber Line Access Multiplexer) in the central office (or at RT site in the field) connects to the PSTN and a data network. The DSLAM multiplexes the

xDSL data in the upper frequency of copper twisted pair. At the customer's premises, a splitter/filter separates the two signals (except for G.Lite ADSL which does not require a splitter), passing the POTS to the existing inside telephone wiring and the ADSL signal to the ATU-R. The ATU-R terminates the ADSL signal and hands the data off to the PC.

Advantages

Every telephony subscriber is served by a dedicated copper twisted pair from the central office (or RT (Remote Terminal) for DLC (Digital Loop Carrier)). This copper pair is not shared with other possible customers. Many of xDSL's strengths are derived from this point-to-point, physical star architecture.

The point-to-point connection provides innate security since data to/from a given subscriber is not broadcast to other users of the access network.

ADSL typically can provide in the range of 1 Mbps to 6 Mbps to each user. This bandwidth is dedicated to the subscriber in the access network. Also, since the data is isolated from other traffic in the access network the performance over this link is constant.

Different end-to-end QOS (Quality of Service) can be offered in the core network. Since the performance on the access network is constant, the access network will not disturb the QOS.

xDSL uses the embedded copper plant to provide data transport. However, it does not interfere with the operation of POTS over the same loop. xDSL uses the spectrum above the 0-4kHz range used by POTS.

Disadvantages

ADSL provides a constant bit rate data path. (e.g., 1.5 Mbps). However, this is also the maximum line rate and users cannot transmit bursts of data at bit rates higher than this.

Although ADSL uses the embedded copper plant to offer data services, not all existing loops can support ADSL. ADSL is limited to loops that are under a certain length. The maximum length is determined by the bandwidth that is trying to be supported.

Also, other factors affect the performance of ADSL such as bridged taps or load coils on the loop and noise ingress from external sources. The concatenation of these issues can limit the number of customers that can be served with ADSL.

ADSL can also be affected by crosstalk from other data services. ADSL is especially vulnerable to crosstalk from T1/E1 lines and it may not be possible to offer both in the same binder group. In the same way, other data services are affected by crosstalk from ADSL. It is imperative not to degrade current data services with the offering of ADSL.

Since ADSL cannot be ubiquitously offered due to the issues stated above, loop qualification becomes a significant issue. Every time a subscriber requests service, the service provider must determine if the customer's loop can support ADSL. However, the loop data record is typically not accurate enough to make this determination with 100% accuracy.

4.2.4.2. Hybrid Fiber Coax

Figure 4-6 presents VOP Architecture with HFC.

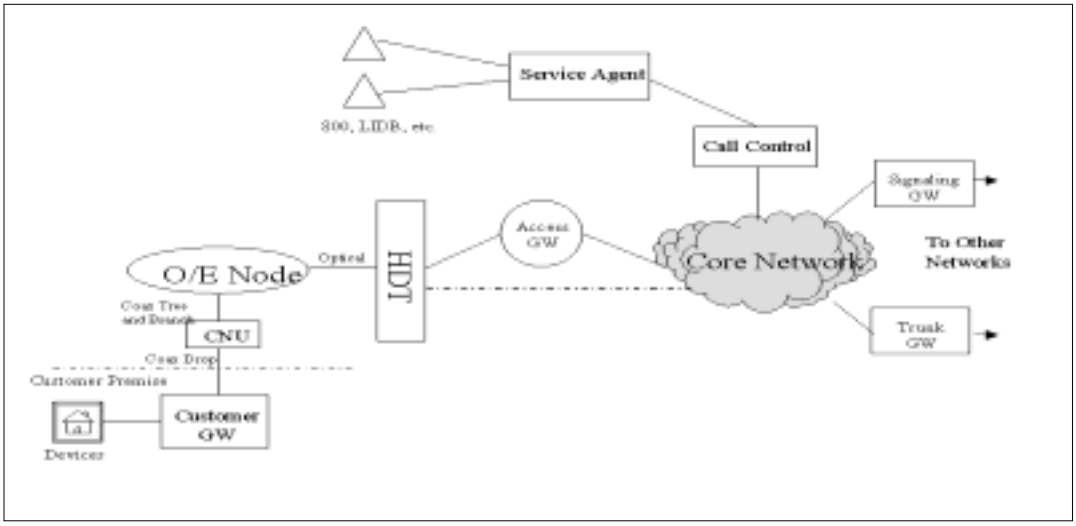

Figure 4-6 VOP Architecture with HFC

Description

The following describes one realization of an HFC system. Several variations are possible based on services carried, technology used, and deployment choices.

An HFC system will typically consist of an HDT (Host Digital Terminal) (located in the exchange), an O/E (Optical to Electrical) Node located within the neighborhood served (about 125 to 500 living units), and several CNUs (Coaxial Network Units) each serving several living units. The HDT and O/E Node are connected with fiber cable while coax cables connect the O/E node and CNUs. The CNUs and the living units are connected over coax and copper drops.

HFC systems use analog transmission, therefore, digital services are sub-carrier multiplexed into 6 to 8 MHz channels (depending on different countries) at the HDT and then combined with analog video channels. The telecommunications and video passband signals are used to modulate separate downstream lasers. At the O/E Node, the optical signals are received, converted to RF (Radio Frequency), amplified and placed on coax buses for transport to curb units, known as Coaxial Network Units (CNUs).

At a CNU, RF signals are received, telecommunications traffic is demultiplexed, video interdiction is provided and video signals are amplified and placed on coax drops while telecommunications traffic is placed on copper drops. Also, CNU provides digital to analog conversion and BORSCHT functionality.

Upstream, these processes are reversed with CNUs performing A/D conversion and multiplexing to place upstream signals on the coax bus. At the O/E node, the RF signals from multiple coax buses are combined and used to modulate an upstream laser for transport back to the HDT. At the HDT, the optical signals are received, demodulated, and routed to the appropriate interfaces to the backbone/switching networks.

The above is only one example implementation of a HFC system. There are several other alternatives depending upon services and vendor choice.

Advantages

Most current systems are based on 300 – 450 MHz technology and are being upgraded to 750 MHz technology with 700 MHz typically allocated to downstream transmission. Many deployments are planned for future upgrades to 1 GHz technology. The fact that the majority of the available bandwidth is allocated for downstream transport makes HFC ideal for the provision of broadcast services. Thus, HFC provides an excellent network for video and data services since these services are highly asymmetric in nature.

All of the components of the HFC network are shared with only the drops being dedicated to a single customer. This sharing, plus the broadcast nature of the architecture makes the HFC approach ideal for the initial introduction of new services that may only have a small percentage of the customers passed subscribe to the service. Only the HDT and the subscribing customer's CNUs need to be equipped to provide these services.

The capability to carry analog video in a format that can directly interface to current television and VCR equipment prevents the need for multiple digital to analog conversions in the network, thereby lowering overall network costs.

As mentioned above, the HFC deployment brings fiber relatively close to the homes served by each O/E Node, typically about 125 to 500 homes passed each. This approach has been adopted by CATV companies to both improve signal quality and the reliability provided to their video customers. This has resulted in drastic reductions in the number of amplifiers in cascade required to provide adequate signal strength to end customers.

The coaxial cable provides for the transport of electrical powering from the O/E Node or other power insertion points out to each CNU and any other active devices required.

Disadvantages

The limited bandwidth available for upstream transmission and its location in a typically noisy portion of the RF spectrum means that robust modulation techniques must be used and that allowances for frequency hopping to vacate portions of the spectrum when noise levels increase must be provided.

The limited upstream bandwidth also leads to potentially expensive network upgrades when large number of symmetric services (e.g., telephony) are carried by these networks.

The relative lack of standards for the material, equipment, tools, and installation methods and procedures throughout the cable industry has resulted in wide variations in network quality and performance. More recently, some efforts towards standardization have resulted in improvements, however, each vendor's overall systems are proprietary in nature as system level standards do not exist.

The coaxial portion of the HFC network is highly susceptible to noise. Steps must be taken to "harden" the plant to both ingress and egress noise. The environment inside the customer's home is known to cause spurious signal impairments that are very difficult to troubleshoot and fix.

The broadcast nature of the coax facility means that without specific steps for prevention, everybody's signals are broadcast to everyone else. The CNU provides signal isolation for telephony services, but, without other steps the video and data signals will be transmitted over all connected drops. This is a security concern as well as a theft of service (unauthorized use of service) issue. The broadcast characteristics of the coaxial cable and its susceptibility to impairments contribute to reliability concerns meaning that a careful assessment of network reliability is required.

Due to the shared bus utilized in HFC, the data path is affected by the number of customers served. Also, HFC is not optimal for symmetric services (i.e., POTS, ISDN) especially if all customers desire such services.

4.2.4.3. Fiber to the Curb

Figure 4-7 presents the VOP Architecture with FTTC.

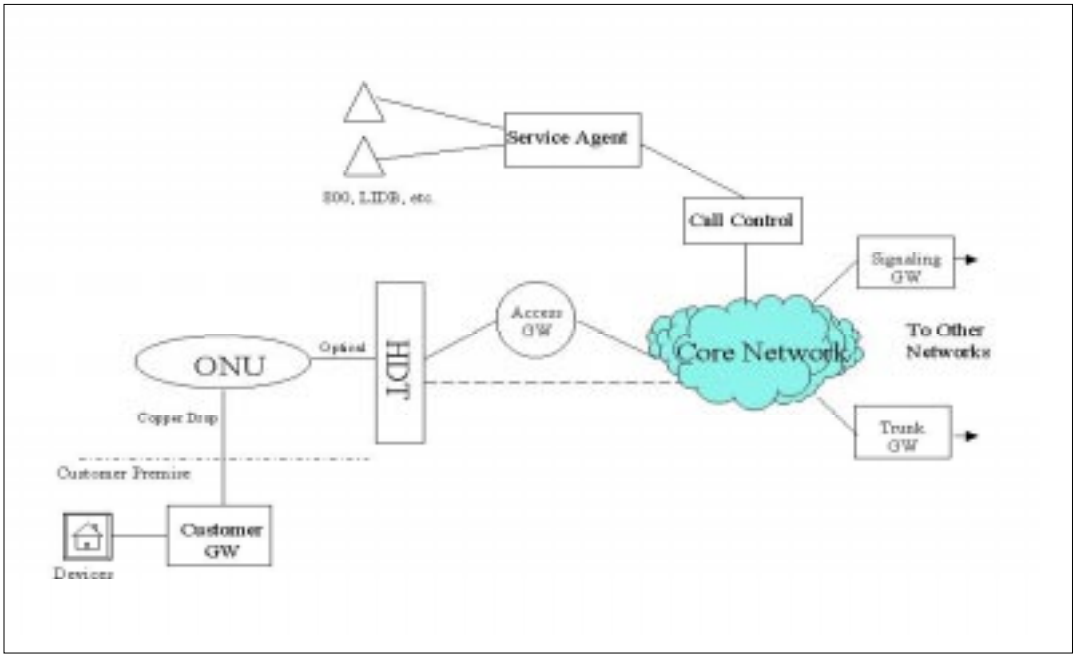

Figure 4-7 VOP Architecture with FTTC

Description

As with HFC systems, many FTTC variations are currently possible including Active Optical Networks (AONs), Passive Optical Networks (PONs), exchange-based and RT-based Host Digital Terminals (HDTs), point-to-point and point-to-multipoint arrangements, etc. However, all of these fundamentally consist of a host network element, most often called an HDT, and sub-tending Optical Network Units (ONUs) which are connected by digital fiber links.

Analog video signals are typically digitized and combined with digital telecommunications, digital data, and digital video signals at the HDT and sent for transport over downstream fibers to ONUs. At the ONUs, the optical signals are

converted to electrical signals, processed and accessed by line cards that develop the various service interfaces. From the ONUs these services are then sent over to each living unit served over copper drops.

Upstream signals are multiplexed and optically transmitted back to the HDT where they are demultiplexed and sent to the appropriate backbone / switching interfaces.

Some of the other facets of the FTTC architecture subject to differences from either vendor design or implementation choice include the following:

- The number of fibers used by each ONU
- The method employed to power ONUs
- The use of coax drops for video signals
- The method used to combine various signals for transport between the HDT and ONUs.

Advantages

The bandwidth capabilities of these systems are only limited by the electronics located at the HDT and ONUs and we observe that technology is constantly increasing this capability. This implies that the fiber plant is truly "permanent" in the sense that future upgrades to increase bandwidth can be accomplished at the HDT and ONUs without disturbing the plant in between.

By placing intelligent Network Elements (NEs) near to the customer, remote provisioning, maintenance, and testing are enabled.

The mature standards associated with optical transport (SONET / SDH) are being migrated into FTTC systems. By eliminating much of the metallic connection between the exchange and the end customer, these systems effectively reduce exposure to electrical interference and noise. Additionally, the use of digital signal processing techniques means that the services carried are not subject to the analog signal degradations found in the current analog network.

Due to the fact that the drop facilities from the ONU site to each customer are dedicated facilities, there is no security concern.

Disadvantages

Because this architecture brings fiber and ONUs relatively close (within a few hundred meters) of the end customer, much of the current copper network is bypassed. This results in little leverage from this embedded network and, therefore, higher initial construction costs for FTTC. Additionally, as this approach distributes some of the functionality performed at the switch in a copper architecture out to the ONUs the number of customers sharing this functionality at each ONU is much less than at the switch. As the volume of deployment is still small, these ONUs are still relatively expensive.

The analog video signal, carried in an optimal manner by an HFC network must be digitized for transport in a FTTC approach. As an example, this means that digital to analog conversions must be completed at the customer's location to provide analog video signals to analog televisions.

As the ONUs distributed widely throughout the secondary network require power to operate, some scheme must be used to provided distributed powering. The fiber cables cannot carry enough power for this, therefore, power must be either carried to the ONUs by a metallic network (either copper or coax) or accessed locally at each ONU site. The distributed nature of this network impacts the provision of back-up power capabilities also. Note that some deployments use coax cables to carry power to the ONUs and also to carry analog video without requiring the A to D (Analog to Digital) and D to A conversions mentioned above.

Although fiber networks are typically considered very reliable, the distributed electronics of the FTTC approach must also be very reliable to afford overall network reliability. The intelligence of these network elements and the capability for remote alarms and diagnostics should help alleviate these concerns.

4.2.4.4. Fiber to the Home

Figure 4-8 presents the VOP Architecture with FTTH.

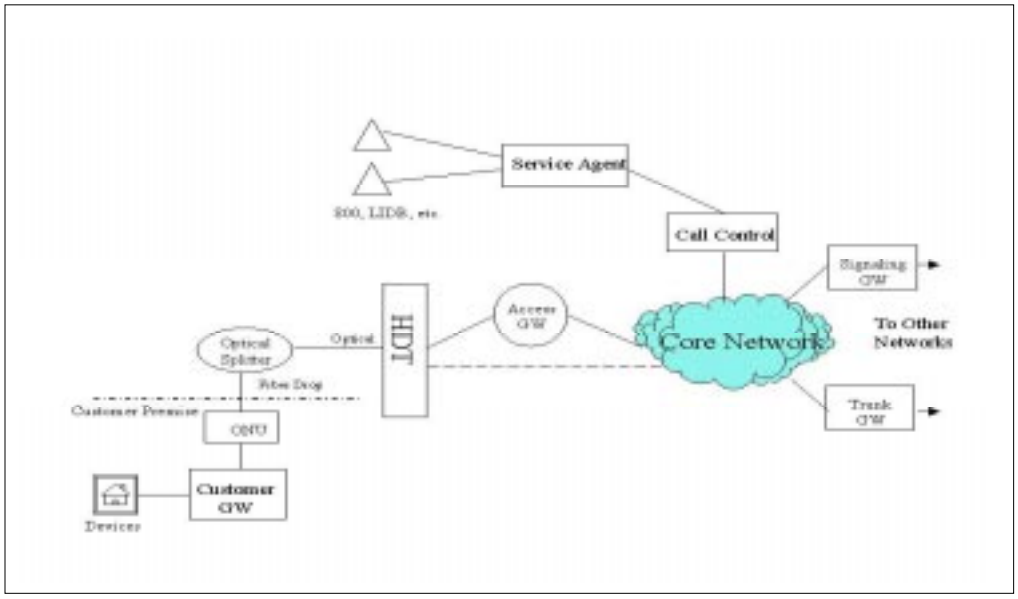

Figure 4-8 VOP Architecture with FTTH

Description

As many aspects of FTTH are so similar to the previous discussion of FTTC we will concentrate discussion here on only those areas where there are differences.

The primary difference between FTTC and FTTH is that the ONUs in the FTTC approach are shared by multiple customers. With FTTH, each ONU is dedicated to only one customer, thus the H in FTTH, e.g., each home has a separate ONU and each ONU provides services to only one customer or home.

One other difference is that an additional powering option is available. With FTTH it is possible to power the ONU from the customer's site.

Security concerns are handled by the digital signal processing that occurs at each ONU. Only those services intended for the single customer served are presented for connection to the inside wiring (copper or coax) by the service defining plug-ins facing the customer.

Advantages

As the ONUs are located at the customer's premise it is possible to implement a totally passive outside plant network when the HDT is placed in the exchange. This means there are no active network elements between the exchange and the customers, implying reduced service activation and service assurance expenses.

The potential to power each ONU from the customer's site leads to power cost reductions. Additionally, the issue of having the customer responsible for the back-up battery should be investigated.

Additionally, FTTH provides higher bandwidth to end users and immunity to lightning.

Disadvantages

Compared to the FTTC options, FTTH requires additional fibers as there are more ONUs required to serve the same number of customers. Also, as each ONU is dedicated, there is no sharing of common functions. These factors contribute to the higher cost of these systems for urban and suburban areas.

4.2.4.5. Local Multipoint Distribution Service

Figure 4-9 presents the VOP Architecture with LMDS.

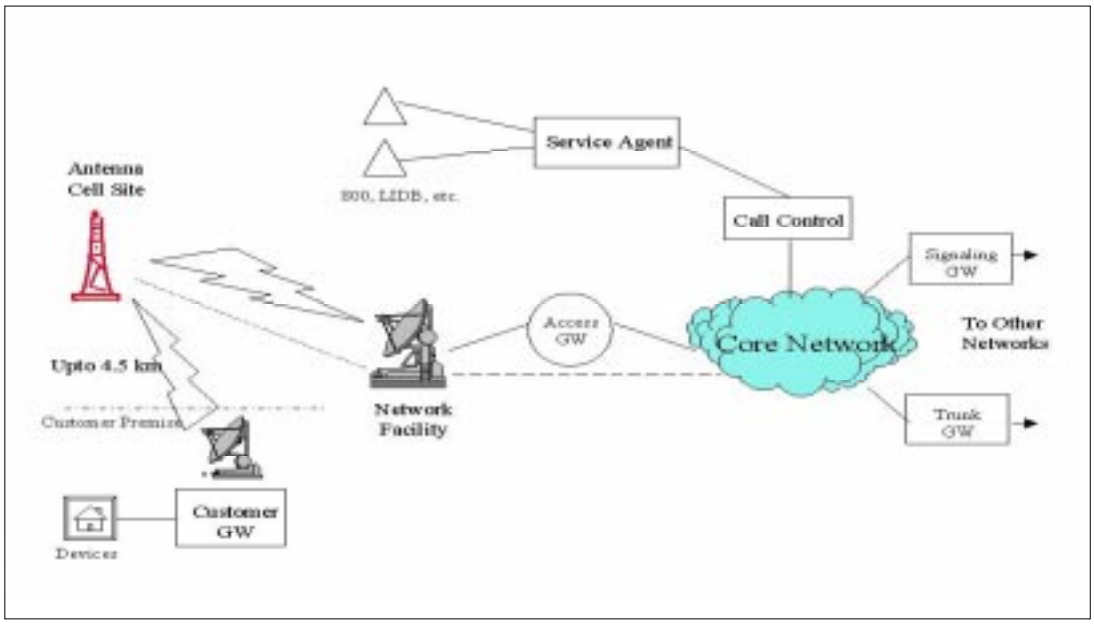

Figure 4-9 VOP Architecture with LMDS

Description

Figure 4-9 shows a high level view of a Local Multipoint Distribution Service (LMDS) system. A similar European technology is MVDS (Multichannel Video Distribution Service) that operates at 40 GHz. LMDS is a fixed wireless system that employs transmitters in 4.5 km (3 mile) radius cells to cover their serving area. In general, there is a single headend facility that gathers the video, telephony, and data signals for distribution to the LMDS cell antennas which broadcast the signal to subscribers. A subscriber will need a small antenna to pick up the signal. A customer unit will be required to convert video signals to a format acceptable for the television. The subscriber antenna must be within line of site of the transmitting antenna in order to receive the signal. Any foliage or buildings between the transmitting and receiving antennas will block the signal. MVDS is similar with slightly less reach than LMDS.

LMDS/MVDS can be used to provide residential telephony, video, and data services. It can also be used to provide high-speed data links to businesses including T-1/E-1 and T3/E3. MVDS was initially aimed at the broadcast video market, but can provide a full service type network, though 100% coverage, such as a wireline system can provide, is not possible, or at least economically unfeasible.

LMDS is set in the 28 GHz range in the U.S. MVDS is usually at 40.5 to 42.5 GHz in Europe, with consideration of using 42.5 to 43.5 GHz for the return path. There are some 28 GHz European trials.

Advantages

In the USA, LMDS is allocated 1300 MHz of bandwidth. This is over 6 times the amount allocated to other lower frequency fixed wireless systems and gives LMDS the ability to handle high volume, two-way traffic. In addition, the relatively small coverage area for each hub, along with the option of frequency polarization and directional antennas, allows for reuse of spectrum from cell to cell. This provides abundant frequency to support virtually any service.

The small cell size associated with LMDS also allows it to support local and niche programming that is targeted to specific demographic areas.

Disadvantages

LMDS operates in the 28 GHz region of the spectrum. Because of this, the receiving antenna must be within line of site to the broadcasting antenna. Furthermore, LMDS is limited be rain attenuation and can be affected by foliage. These factors limit the availability of service from LMDS and cause small cell sizes to be used in order to maintain high service availability. Additionally, ubiquitous coverage is not possible within a cell due to these issues. MVDS, at 40.5 to 42.5 GHz has the same, but a slightly more severe problem.

The small cell size means that multiple cell sites will be needed within a city. The cell sites will then need to be inter-connected via a fiber or microwave network, adding additional cost to the service. These multiple cell sites may also interfere with each other again reducing coverage.

As with all wireless networks, signals are broadcast throughout the coverage area. Because of this, security is a concern, as unauthorized users may attempt to steal the signal or impersonate legitimate users. The security concern for LMDS is limited because LMDS utilizes a narrow beam and fraudulent users are easy to detect due to the two-way traffic.

4.3. Sample Call Flows

This section describes overviews of sample, high-level, end-to-end message flows. These flows include examples of successful basic call setup and release as well as a potential difficulty involving resource management. The description of the flows in this section provide a clearer view of how the FEs, discussed in Section 4.2.1, interact to support voice call completion. Details of these call flows are provided in Appendix C. In addition this section lists some of the assumptions being considered for end-to-end calls in this architecture. Note that these assumptions are preliminary and may be revised as additional details of the network are specified.

The details of these call flows provide an indication of the complexity involved in even a simple call. The process becomes even more complex as key telephony services (such as a call involving a query to a SCP) are incorporated into the call flow. However, for the VOP network to have parity with the PSTN in terms of voice and voiceband services, such complexity along with the associated possibility of interactions between various features and services would have to be considered. As GRs are developed for the various FEs (initial functional requirements are provided in Section 5), they will have to consider such call flows to ensure that they can handle the typical scenarios associated with voice calls.

4.3.1.1. Assumptions

The call flows in this section depend on the following assumptions:

1. A CCA contains all information (e.g., trunk status tables) that a normal PSTN switch needs for call processing.
2. Each network node contains procedures that ensure the delivery of error-free messages between network nodes. Furthermore, these procedures maintain message sequencing.
3. Each trunk between a PSTN switch and a TG is uniquely identified by the switch's Point Code (PC) and a CIC. The trunk is also uniquely identified by the TG's address and a channel_number.
4. All calls have identical QOS and bandwidth requirements.
5. The voice to packet converters (VPCs) in a TG are interchangeable in the sense that any one may be used during call setup. In other words, neither the caller nor the CCA prefers one VPC to another.
6. The virtual circuits out of a TG are interchangeable in the sense that any one may be used during call setup. In other words, neither the caller nor the CCA prefers one virtual circuit to another.
7. Given a Called Party Number and the address of a TG, an RTS is able to determine the address of the next CCA that should handle a call.
8. The virtual circuits in the packet network are switched.
9. Each CCA manages the trunks terminating at its subordinate TGs.
10. Each TG manages its internal VPCs and the virtual circuits that it terminates.
11. Each trunk between a PSTN switch and a TG is associated with a single SG, but each SG may serve multiple PSTN switches.
12. One and only one CCA serves each TG, but each CCA may serve multiple TGs.
13. One and only one CCA serves each SG, but each CCA may serve multiple SGs.
14. A TG marks a trunk "busy" only after a CCA instructs it to do so. In other words, a TG never initiates the seizure of a trunk.

4.3.1.2. Successful Call Setup

The message flow in this section describes a successful call setup across the network shown in Figure 4-10. Such a call setup could occur when an IXC with VOP capabilities provides connectivity between SSP1 and SSP2. In other words, when the IXC's network contains all network nodes in the figure except SSP1 and SSP2.

Note that the message flow in this section is only an example and is based on the prior assumptions. Actual message flows may vary depending on the network protocols used and the types of interconnectivity offered (e.g., PVCs versus SVCs in the packet network).

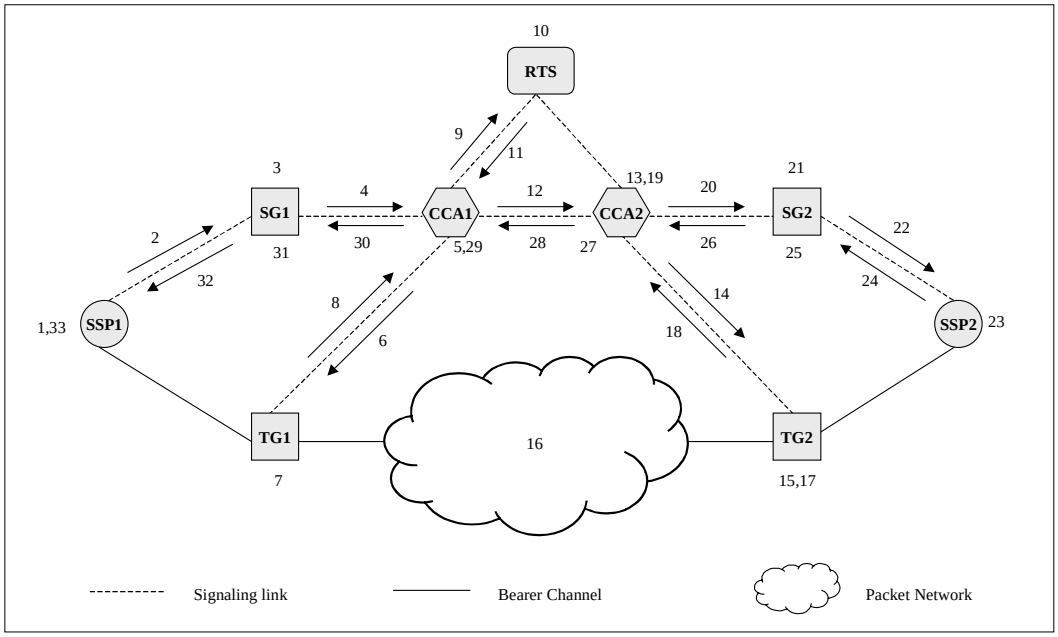

Figure 4-10 A Message Flow for a Successful Call Setup

Overview

The message flow in Figure 4-10 can be broken down into nine major components:

1. SSP1 sends a "connect request" to CCA1 (see Steps 1 through 4).
2. CCA1 instructs TG1 to switch the incoming trunk through to an outgoing virtual circuit (see Steps 5 through 8).
3. CCA1 queries the RTS to determine the address of a CCA serving the terminating PSTN switch (i.e., SSP2) (see Steps 9 through 11).
4. CCA1 sends a "connect request" to CCA2 (see Step 12).
5. CCA2 instructs TG2 to switch a virtual circuit through to a trunk going to SSP2, and TG2 establishes a virtual circuit to TG1 (see Steps 13 through 18).
6. CCA2 sends a "connect request" to SSP2, and SSP2 completes the call setup (e.g., provides power ringing to the called party and audible ringing to the calling party) (see Steps 19 through 23).
7. After SSP2 provides power ringing, it returns a "connect acknowledgement." This acknowledgement passes through SG2, CCA2, CCA1, and SG1 before arriving at SSP1 (see Steps 24 through 33).
8. When the Called Party answers, SSP2 removes audible and power ringing, switches the trunk through to the access line, and returns an "answer message." This "answer message" propagates back to SSP1 in the same way that the "connect acknowledgement" did.
9. SSP1 switches through the call in both directions, and the call setup is complete.

The above discussion describes the message flow in Figure 4-10 at a high level. Details of the actions at each step are listed in Appendix C. In addition to the steps taken in a

successful call setup, requirements for the FEs will have to take into account numerous failure scenarios. For example, procedures will have to be defined to allow the VOP network to gracefully handle scenarios in which the call setup is not completed due to the failure to complete one or more of the above steps.

4.3.1.3. Successful Call Release Initiated by the Calling Party

The message flow in this section describes a successful call release across the network shown in Figure 4-11. Note again that the message flow in this section is only an example.

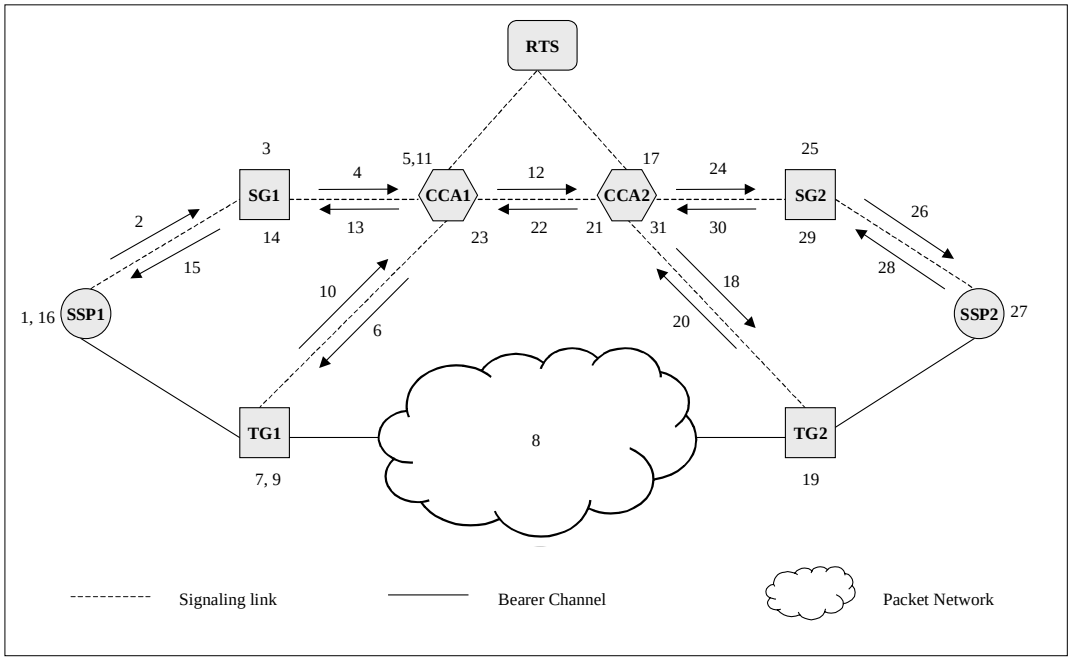

Figure 4-11 A Message Flow for a Successful Call Release Initiated by the Calling Party

Overview

The message flow in Figure 4-11 can be broken down into the following six major components:

1. SSP1 sends a "disconnect request" to the CCA1. (Steps 1 through 4)
2. CCA1 instructs TG1 to release the incoming trunk, the VPC, and the outgoing virtual circuit. (Steps 5 through 10)
3. CCA1 sends a "disconnect request" to CCA2 and a "disconnect acknowledgement" to the originating PSTN switch. (Steps 11 through 16)
4. CCA2 instructs TG2 to release the incoming virtual circuit, the VPC, and the outgoing trunk. (Steps 17 through 20)
5. CCA2 sends a "disconnect request" to SSP2 and a "disconnect acknowledgement" to CCA1. (Steps 21 through 26)

6. SSP2 releases the trunk and access line and returns a "disconnect acknowledgement" to CCA2. (Steps 27 through 31).

The details of each step in the above message flow are described in Appendix C.

4.3.1.4. Difficulty in Managing Remote Resources

This section highlights a potential difficulty that a CCA may experience when managing TG resources. This difficulty exists even when all of the assumptions in Section 4.3.1.1 are met. The purpose of this discussion is to provide an example of the sort of issues that would have to be considered when describing the functions of the CCA and the interactions it would have with the gateways.

Specifically, assumption 9 states that each CCA will contain a status map that tracks the busy/idle state of each trunk terminating at its subordinate TGs. Call processing in each CCA will use this status map to signal and route calls appropriately.

The separation of the busy/idle state of a trunk in a CCA from its actual state in a TG may cause a difficulty. Should the two states go out of sync, call processing in the CCA could make incorrect decisions and cause a reduction in call throughput at the TG.

To keep these states in sync, the protocol between a CCA and a TG should be designed to minimize such synchronization errors. Including an "audit" message, which could be sent by a CCA to collect and return the status of a TG's resources, is one possible solution[1]. When the CCA receives an "audit response," it would update its status map according to the contents of the message.

Such auditing of a TG's resources, however, can corrupt an otherwise accurate status map in a CCA unless sufficient safeguards are devised. In particular, corruption can occur when a TG processes messages in the order that is different than their creation order in a CCA. This reordering may be caused by the TG's architecture (e.g., distributed) or by the network between a CCA and a TG altering the sequencing of messages.

To prevent such corruption, the network link between a CCA and a TG should ensure that messages are delivered in the order that they are sent. One drawback of MGCP is that messages are transmitted over UDP, which does not ensure message sequencing.

Additionally, the CCAs and/or the TGs may need more sophisticated state machines or the CCAs may need to time-stamp messages as they are created so that a TG can execute them in the same sequence. At this time, MGCP messages have transaction identifiers but no time-stamps or sequence numbers. Further work is needed to ensure that MGCP manages remote resources well. Alternately, a different auditing mechanism may be useful.

Appendix C provides an example message flow between CCA1 and TG1 in Figure 4-11 that would cause an error in CCA1's status map. This error would occur without CCA1, TG1, or SSP1 knowing that it happened and would cause SSP1 to repeatedly drop new calls.

[1] In fact, MGCP has two such "audit" messages: Audit Connection and Audit Endpoint.

4.4. Implementations of Framework Architecture in Physical Nodes

As referred in Section 4.2, this document describes the VOP network architecture in terms of functional elements but does not seek to endorse any particular physical architecture. The specifications of the functional elements and the interfaces between key functional elements are not meant to imply any specific physical implementation. Various suppliers should be able to develop functional elements within a single physical node and communicate with the relevant elements in other nodes. In a similar vein carriers should be able to implement components of this architecture to meet their business strategies (e.g., to offer only long distance services initially) using network nodes from their chosen suppliers that include multiple functional elements with in any particular node. There would be differing tradeoffs in terms of cost, reliability, performance, etc. for the various potential implementations. This section provides a few potential implementations of these functional elements as examples. Analysis of the tradeoffs in the various potential implementations is beyond the scope of this document.

The architecture recognizes the CCA and the Service Agent (SA) as two distinct functional elements. This enables the separation of basic call processing from many of the services provided in the network. As the VOP network supports new services, these services would require enhancements to the SA with smaller changes to the CCA. However, suppliers could choose to offer the CCA and the SA in a single node. In cases where a service provider already has a services strategy, the supplier could offer the CCA and the SA bundled into a single node with the functionality to support the services offered by the service provider. Note that even in the cases where a supplier offers the two functional elements (i.e., the CCA and the SA) in a single physical node, the two functional elements could still be treated as distinct logical elements from the perspective of the node's architecture.

Although the elements of the functional architecture may be implemented in a VOP network using relatively small gateway nodes (AG, CG, SG and TG) being controlled by one or more CCAs, the framework architecture does not preclude the implementation of an architecture that consists of network nodes with multiple functional elements. For example, one implementation could deploy a CCA and the AGs controlled by the CCA in a single physical switching node. Such a node would provide functions that are analogous to a local switch in the existing PSTN. Similarly, functions analogous to a tandem switch could be obtained by implementing a CCA and the SGs and TGs associated with the CCA in a single physical switching node. In many instances such an implementation may be preferred by service providers (especially existing carriers deploying VOP to supplement their circuit-switched networks), since such an implementation would be similar to switches in their existing network architecture and could use similar planning guidelines. However, specifics of the implementation scenario would have to be determined through an evaluation of tradeoffs, such as cost, reliability, and performance.

4.5. Roadmap for Generic Requirements

There are essentially three classes of elements that would have to be specified to enable the deployment of interoperable VOP networks. These are described as follows:

1. *Specifications for Functional Elements*

   FEs are the individual building blocks of the VOP network. The key FEs in the VOP network are listed in Section 4.2.1. In addition, this would include the specifications

for the core network to enable the necessary features in the transport network such as QOS. Specification of these elements would provide a common understanding of what functionality is expected from each of the building blocks of the VOP network. These specifications would also have to include the interactions with other FEs.

2. *Specifications of Functionality or Capability of the VOP Network*

   These are the elements that span multiple classes of FEs in the VOP network. Examples of such specifications would include the specifications for aspects such as performance, security and billing in the VOP network. Some other aspects are the specifications for the interface with other networks (PSTN, other VOP networks, other data networks, etc.). Other examples of such elements include the support of advanced services (including services such AIN, E911) in the VOP network. Many of these services would depend on interactions with the PSTN (e.g., for many services it may be necessary to access SCPs in the incumbent LEC network). Such interactions with the PSTN would have to be included in these specifications. While these elements have a broader scope in the network, they depend on specific capabilities within individual FEs. For example, while there is a need for an overall billing strategy, such a strategy would depend on the usage measurements collected in individual FEs.

3. *Specifications for the Protocols to be Used in the Various Interfaces in the VOP Network*

   While the interactions between FEs would be specified in the specifications for the FEs, there may be a need to define new protocols or enhance existing protocols to enable such interactions. For example, while it has been proposed that MGCP could be used for interactions between the CCA and gateways (AG, CG, SG and TG) there may be a need to enhance MGCP to support the interactions needed for the VOP network. Such enhancements would fall under this class of work.

It is proposed that Bellcore Generic Requirements (GRs) would be a suitable medium for specifying the first two elements listed above. However, it may be appropriate to standardize the protocols that are used for the interfaces, since most of the protocols that are used are already standardized, or are expected to be standardized in the near future.

In addition, for the VOP network to be viable, operations and management generic requirements would also have to be considered. Currently, there is no single industry standard that has identified operations and management generic requirements that are specific to VOP operations. An added value of this GR effort will be to provide a common operations specification for the industry. Hence, Bellcore proposes to write functional requirements for operations and management. The initial focus is planned to consist of the following:

- Operations and management subsections to the FE GRs
- A separate VOP Element Management Systems (EMS) GR, the relationship of which to the FE operation is shown in Figure 4-12.

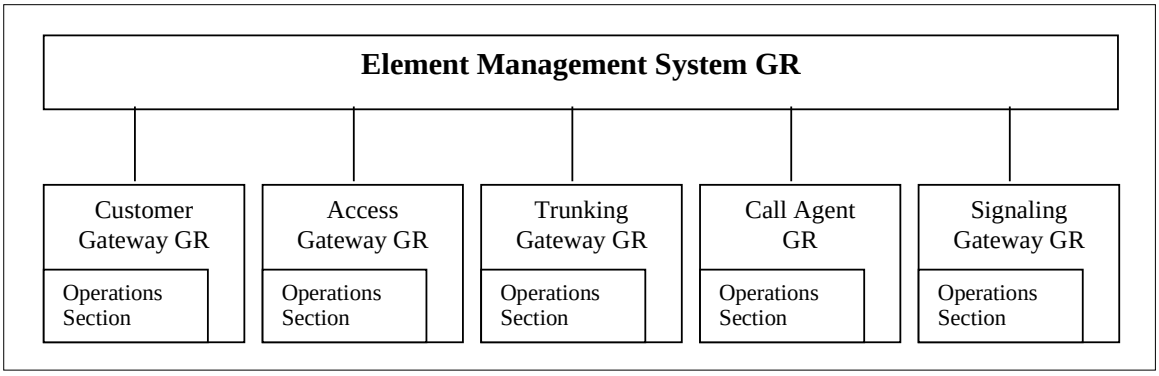

Figure 4-12 Relationship of EMS GR to Operations Sections in the 5 FE GRs

Future operations GR work is planned for the second phase and may cover VOP Network Management System (NMS) and inter-domain management generic requirements.

This GR work is important because it will help create a unified approach to the operations and management interoperability issues currently faced between different networks, services, protocols and equipment. Current telecommunications companies are presently forced to bundle services offered on separate circuit and packet networks for their customers, with separate operations and management systems, resulting in higher capital and operating costs, quality of service limitations, and inefficiencies in delivery. A unified approach to operations and management will have profound affects on improving the delivery of services, and on reducing operations costs for building and operating a single integrated network.

In proposing a path forward for defining a Bellcore GR program for VOP, it may be helpful to consider a sequence of GRs and Special Reports (SRs) to be spread over the near future. GRs that specify individual FEs (item #1 above) could be developed based on the framework developed in this SR to support end to end voice calls over the VOP network. However, GRs for network functionality/capability that span multiple FEs (item #2 above) will have to be based on a higher level strategy for those aspects to be developed in later issues of SRs. In addition, as the functionality in initial GRs is refined and there is a better understanding of industry positions over time, it may be necessary to re-issue a GR that had been developed at an earlier stage. For example, an Issue 2 of a CCA GR would refine/modify the functionality specified for the CCA in Issue 1 of the CCA GR.

Based on the above, the following roadmap is proposed for SRs and GRs in 1999.

An initial set of nine GRs to define key aspects based on the framework in this SR to be started in March/April 1999.

1. GR for User Gateways (AG and CG)
2. GR for Network Gateway (TG)
3. GR for Signaling Gateway (SG)
4. GR for CCA

5. GR for Core Network
6. GR for a Framework of Services
7. GR for Billing Usage Measurements (encompassing the BUM functionality in the CCA and BA)
8. GR for Performance of VOP Network
9. GR for VOP EMS.

In parallel (starting in April), a SR is proposed to provide a detailed strategy for the key network capabilities. Possible aspects to explore in this SR could be the support of key new services, support for LNP, support of E911, and strategies for billing, security and reliability.

A second phase of GRs would have to define specifications of some of these key aspects, in addition to the specifications for the Service Agent (SA). It is assumed that the second phase of GRs would be started six to eight months after the start of the first phase. The specific topics of the second phase of GRs should be decided based on the response to the initial set of GRs and on the feedback obtained in the VOP Forum.

Note that the above discussion is preliminary, and is subject to significant change based on later review and feedback from various participants.

5. Functional Requirements for VOP Network

5.1. Gateway Requirements

5.1.1. Access Gateway

The AG provides customer access to the VOP network from traditional network access interfaces supported in circuit switched networks. In providing this access, the AG is expected to support the following interfaces:

- Non-ISDN Analog line (Conventional 2-wire PSTN access)
- Non-ISDN PBX Trunk Group
- ISDN Basic Rate Interface (BRI)
- ISDN Primary Rate Interface (PRI).

Support for additional interface types beyond those listed here (e.g., Digital Loop Carrier [DLC] system interfaces, interfaces to wireless Radio Systems) is for further study.

Implicit in the VOP architecture is the support of "filtered" analog terminations from ADSL interfaces at the Customer Gateway (CG). That is, an analog signal separated out from an ADSL interface via a splitter is also expected to be terminated at the AG. From the AG's perspective, this analog line appearance is considered to be no different than other analog lines appearances served by the AG.

Within the VOP architecture, each AG is served by one and only one Call Connection Agent (CCA). However, each CCA may serve more than one AG. In the future, each AG may be allowed to be served by more than one CCA. Allowing this capability could be helpful from the perspective of reliability (CCA outages), network unbundling (where individual access interfaces on an AG may be served by different network providers), and possibly number portability (where individual access interfaces on an AG may be served by different network providers).

Call Control for all of these interfaces is governed by the CCA where the AG provides a supporting role. The AG however, needs to participate in the process of logical connection establishment/release via the core packet network. To some extent, the AG needs to participate in the delivery of certain network capabilities and supplementary services to these end users.

As part of logical connection establishment, the AG provides circuit mode to packet mode call conversion (and vice versa), and tones and announcements as appropriate.

5.1.1.1. Overview

The AG provides the primary communication path interface between traditional access interfaces and the VOP network. The functionality ascribed to the AG is similar to that of the access portion of the traditional digital circuit switches, but certainly is not as complex. Figure 4-1 shows how the AG fits into the overall network architecture of a VOP network.

Unlike the architecture of a digital circuit switch, the VOP architecture assumes that the call control capability is resident at the CCA rather than at the AG. On the line-side of the AG, interfaces to the following types of traditional circuit switched CPE are presumed to be supported:

- PBX (over non-ISDN T1 trunk group)
- PBX over an ISDN PRI
- Non-ISDN set (e.g., 2500 set) over a conventional non-ISDN line
- ISDN Terminal(s) over an ISDN BRI.

Each type of access interface has its own characteristics and needs. However, in all cases, the AG operates under the governance of the CCA. Based on instructions from the CCA, the AG performs transcoding of the speech signal from an access line/trunk into packets that are sent to a particular remote node (e.g., a remote AG) providing access to the called user. In this case, a logical connection is used to transport the packets between the local AG and the remote gateway. The AG may need to transcode the voice samples from the access line to a lower bit-rate coding method (such as 32 kb/s ADPCM), maintain the same coding (e.g., μ-law), or for certain international calls perform conversion between μ-law and A-law encodings.

When the AG terminates analog lines, the AG is assumed to provide tones/announcements to the caller during call origination. Tones and announcements could be provided via a local tones and announcements server, a remote tones and announcements server, or via internal tones and announcements capabilities. Identification of specific tones and announcements could be signaled by the CCA to the AG.

To establish calls during a user's request for call origination, the AG must be able to send call request indications to the CCA including the dialed digit information and other information that allows the CCA to identify the source of the call. The type of call request also needs to be indicated (e.g., speech or data).

During call establishment, the AG is expected to interact with the CCA to select a virtual circuit to be used to support the call. The AG must identify the logical connection to the CCA. This is done so that the remote gateway (e.g., AG) and the originating AG both use the same logical connection for the call.

Upon receiving an indication of the successful progression of the call origination, the AG is expected to associate the originating user's circuit/channel with the outgoing logical connection.

During call termination, the terminating AG is expected to establish a logical connection to be used for the call. The AG must identify the logical connection to the CCA. After detecting call answer, the AG is expected to associate the called user's circuit/channel with the incoming logical connection.

5.1.1.2. Architecture and Functions

The AG may be decomposed by identifying the various functions performed by the AG on its own and in terms of interacting with CPE and other network elements. The

architecture of the AG is intended to describe the components of an AG that are essential for providing AG functionality.

Functional components comprising the AG include the following:

- *Access Interfaces*

  The AG supports non-ISDN lines, ISDN BRIs, and multiple DS1 level interfaces to end user CPE (e.g., PBXs) including non-ISDN T1 trunks and ISDN PRIs. Support for additional interface types beyond those listed here (e.g., Digital Loop Carrier [DLC] system interfaces, interfaces to wireless Radio Systems) is for further study. The AG appears to the CPE as a public carrier switch. Support of these interfaces by the AG permits the VOP network to support users with a wide range of existing CPE and CPE likely to be developed in the near future.

- *Connection and Signaling Manager*

  The connection and signaling manager communicates with the CCA. It receives instructions from the CCA to help it set up logical connections, including the associated mapping of AG lines to logical connections via the core packet network. When the access interface is ISDN, this may require transfer of Narrowband ISDN protocol over the packet interface supporting communication with the CCA. However, when the access interface is T1 with AB-bit signaling, this manager must also terminate the inband signaling and be able to forward relevant information to the CCA for processing.

- *Circuit-Mode to Packet-Mode Conversion for Media Streams*

  The various media streams are converted from circuit-mode to packet-mode. Depending on the stream type (e.g., true speech, voiceband data, or 64 kbps circuit mode data), a different conversion technique may be used.

- *Echo Cancellation*

  An adaptive echo cancellation function is included to reduce the impact of near-end echo from any 4-wire to 2-wire conversion that is present between the AG and the end user CPE.

- *Transcoder and Audio Mixing*

  One or more transcoders are used to translate 64 kbps speech signals encoded according to G.711 into other coding schemes. At a minimum, the AG is expected to support transcoders for G.726 and G.728. In addition, it shall be possible to transcode between the A-law and μ-law versions of G.711. Transcoding support for other audio codecs may also be supported. In addition, audio mixing functionality is provided to permit at least two audio data streams to be combined, in support of functions such as operator barge-in.

- *Loopback*

  A loopback capability at each access interface is included in support of access facility testing.

- *Data Detector*

  This optional function detects fax and modem signals. This allows the AG to optionally compress voice connections while leaving fax and modem connections uncompressed. The output of the data detector determines which transcoder is used

for the connection. The detector could also be used to distinguish between fax and data modem and/or to determine the modem speed/type. These capabilities could be useful in generating customer profile information and/or in optimizing network performance. Fax/modem distinctions might be useful in determining optimum packet size or network path establishment. In the future, fax detection capabilities may also be used in support of store-and-forward and other enhanced fax services.

- *Silence Detection/Suppression and Comfort Noise Insertion*

  At the transmitting end, the AG monitors the incoming (from the access) audio stream to detect audio silence based on audio power below a certain threshold. During such periods, no audio payload packets are sent, to increase effective compression. At the receiving end, comfort noise is inserted into the outgoing (to the access) audio during silence intervals (i.e., speech gaps) to simulate background noise.

- *Receive Path Delay*

  This function is used on the receive side to smooth the arrival time of packets in order to reduce distortion to the speech signal associated with jitter.

- *Interface to Core Packet Network*

  The AG has an interface to the Packet Core Network. This interface is used for the exchange of control and signaling with the CCA over secured sessions as well as transmission and receipt of the user information packets associated with each call.

- *Packet Usage and Performance Statistics*

  Usage information for accounting purposes is kept by the AG. In addition, such usage information may be used for network capacity planning, performance measurement and other functions. The AG is expected to communicate this information to the CCA.

- *AG Configuration and Management*

  This function communicates with the network administration personnel or network management systems to support configuration management, fault management and performance management functions.

- *Tone Detection and Generation*

  Tone generation and detection functions are necessary in support of functions such as testing and authorization/accounting code services. Tones generated and/or detected would include DTMF tones as well as single-frequency tones.

5.1.1.3. Access Interfaces

This section describes the access interfaces that may be supported by the AG. A particular AG may support one or more of the interfaces described here.

5.1.1.3.1. Non-ISDN Line

The AG is assumed to support the termination of a conventional non-ISDN interface used with traditional telephone sets (e.g., 2500 sets).

As part of the support of non-ISDN lines, the AG supports the following capabilities:

- Detect Off-Hook
- Provide connection to Tones and Announcements to the non-ISDN line as instructed by CCA
- Detect On-Hook
- Detect Switchhook Flash
- Collect Digits from line via DTMF signaling and Dial-pulse signaling
- Provide Power Ringing to the called party
- Provide Distinctive Alerting Patterns to the called party
- Provide connection to Tones and Announcements for the remote party (called or calling)
- Support timer to be used when called user disconnects to detect off-hook (for re-connection to the call)
- Bridge multiple calls into a multi-way call
- Frequency Shift Key (FSK) signaling (e.g., for delivery of caller ID)
  - For an idle line, transmittal of FSK between power rings
  - For an active line, precede transmittal of FSK with CPE Alerting Signal.
- Application of Call Waiting Alerting tones (including Distinctive Alerting tones).

For call origination, the AG is expected to support the detection of call initiation for these lines (i.e., an Off-Hook indication). Upon determining that a call is to be established, the AG informs the CCA of this event. In this notification, the AG communicates the following information: identification of the originating interface/channel, the type of call to be established (speech or voiceband data), and optionally the resources to be used for the logical connection. As part of the logical connection establishment, the AG associates the indicated logical connection with the originating interface/channel. In addition, the AG needs to perform the appropriate circuit-mode to packet-mode conversion for the requested call.

The AG sends digits to the CCA after collecting all digits provided by the user. If needed, the CCA will request that the AG collect additional digits. In this case, the CCA may also request that the AG provide a tone or announcement as part of the prompt to collect additional digits. Knowledge of how many digits are to be collected from the non-ISDN line is essential from the perspective of the AG. Such knowledge can be pre-provisioned into the AG or provided to the AG by the CCA via a control channel. The collected digits are to be sent to the CCA for interpretation and call handling.

An interesting aspect of indicating the type of call to be established is the determination of whether the call is a true speech call or voiceband data call. Knowledge of the type of call is important in terms of determining whether echo cancellation techniques need to be applied to the call as well as the type of circuit-mode to packet-mode conversion to be applied. Determining whether the call is a true speech call or a voiceband data call could be done in one of several ways.

One way of determining the type of call is by listening for a fax or modem tone. Since the fax or modem tone would be applied by the CPE later in the call than at the time of digit collection, a critical timing issue is when to listen for this fax tone. Another factor to consider is whether listening for a fax/modem tone is intrusive and/or causes any regulatory problems.

Another approach would require the user to dial a code (prefix) before fax calls so that the AG and/or the CCA will be able to identify a fax or modem call prior to the beginning of call/connection establishment. However, this would cause a difference from the user's expected dialing behavior when compared to the circuit switched network.

During call origination, the CCA may instruct the AG to provide a connection to a particular tone or announcement. The AG should not only be able to do this, but it should also be able to provide certain tones autonomously (e.g., dial tone).

When the AG receives an indication from the CCA that a call is to be terminated to a non-ISDN line, the AG is expected to establish a logical connection to the originating gateway. In addition, the AG provides power ringing to the non-ISDN line identified by the CCA. At this time, the AG also provides inband audible ringing towards the calling user for a speech or 3.1-kHz audio call. Provision of the inband audible ring could be accomplished via an interaction with a Tones and Announcements server. The AG may notify the CCA when power ringing has been applied.

If the called line answers the call, the AG is expected to send an answer indication to the CCA and connect the line to the logical connection. In addition, the AG needs to perform the appropriate circuit-mode to packet-mode conversion.

The support of calls that involve an Analog Display Services Interface (ADSI) requires special attention. These calls are established as normal voice calls. However, after the call is answered, the call at some later point transitions to a voiceband data call. Thus, the handling of such calls as true speech calls may hinder the operation of the inband protocol. Further study is required to determine the most appropriate method of handling such calls (e.g., changing the properties of the call after it has been established). Other applications that also use an end-to-end inband protocol over a voice channel through the circuit switched network may encounter similar problems within the VOP network.

Communications between the AG and CCA on behalf of non-ISDN lines for the purposes of call/connection control can take one of the three following forms:

1. Use of Q.931 for call control and MGCP for connection control
2. Use of Q.931+ for call control and connection control
3. Use of MGCP for call and connection control.

Alternative 1 is where the signals received from the non-ISDN line are converted into ISDN Q.931 messages and sent to the CCA for processing. The line is identified via the Channel Identification information element of the ISDN Q.931 protocol. MGCP is used for connection control to establish the call to the called line. MGCP is also used to provide connections to announcements and tones.

Alternative 2 is an extension of Alternative 1 where the Q.931 protocol is enhanced to incorporate a few new elements to handle the identification of the logical connection to be used for the call, identification of an announcement to be played, and possibly the

inclusion of a global call identifier. In this case, the AG is acting very much like an ISDN Terminal Adapter with a few differences.

Alternative 3 is where MGCP is exclusively used for call and connection control signaling between the AG and the CCA.

Alternatives 1 and 2 presume that the control signals from a designated set of non-ISDN lines are converted to Q.931 signaling at the AG. These control signals are then multiplexed into a virtual ISDN D-Channel (signaling channel) between the AG and the CCA for the purpose of exchanging ISDN Q.931 control signaling between the AG and the CCA.

When a selection is to be made from one of the above alternatives, consideration should be given to similar selections to be made for ISDN BRIs, ISDN PRIs, and non-ISDN PBX Trunks so that if possible a uniform, consistent, and common interface is provided between the AG and the CCA for call/connection control.

Support for Supplementary Services requires further study, including handling of switchhook flash, etc.

5.1.1.3.2. Non-ISDN Trunk to a PBX

For this document, only T1 based facilities will be considered. E1 facilities are beyond the scope of this document. In addition, the T1 facilities are considered to be structured facilities supporting 24 channels of 64 kbps each.

Assumptions and requirements of an AG interacting with a CCA in support of a non-ISDN trunk to a PBX are very similar, to those for an AG interacting with a CCA in support of a non-ISDN line (see Section 5.1.1.3.1). A major difference is that the access structure and signaling used on the non-ISDN trunk are unique and distinct from those used on the non-ISDN line. This section will describe those aspects needed for the AG to support a non-ISDN Trunk that are unique or different from the description provided in Section 5.1.1.3.1.

The non-ISDN trunks discussed in this section are digital trunks that support inband signaling (also known as channel-associated signaling). The AG is expected to terminate the channel-associated signaling from the PBX at the AG while sending the appropriate signaling information to the CCA. The AG will need to support all of the signaling techniques that may be applied on a T1 trunk group from a PBX as provided in today's circuit switched network (see Section 5.1.1.3.2.1).

The AG interacts with the CCA as described in Section 5.1.1.3.1 to establish the call/connection. This includes informing the CCA of the type of call, identification of the interface/channel originating the call, and identification of the resources to be used for the logical connection.

A glare condition occurs when the CCA wants to select a channel for call termination that has already been seized for an originating call (by the PBX) where the AG is still collecting digits for the originating call. Such situations can be handled correctly if an alternate channel is used for the terminating call after detection of the glare condition. The possibility for a glare condition occurring is significant in the case of non-ISDN

trunks because inband digit collection on these trunks takes more time than the use of ISDN.

For signaling between the AG and the CCA, the three options described in Section 5.1.1.3.1 apply to the Non-ISDN trunk except that the grouping of multiple non-ISDN T1 trunk groups is not required. That is, a single ISDN virtual D-channel can be used for a T1 trunk group, but the use of a single ISDN virtual D-channel for a group of multiple T1 trunk groups is not required.

Support for Supplementary Services is being considered for further study.

5.1.1.3.2.1. Inband Signaling

Inband signaling trunks are supported on the AG as emulations of particular types of analog voiceband lines and trunks. These emulations are implemented on individual DS-0 channels of DS-1s, which use stolen AB bit signaling. Mappings of the AB bits to supervisory states are described in Section C of MDP-326-140, “Digital Channel Bank - Requirements and Objectives,” formerly known as AT&T PUB 43801, November 1982.

5.1.1.3.2.1.1. Emulated Basic PBX Trunk - Ground-Start or Loop Start Supervision

The most basic non-ISDN trunk interface is an emulated ground-start or loop-start PBX trunk. This type of trunk uses "line-like" call processing: DTMF or dial-pulse addressing, dialtone originating, ring-down terminating. The basic PBX trunk uses the "foreign exchange" AB protocol described in MDP-326-140 for FXO and FXS channel units.

Support of non-ISDN basic PBX trunks is required for the AG. DTMF address signaling is assumed to be standard. Dial-pulse address signaling may be desirable in a small and declining number of applications, but is a low priority for inclusion in an AG.

Ground-start signaling is preferred on basic PBX trunks, because it provides positive recognition of disconnects. Unlike the situation seen with physical voiceband loops for basic PBX trunks (where the cost of loop start is less than the cost of ground start interfaces), the cost of emulated loop-start interfaces and the cost of emulated ground-start interfaces are exactly the same. Therefore, there will be little motivation to use loop-start type signaling, unless a user simply does not wish to go to the trouble of changing options in the PBX. Therefore, ground-start AB bit signaling is required for AG, while loop-start AB bit signaling is desirable but not strictly required.

The basic PBX trunk provides no calling station identification on originating calls, no calling party identification on terminating calls, and no direct-to-station calling on terminating calls. All calls terminating to the basic PBX trunk group must be handled by an attendant at the PBX. Consequently, this type of trunk has limited usefulness for 2-way traffic.

5.1.1.3.2.1.2. Emulated DID/DOD Trunk - E&M or Loop/RB Supervision

A more-capable form of non-ISDN trunk interface is an emulated Direct Inward Dialing (DID) trunk. It is often deployed in a 2-way arrangement which includes both DID and Direct Outward Dialing (DOD). The DID/DOD type of trunk uses "trunk-like" call

processing: MF, DTMF or dial-pulse addressing, with wink start in both directions, and also the possibility for dial tone in the originating direction. The basic PBX trunk uses the "E&M" A/B protocol (or "Loop/Reverse Battery" protocol, which is identical) described in MDP-326-140 for E&M or LPO/LPT channel units.

The DID/DOD trunks provide no calling station identification on originating calls and no calling party identification on terminating calls. They do, however, provide direct-to-station calling on terminating calls, and are therefore preferred by users over basic PBX trunks for terminating service.

A common historical arrangement for a PBX consists of a 1-way terminating DID group in combination with a 1-way originating basic PBX trunk group. Current practice favors the use of 2-way DID/DOD groups for local exchange service. Note that if only 1-way originating non-ISDN trunk interface service is desired, there is little to distinguish between DOD originating service and basic PBX trunk originating service.

Support of 2-way DID/DOD non-ISDN trunks is required for the AG in order for the VOP network to offer terminating non-ISDN trunk service. Both DTMF and MF address signaling are required. Dial-pulse address signaling is not required for AG DID/DOD trunks.

5.1.1.3.3. ISDN BRI

An ISDN interface as defined in National ISDN provides for a standardized network access method over which two B-channels are provided to support calls and a 16 kbps channel (D-channel) supports call control and service control signaling.

Up to eight terminals may be supported on a given ISDN BRI. However, the most common applications include the following configurations:

- A single user where the user supports up to two B-channel terminals for circuit switched voice or data and one or more D-channel packet terminals.
- A single user with a single terminal that can access multiple B-channels for circuit switched voice or data
- Two users where each user has a terminal that can access one B-channel for alternate circuit switched voice or data.

In order to support a National ISDN BRI, the AG must support the following:

- Standard physical layer aspects of a BRI (e.g., 2B1Q transmission)
- Layer 2 - LAPD (Optional)
- Layer 3 – Q.931 (Optional).

Several options exist for how the AG and the VOP network can support an ISDN BRI in terms of call and connection control and ISDN Signaling:

1) Pass ISDN Layer 2 Signaling to the CCA
   1a) Pass ISDN Layer 2 Signaling (including Q.931 messages) to the CCA for call control and use MGCP for connection control
   1b) Pass ISDN Layer 2 Signaling (including Q.931+ messages) to the CCA for call and connection control.

2) Terminate ISDN Layer 2 Signaling at the AG
   2a) Pass ISDN Layer 3 (Q.931 messages) to the CCA for call control and Use MGCP for connection control
   2b) Pass ISDN Layer 3+ (Q.931+ messages) to the CCA for call and connection control.

3) Terminate ISDN Layer 2 and Layer 3 Signaling at the AG, Use MGCP+ (i.e., MGCP enhanced to support ISDN information) for call and connection control signaling between the AG and the CCA.

If Alternative 1 is selected, the AG passes ISDN Layer 2 signaling to the CCA and does not process that signaling.

With Alternative 1a), the AG also simply passes the Q.931 signaling directly to the CCA (for call control) and MGCP is used for connection control.

With 1b), the AG does not process the Q.931 signaling, it does however "look" at some parts of the Q.931 messages (e.g., to identify the B-channel to be used for the call) and adds information relative to connection control (e.g., identification of the logical connection to be used). The CCA could also include information destined for the AG in the Q.931+ messages (e.g., unique global call identifier or announcement to be played).

Within Alternative 1, 1a) provides for transparency of Q.931 signaling (i.e., the AG is not involved at all) whereas alternative 1b) requires the AG to be able to look at certain aspects of the Q.931 messages and be able to add and remove information from those messages. An advantage of alternative 1b) is that it would require less messaging between the CCA and AG to effect connection control since Q.931 messages are being passed anyway. Furthermore, alternative 1b) resolves the issue of timing of when a tone or announcement is provided to the ISDN user relative to when a corresponding Q.931 message is sent (an indication of the tone are included in the Q.931 message). When a tone or announcement is to be provided to the user (with Alternative 1a), the CCA would send a Q.931 message to the user to indicate that a tone or announcement is about to be provided and there the user should "listen" to the channel while an MGCP message is used to instruct the AG to provide the tone. Depending on when the Q.931 message arrives at the user much later than when the MGCP message arrives at the AG, the user may miss the beginning of or perhaps the entire tone or announcement.

In alternative 2), the ISDN Layer 2 signaling is terminated at the AG, but the ISDN Layer 3 signaling is passed on to the CCA. In this case, the AG needs to identify the Layer 2 source of a Q.931 message to the CCA so that the appropriate treatment can be provided to the user. Layer 2/Layer 3 interaction indicators may now need to be passed between the CCA and the AG perhaps by the signaling of the primitives that are exchanged between Layers 2 and Layer 3. For example, if a Terminal Endpoint Identifier (TEI) is removed from service by the AG, the CCA needs to be informed. If a Data link failure occurs at the AG, the AG may need to inform the CCA so that appropriate action is taken on the existing calls on that data link.

In alternative 2a), Q.931 signaling is passed transparently to the CCA by the AG (for call control). MGCP is used for connection control. Passing of Layer-2 to Layer-3 primitive signaling could make use of the transport used for Q.931. Alternatively, this signaling could be via MGCP++ (MGCP enhanced to carry the Layer 2/3 primitives for ISDN).

In alternative 2b), Q.931 signaling is enhanced as described in Alternative 1b) above. In this case, ISDN Layer 2 primitives would use the same transport as the Q.931+ signaling between the CCA and the AG.

In alternative 3, MGCP+ (MGCP is enhanced to support ISDN signaling information) is used to provide call and connection control between the AG and the CCA. In this case, the AG terminates ISDN Layer 2 and 3 signaling, maintains the call states for ISDN, maps MGCP+ signaling to the corresponding ISDN messages as appropriate. In addition, this alternative requires a careful study of how functionality should be partitioned between the CCA and the AG.

Overall, alternative 1 probably has the least impact on the AG and the most impact on the CCA. Alternative 2 should have less of an impact on the CCA compared to Alternative 1. Alternative 3 probably has the greatest impact on functionality required at the AG while the difference between Alternative 2 and 3 may be negligible from a CCA perspective. Table 5-1 summarizes these options.

Table 5-1 Options for Call and Connection Control for ISDN Accesses

Case	AG <-> CCA	
	Call Control	**Connection Control**
1. Pass ISDN Layer 2 and Layer 3		
1a)	Q.931/LAPD	MGCP
1b)	Q.931+/LAPD	Q.931+/LAPD
2. Pass ISDN Layer 3		
2a)	Q.931	MGCP
2b)	Q.931+	Q.931+
3. Terminate ISDN Signaling at AG	MGCP+	MGCP+

In all cases, the AG needs to support 3 qualities of service for the different types of calls that are associated with ISDN BRIs: true speech calls, voiceband data calls, and 64 kbps constant-bit-rate circuit-mode calls. Correspondingly, the appropriate circuit-mode to packet-mode conversion technique needs to be supported. Data detection for ISDN users can be as simple as identifying the originating bearer capability. It is expected that there would be no need to listen inband for any fax/modem tone from an originating ISDN user at an ISDN BRI.

The signaling protocol stack incoming to the AG consists of Q.931 (Layer 3) over Q.921 (Layer 2). The National ISDN version of Q.931 and Q.921 to be supported for the access interface is specified in SR-4620.

Overlap sending is supported on ISDN BRIs (i.e., where the CPE sends called address information to the network over several Q.931 messages). This poses an interesting issue in that for non-ISDN lines, non-ISDN PBX Trunks, and ISDN PRIs, signaling sent from the AG to the CCA assumes that all called address information is sent en-bloc (i.e., in a single signaling message between the AG and the CCA). To support ISDN BRIs, either the AG needs to terminate ISDN layer 3 signaling, collect all address information and

send this information to the CCA (similar to Alternative 3 above) or send all layer 3 messages to the CCA resulting in the called number digits being sent one digit at a time in some cases for overlap sending.

Support for Supplementary Services requires further study.

5.1.1.3.4. ISDN PRI

Support for ISDN PRIs should be similar to the support of ISDN BRIs, however, in this case, it is assumed that there is one CPE interacting with the network over a point-to-point interface. An ISDN Primary Rate Interface (PRI) is structured as follows:

- Single DS1 - 23B+D
- Multiple DS1 – 23B+D + Nx24B
- Backup D-channel – 2x(23B+D) + Nx24B.

In the case of Backup D-channel, one of the D-channels is the primary while the other is the Back-up D-channel. Call control signaling is only exchanged over the primary D-channel.

A National ISDN PRI may support up to 20 DS1s with a Backup D-channel. Some existing implementations go beyond 20 DS1s (up to 28 DS1s providing for up to 670 B-channels).

The alternatives described in 5.1.1.3.3 also apply to an ISDN PRI supported by an AG. For an ISDN PRI, the issues associated with passing L2/L3 primitive information between the AG and the CCA have the most impact in cases where the Backup D-channel is supported.

Thus, for D-channel Backup cases, within alternatives 1 and 2, the AG needs to indicate to the CCA which D-channel a particular Layer 3 message came from. Conversely, the CCA needs to indicate to the AG on which D-channel a Layer 3 message should be sent. Depending on where Layer 3 ISDN Signaling is terminated the AG may or may know which D-channel is primary versus backup.

It should be noted that the network management protocol used on PRI for D-channel Backup and B-channel Availability use a different protocol discriminator than that used by Q.931 messages. However, throughout the use of the term “Q.931 messages” should be understood to include Layer 3 network management messages.

Other aspects for call handling and connection management are as described in Section 5.1.1.3.3.

The National ISDN version of Layer 3 and Layer 2 to be supported for the interface is specified in SR-4619.

5.1.1.4. Management

The AG must provide management capabilities to the VOP Network Operator organized according to the following five management functional areas (based on ITU-T's Telecommunications Management Network [TMN]):

1. Configuration Management
2. Performance Management
3. Fault Management
4. Accounting Management
5. Security Management.

Further details regarding the management capabilities are being considered for further study. Support for Embedded Operations Channels (EOCs) on AG interfaces is also for further study.

5.1.2. Customer Gateway

5.1.2.1. Overview

While the Access Gateway (AG), discussed in Section 5.1.1, provides customer access to the VOP network from traditional access interfaces supported in circuit switched networks, the Customer Gateway (CG) provides network access to some non-traditional CPE, such as IP-phones, personal computers, etc., that could have an associated IP address. Calls originating in the CG would by-pass the AG and go directly into the core network. This functional element is associated with a particular customer (business or residence). The CG will perform the function of adapting the output of the CPE to a form that is compatible with the access network, based on the protocols used. In general, the CG can perform signaling functions for call control, the functions of an ATU-R, etc.

The CG will have a physical interface to the CPE and the network (see Figure 5-1). Also, there will be logical interfaces for network management and the gateway control protocol.

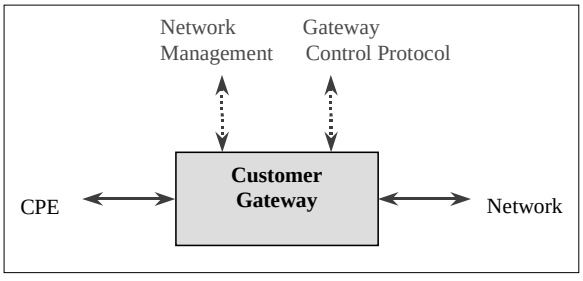

Figure 5-1 Interfaces to the Customer Gateway

5.1.2.2. Working Assumptions for the CG

- CG is located on the customer premise
- No assumption on who owns the gateway – customer or provider

- No assumption on who manages the gateway – customer or provider
- CG is a functional element with different allowed physical implementations.

5.1.2.3. Functions of the CG

There can be different flavors of the CG based on the amount of functionality required and the end system connected to the CG. Typically a CG would perform some combination of the functions listed below. However, in the case of an intelligent device which can perform packetization and other essential functions, the CG can provide minimal functionality such as tunneling of information and resource management. On the other hand, in case of a business customer, using PBXs, one might want to add more functionality to the CG. For example the CG could perform functions such as address translations, call admission control, authentication etc. The selection of the appropriate CG depends on many factors which are for further study.

5.1.2.4. Functional Requirements

The CG may provide a combination of the following functions:

- *Packetization*

  The CG will have to packetize voice into IP/ATM packets for transmission over the network.

- *Call setup and release*

  The CG will communicate with the Call Connection Agent (CCA) to facilitate call setup and release.

- *Call progress information*

  The CG will have to provide the necessary call progress information, such as “dialing number…”, using visual messages or tones as necessary.

- *Translation of protocols*

  Depending on the protocols used in the network, i.e. IP/ATM, and the CPE, the CG will handle protocol translations as required.

- *Interworking of H.323/SIP (customer premise side) with the gateway control protocol (network side)*

  Depending on the capability of the CPE and the flavor of the CG used, this interworking can be done either at the CCA or at the CG.

- *Conversion of media formats between CPE and access network (physical layer)*

  The CG will perform media conversion by translating between analog voice-band signals and digital packetized voice.

- *Interface (logical) with the CCA*

  The CCA will interface with the CG for control functions.

- *Resource management*

  The CG will execute resource management functions for lines and ports, such as access control, mapping of incoming calls to the correct CPE, etc.

The following functions may also be considered:

- Possibly have a mapping of the E.164 number to the IP/ATM address stored in its memory for a quick look up. Alternatively this function could be implemented within the CPE.
- In order to minimize separate CPE boxes, the functions of the CG may be combined with other equipment such as a PBX, an ATU-R in the case of xDSL, etc.

Each function will be researched in depth in the GR.

5.1.2.5. Methods of Access that May Be Used by the Customer

Following is a short list of the different access types that may be used by the customer:

- Twisted Pair – ISDN, xDSL
- Coax and Fiber – HFC
- All Fiber – SONET, PON
- Wireless – Satellite, Cellular, PCS, MMDS, LMDS.

The various CPE that may be used by the customers include the following: PC, Internet phone, cable modem, Ethernet/LAN, PBX, (connected to VOP trunks), wireless phone etc.

5.1.2.6. H.323

H.323 is a standard that specifies the components, protocols and procedures that provide multimedia communication services, such as real-time audio, video and data communications, over packet networks. H.323 is part of a family of ITU-T recommendations called H.32x that provides multimedia communications over a variety of networks. An H.323 terminal can either be a PC or a stand-alone device running an H.323 stack and multimedia applications.

The H.323 standard includes the following core documents:

- H.323 – System Document
- H.225 – Call Signaling
  - RAS – Terminal and gatekeeper association
  - Q.931 – Call signaling
  - RTP/RTCP – Media packetization.
- H.245 – Connection control
- RTP/RTCP – Media transport.

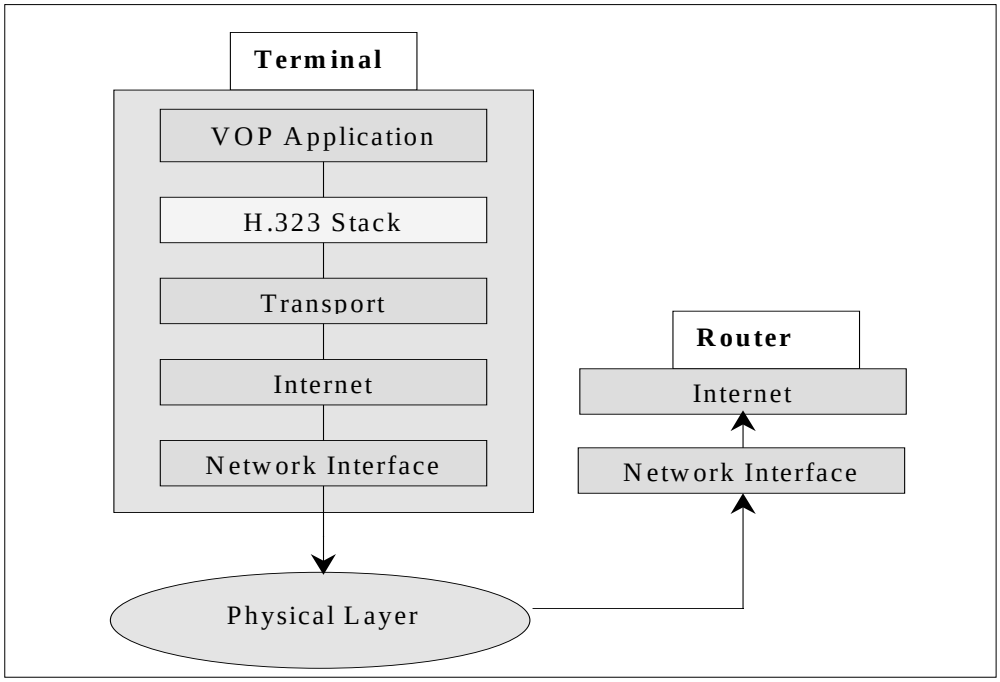

Figure 5-2 H.323 Protocol Stack - Layer Location

5.1.2.7. Session Initiation Protocol

SIP is an application layer, control protocol designed by the IETF. SIP is designed to be independent of the lower layer protocol and makes minimal assumptions about the underlying transport and network layer protocols.

5.1.2.8. H.323 Vs. SIP

Figure 5-2 and Figure 5-3 show the position of the various protocols in the stack when H.323 or SIP is used. H.323 (ITU recommendation) and SIP (developed by IETF) are both standards for signaling and control for Internet telephony. SIP, however, is much simpler. In terms of functionality, H.323 functions can be implemented by the combination of SIP+SDP (Session Description Protocol). H.323 uses TCP for the call signaling and control channel and UDP for the audio channel. H.323 terminals must support the G.711 voice standard for speech compression. SIP can use both TCP and UDP as the transport protocol. H.323 uses binary notation for the messages. SIP, on the other hand, is a text-based protocol. H.323 operations require interactions between many different component protocols, while in SIP all the information is integrated in the SIP request or response. H.323 also has scalability issues.

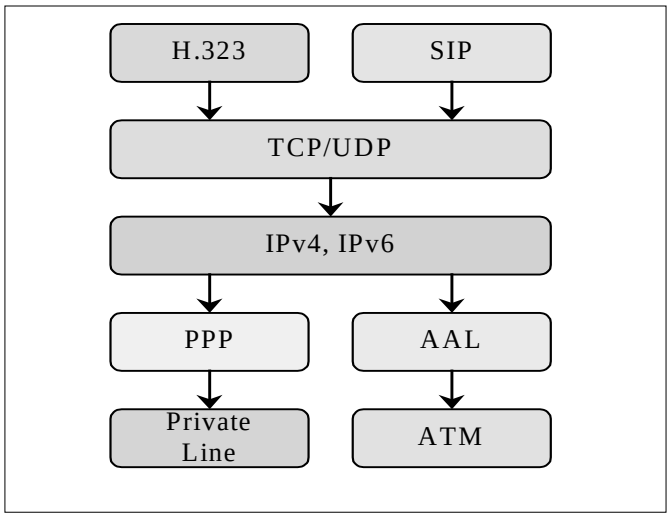

Figure 5-3 H.323, SIP Protocol Stack

5.1.2.9. Gateway Control Protocol

There are a number of control protocols for controlling telephony gateways from external call control elements, i.e., call agents. These are generally master/slave protocols, where the gateways are expected to execute commands sent by the call agent. The choice of the appropriate control protocol is for further study.

5.1.2.10. Open Issues

The following issues are being considered for further study:

- *Functionality of the CG based on customer type and CPE used*

  The functionality of the CG will have different physical implementations based on the different CPE used. For example, if the CPE is attached to an IP phone, it may need to perform call control functions, but may not need to perform packetization. Or in case of ADSL access, the functions of the ATU-R may be integrated into the CG. For customers accessing the network through a PBX, the CG design may be more complicated than in a residential access scenario. These and other similar factors should be considered in further detail.

- *Signaling to and from the CG*

  As shown before the CG has to interact with the network, the CCA and the CPE. Appropriate signaling functions will have to be integrated into the CG for it to be able to communicate successfully with all these devices

- *Interfaces to the CG*

  The CG has to support a number of protocols in order to interface with the various CPE and access networks. The support of the interfaces and the equipment require further consideration.

- *Lifeline support*

  Another issue is that of powering the CG and the CPE during a local power outage. If a subscriber wants to use an IP telephone as their only phone, there may be a need to consider an Uninterrupted Power Supply (UPS) for the CG and the CPE. This issue is being considered for further study.

5.1.3. Trunk Gateway

The Trunk Gateway (TG) provides the communications interface between the PSTN and the Core (VOP) network. One or more TGs (in the same geographic region) may operate under the control of a Call Connection Agent (CCA) to provide interfaces to the PSTN. For voice traffic arriving at the TG from the PSTN, the TG extracts digital voice samples from a specified trunk and inserts them into user information packets which are then routed through the Core network to the destination (such as to a receiving TG or an Access Gateway (AG)). For user information packets arriving at the TG from the Core network, the TG extracts the information samples from the received packets, performs the inverse coding conversion and places the resulting digital signals on a specified trunk for transmission to the destination (via the PSTN). In addition, the TG may perform signal quality enhancements and silence suppression to send packets only when a talker is active to optimize the utilization of the Core network.

The TG consists of the following functional components:

- *Trunk Gateway Manager Module*

  This module is the heart of the TG. This module interacts with all other TG components in the exchange of commands and messages. In addition, some internal system diagnostic, error conditions processing and usage data reporting functions are performed by this module.

- *Logical Connection Manager Module*

  The logical connection manager communicates with the CCA via the Trunk Gateway Manager Module and the CCA Interface. It receives instructions from the CCA to help it set up logical connections including the associated mapping of trunks to Core network addresses.

- *Core Network Interface and Communications Control Module*

  The function of this module is to aggregate voice traffic from multiple users and deliver this traffic to the VOP network for transmission.

- *CCA Interface*

  The TG has an interface that supports the exchange of signaling with the CCA over a secured session as well as transmission and receipt of the CCA-TG packets associated with each logical connection.

- *Operations Functions Interface*

  This interface communicates with the network management and operations support systems to provide configuration, fault and performance management functions.

- *Trunk Interface*

  The TG supports DS0, DS1 and DS3 interfaces. Additionally, a loopback capability at the trunk interface is desirable to support facility testing.

- *Packetization and Depacketization Module*

  This module performs packetization of audio signals (received from the PSTN) and depacketization of data (received from the Core network).

- *Data Detector Module*

  This function detects fax and modem signals. This allows the TG to optionally compress voice connections while leaving fax and modem connections uncompressed. The output of the data detector determines which transcoder is used for the connection. The detector could also be used to distinguish between fax and data modem and/or to determine the modem speed/type. These capabilities could be useful in generating customer profile information and/or in optimizing network performance. Fax/modem distinctions might be useful in determining optimum packet size or IP network path establishment.

- *Echo Cancellation Module*

  This module performs the adaptive echo cancellation function which reduces the impact of near-end echo from the 4-wire to 2-wire conversion on the loop side of the local switch.

- *Transcoder and Audio Mixing Module*

  This module has one or more transcoders to translate encoded speech signals (from data to voice or from voice to data). In addition, audio mixing functionality is provided to permit at least two audio data streams to be combined, in support of functions such as operator barge-in or bridging.

- *Silence Detection/Suppression and Comfort Noise Insertion Module*

  This module monitors the audio stream at the transmitting end to detect audio silence based on audio power below a certain threshold. During such periods, no audio payload packets are sent, to increase effective compression. At the terminating end, comfort noise is inserted into the received audio during silence intervals (i.e., speech gaps) to simulate background noise.

- *Receive Path Delay Module*

  This function is used on the receiver side to smooth the arrival time of packets in order to reduce distortion to the speech signal associated with jitter.

Figure 5-4 presents the functional architecture of the TG. Details of the above functional components are described in the following subsections.

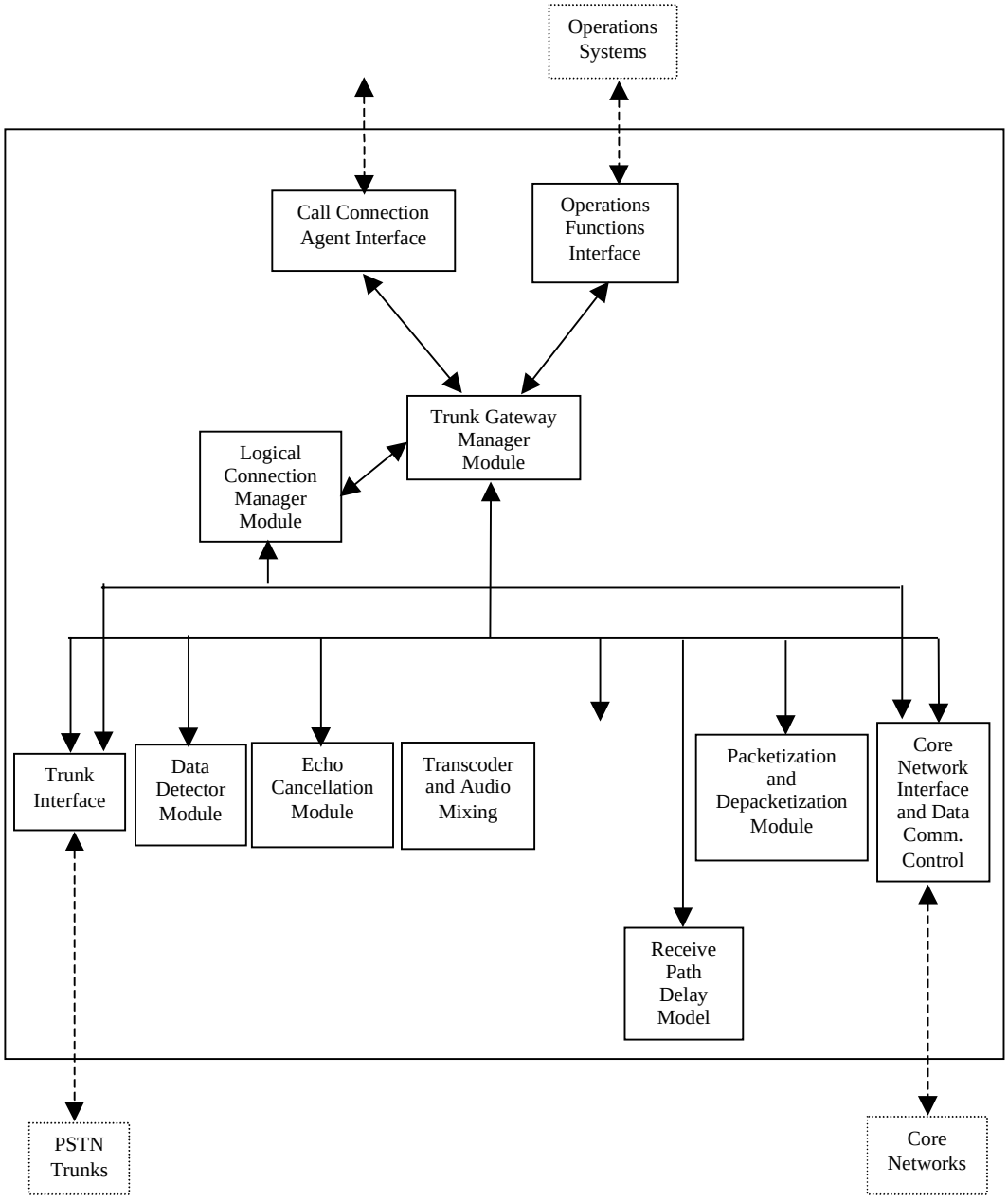

Figure 5-4 Functional Architecture of the TG

5.1.3.1. Trunk Gateway Manager Module

The Trunk Gateway Manager Module is the heart of the TG. This module uses a high speed data bus to interact with all other TG components in the exchange of commands and messages for session control: setting-up, maintaining, and terminating a session under instructions from the CCA. The Trunk Gateway Manager Module also provides near real-time diagnostic and monitoring of port and user status, so that the state information can be sent to the CCA which implements TG control and management policy decisions. Some usage information may be collected by the Trunk Gateway Manager Module for network capacity planning and performance measurement.

5.1.3.2. Logical Connection Manager Module

The Logical Connection Manager in the TG performs a collection of functions necessary to set up, maintain, and terminate connections requested by the CCA. The Logical Connection Manager shall be capable of terminating DS0, DS1 and DS3 trunk circuits. The Logical Connection Manager can have the capability to attach a digital signal processor of the appropriate type to an incoming SS7 trunk circuit on a per-connection basis, such that signal processors will not need to be dedicated to each trunk termination or to a specific trunk group.

Logical connection setup and teardown is controlled by a CCA and communicates the resource control to the TG via a generic industry standard protocol. In order to simplify logical connection control interactions, allow maximum flexibility for future service introduction, and reduce the cost of the TG, minimal logical connection control intelligence may be implemented in the TG, which simply maps and unmaps trunks to ports under CCA control. It will be necessary for the CCA to be able to verify that the status of a logical connection at the TG is consistent with its own record of connection status. In support of this logical connection audit need, the TG shall respond to CCA inquiries concerning the following: (a) the status/existence of a logical connection based on the associated logical connection identifier, and (b) whether a trunk termination is idle and available for assignment to a new call.

5.1.3.3. Core Network Interface and Communications Control Module

From the data communications point-of-view, a TG is like an “Edge Server”, where it sits on the edge of a packet switched data network and allows dynamic access to it. The basic function of the TG’s Communications Control module is to aggregate voice traffic from multiple users and deliver this traffic to the Core network for transmission. By aggregating traffic to provide a highly-filled interface to a packet network, a TG could allow better use of access facilities and the Core network’s switching capacity.

The basic functions of the Communications Control module include the following:

- Acting as a common platform to provide broadband service access interfaces (i.e., PVC) for Frame Relay (FR) and Asynchronous Transfer Mode (ATM) networks
- Multiplexing packets onto a higher-rate digital interface on the Core network
- Support of the lowest layer(s) interface functions for the Core network

- Conduct traffic management to permit Quality of Service (QOS) differentiation in the Core network.

5.1.3.4. CCA Interface

The CCA interface is responsible for sending and receiving all messages between the TG and its CCA node. This interface must establish secure associations with the CCA, according to a standard security architecture as specified by the IETF.

5.1.3.5. Operations Functions Interface

The Operation Functions Interface communicates with an external Element Management System (EMS) which provides a gateway to upstream Operations Systems responsible for the following five management functional areas:

1. The Configuration Management function includes network configuration and installation support.
2. The Performance Management function monitors the effectiveness and status of equipment and physical transport facilities.
3. The Fault Management function includes detecting, reporting, and isolating faults in the network and controlling network resources to protect services. The TG will need to report alarms and support diagnostics and network testing at its interfaces.
4. Accounting Management- For each call attempt made through the TG, the TG may record/compute the following information, log it to recoverable media, and report this information to an external accounting system at the completion of the call:

- Unique call identifier (the CallId provided by the CCA to uniquely identify each call)
- Security authentication certificate
- Number of audio packets sent
- Number of audio packets received
- Number of audio packets lost
- Number of audio bytes transferred.

The above information will be supplemented by information otherwise collected or computed by the CCA (e.g., call end reason, call start and end timing) in support of service management functions such as providing customer rebates based on quality of service.

Security management- This function provides for the prevention and detection of improper use of network resources and services, for containment of and recovery from theft of service and other breaches of security, and for security administration.

5.1.3.6. Trunk Interface

Support of DS0, DS1 and DS3 trunk interfaces by the TG is required for interfacing with the PSTN. In addition, tone generation and tone detection will be needed to support continuity checks, loopback testing, and test calls. In support of these functions, the TG must be capable of applying tones used as prompts, confirmations, and rejections under CCA direction, over the control interface.

5.1.3.7. Packetization and Depacketization Module

Voice signals are packetized and depacketized using RTP and RTCP as specified in IETF's RFC 1889. RTP is used for real-time service support such as timestamping and sequence numbering. RTCP is used for assessing quality of service. In addition, RFC 1890 includes specifications of standard audio encodings and their naming for use within RTP that are applicable.

5.1.3.8. Data Detector Module

The Data Detector function allows the TG to determine whether the signal on the trunk is a voice or a non-voice (e. g., G3 fax, modem) signal. This function can apply DSP technology to the audio stream to detect the fax CNG signal and corresponding signals used by various modems. The ability to discriminate among the various ITU-T specified modem and fax standards and speeds of operation is desirable. If the signal is determined to be non-voice, the TG may dynamically change its transcoder to a coding scheme that ensures an appropriate level of signal transparency. The ability to distinguish among different modem types/speeds permits additional compression to be achieved in the case of certain lower speed modems. The detection of disabling tones may be considered to be part of the data detector function to be implemented within the TG.

5.1.3.9. Echo Cancellation Module

At some point between the Trunking Gateway and the near-end customer's telephone, there will be a 4-wire to 2-wire conversion (for example, at the LEC SPCS or in a digital loop carrier system), which will create an echo path. To mitigate the impact of this echo, the TG must allow for insertion of digital echo cancellation as specified in ITU Recommendation G.168.

5.1.3.10. Silence Detection/Suppression and Comfort Noise Insertion Module

The TG must support active speech detection capability and silence suppression. A gap in speech is determined on the basis of the associated audio signal power level dropping below a specified threshold. To reduce speech clipping problems and facilitate the setting of an appropriate comfort noise level at the receiving end during silence suppression periods, the transmitting TG should continue to send audio packets for a short period even after the silence criteria is achieved. However, to assure that silence suppression achieves its compression objectives, the period covered by active audio packets should not exceed the period of actual speech activity (according to the established criterion used by the speech detector) by more than 5%. The TG must disable silence suppression if voiceband data is detected or a modem echo cancellation disabling tone is detected.

If silence suppression is used, an "uncomfortable" silence occurs at the receiving end if the end user hears total silence. Thus, during intervals of silence suppression, the terminating end TG inserts "comfort" noise or white noise designed to mimic normal background noise for the connection. This minimizes the perception of abrupt transitions between periods of silence and speech and assures the listener that the connection is still active. It is recommended that the terminating end determine the appropriate power level for the comfort noise to be inserted during silence intervals by measuring the corresponding power level at the tail end of the preceding talk spurt. This is another

reason why the transmitting TG end should include *at least* one packet with background noise following the end of the talk spurt before initiating the ensuing speech gap (i.e., stopping the transmission of packets with audio content to signal a period of silence.)

5.1.3.11. Transcoder and Audio Mixing Module

In setting the encoding scheme and audio payload size, one generally wishes to meet the needs of the audio content being transported and minimize delay, while making effective utilization of network bandwidth. Larger packet payloads improve network utilization by reducing the per-packet effective overhead. However, larger packets also result in increased end-to-end delay. The following factors determine the appropriate encoding scheme and audio payload per packet:

- The type of content (i.e., voice or fax/data)
- The prevailing network congestion, as indicated by the packet loss rate experienced.

The nominal value for the sampling rate is 8000 samples per second (8 kHz) with a tolerance rate of 50 parts per million. As part of the transcoding from G.711 64 kb/s PCM to other encoding laws, provision must be made for conversion of encoded digital signals to and from uniform PCM (i.e., 14 bit linear PCM). Transcoding to/from the uniform PCM stream and 32 kb/s Adaptive Differential PCM stream (ADPCM), as specified in G.726, should be supported. This transcoding should be via 15-level non-uniform adaptive quantizer with each quantized level specified in G.726, using four binary digits per sample. The TG should also support 16 kb/s Code Excited Linear Prediction (CELP) audio encoding as specified in G.728 and associated transcodings to and from other supported encoding options.

The audio mixing functionality permits incoming audio data streams of at least three call legs to be combined to support functions such as operator barge-in. This audio mixing function performs digital addition of separate encoded audio streams and selective on-off control of the talk and listen paths for each stream, along with any necessary conversions to/from linear PCM and level adjustments to assure intelligibility of the resulting combined audio.

5.1.3.12. Receive Path Delay Module

Receive path delay is designed to provide a continuous audio stream at the receiving end in the presence of jitter within the network. Setting the appropriate delay and buffer requirements represents a tradeoff between memory cost and end-to-end delay concerns on one hand (i.e., receive path delay too high) and excessive rate of audio packet discards on the other hand. If the receive path delay is not high enough, an unacceptably high fraction of audio packets will arrive with a relative jitter delay that is larger than can be accommodated by the configured delay buffer. The approach to setting an appropriate receive path delay will be based on dynamic estimation of the mean value of jitter at the TG. The criteria for determining the delay buffer size based on the measured jitter should assure that no more than 1% of packets are dropped because they arrived too late.

5.1.4. SS7 Signaling Gateway

VOP signaling interconnection to the PSTN will be provided by the SS7 Signaling Gateway (SG). The signaling gateway is responsible for receiving SS7 messages over a set of links from a SS7 node and encapsulating the user information (either ISUP for call

setup or SCCP/TCAP for service related signaling) contained in the message for distribution to the CCA. The signaling gateway is also responsible for receiving user information (either ISUP or SCCP/TCAP) from the CCA and performing lower level transport management on the message before sending the message out on the links to the interconnecting SS7 node. The interconnection model used for the signaling gateway interconnection should be that of a signaling end point, specifically an SS7 capable switching point (i.e., SSP). As a result of this interconnection model, each signaling gateway should have at least one SS7 Signaling Point Code (SPC) assigned to it and should be responsible for all signaling interconnection for a set of trunk gateways. Also, this interconnection model implies that the signaling linksets between the signaling gateway and the interconnecting SS7 node will be either A-links or F-links. If the signaling gateway interconnects to the PSTN via a STP pair in the SS7 network, A-linkset interconnection will be used. F-linkset interconnection would be used when a signaling gateway interconnects to a SS7 end node (e.g., SSP or SCP).

Interconnection to the PSTN using A-links or F-links allows the VOP network to "appear" as an interconnecting switch. This reduces the complexity of the interconnection because the SG only needs to support a subset of the complete MTP capabilities that apply to end nodes (as opposed to STPs). For example, if the SG uses an A-link interconnection to the PSTN, it is not required to support the full network management procedures (such as broadcast TFP/TCP procedures) and only needs to implement the adjacent MTP Restart procedures. The specific MTP functions that the signaling gateway should support are described in the next subsection.

The relationship between CCAs and signaling gateways is based on support of the trunk gateways. Specifically, each signaling gateway should send all received user information to the CCA that manages the trunk gateways. Therefore, each signaling gateway should interact with a single CCA, but each CCA may be responsible for interacting with multiple signaling gateways. Figure 5-5 illustrates A-linkset interconnection to the PSTN(s) and the relationship between multiple signaling gateways and a single CCA.

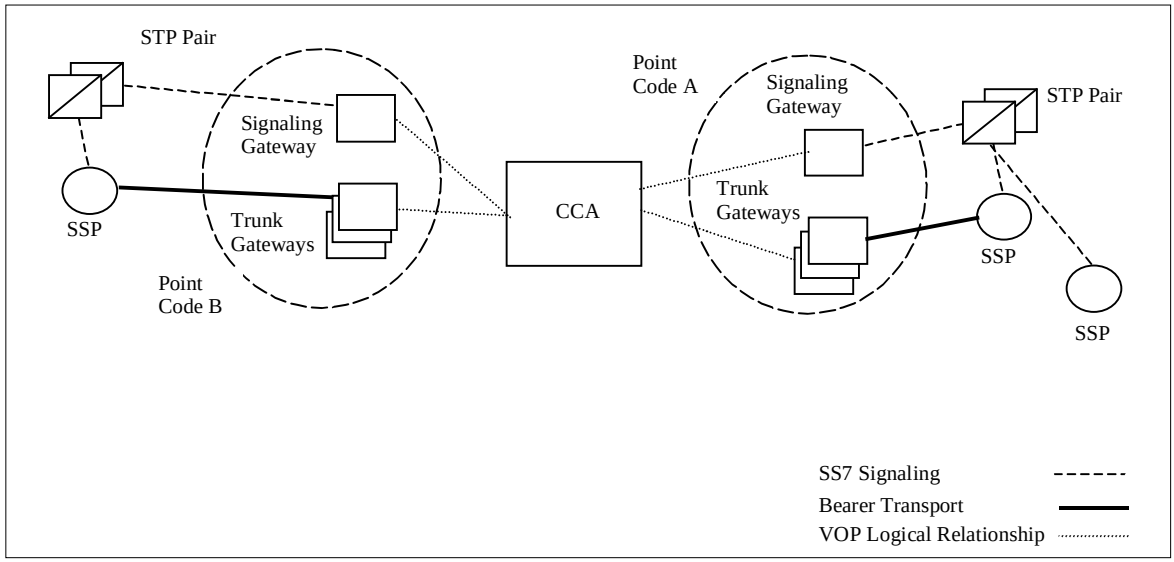

Figure 5-5 Example A-Link Interconnection

5.1.4.1. SS7 Functions

The Signaling Gateway should support MTP level 1, 2, and 3 for the purposes of providing the CCA with SS7 interconnection to the PSTN. The Signaling Gateway should support only the set of MTP procedures that apply to a signaling end point because it will interface with the PSTN via A-linksets or F-links. Specifically, the Signaling Gateway should conform to the MTP functions described in the following subsections.

5.1.4.1.1. MTP Level 1

MTP Level 1 defines the physical, electrical, and functional characteristics of a signaling data link and the means to access it. Level 1 provides a bearer for the signaling link.

The signaling gateway will need to support SS7 signaling data link interconnection to the PSTN. Each signaling link that connects a SG to a CCS node should be a digital bi-directional transmission facility. The two data channels providing opposite directions of transmission should each operate together at a data rate of 56-kbps. The operational signaling data link should be exclusively dedicated to the use of SS7 signaling between the SG and the interconnecting CCS node.

5.1.4.1.2. MTP Level 2

MTP Level 2 defines the functions and procedures for, and relating to, the transfer of signaling messages over one individual signaling data link. The Level 2 functions together with a level 1 signaling data link as a bearer provides a signaling link for reliable transfer of signaling messages between two points.

1. *Signaling Unit Delimitation and Alignment*

   Each signaling unit is indicated by a special 8-bit pattern at the beginning and of the message. Specifications for signaling unit encoding ensure that the special 8-bit pattern is not replicated in the contents of the signaling unit. If the bit pattern on a link is not allowed by the delimitation procedures (more than 6 consecutive ones) or the signaling unit exceeds a certain length, loss of signaling unit alignment occurs. Once signaling unit alignment had failed on a given link, procedures are initiated as part of the signaling unit error monitor.

2. *Signaling Unit Error Detection*

   At the end of each signaling unit there is a set of 16 bits used for error detection. The check bits are generated at the transmitting node's MTP 2 level function. The specific encoding of the check bits is based on the preceding bits in the signaling unit with the exception of the opening delimitation bits. The receiving nodes MTP function uses the check bits and associated encoding algorithm to assure that the signaling unit contents have not been corrupted during transmission and transport. If the check bits and the signaling unit contents are inconsistent the receiving node's MTP 2 function will indicate the presence of errors and discard the signaling unit.

3. *Signaling Unit Error Correction*

   Error correction as implemented in the MTP level 2 procedures is accomplished via a positive/negative acknowledgment retransmission procedure. A transmitted signaling unit is stored in a buffer until positive acknowledgment is received from the

receiving node. If negative acknowledgment is received, the transmitting node will interrupt the sending of all untransmitted signaling units and resends all signaling units not positively acknowledged starting with the signaling unit that was negatively acknowledged.

4. *Signaling Link Initial Alignment*

   Signaling link initial alignment procedures are executed each time a new link is brought into service and when a link is returned to service after a failure. When this procedure is executed the MTP level 2 function at each end of the link that is being aligned exchange status information and provision a proving period for the link. Only the link that is being aligned is involved in the re-alignment procedure; no other link is used for transmission of alignment information.

5. *Signaling Link Error Monitoring*

   There are two types of signaling link error monitoring employed by MTP level 2. The first signaling link error monitor is called the "alignment error rate monitor" and is used during a link's proving period. This error monitor is used to assure that a newly aligned link is able to carry "real" traffic without error using test bit patterns.

   The second error monitor is called the "signaling unit error rate monitor" and is based on the signaling unit error count. The signaling unit error count is then incremented or decremented by using the "leaky bucket" principle. The leaky bucket principle adjusts the signaling unit error count based on the error performance of the link (i.e., how long the link has operated error free). This error monitoring procedure is used during normal link operation when it is in service and uses a set of criteria based on the error measurement for determining when to take a link out of service.

6. *Flow Control*

   When congestion is detected at the receiving end of a signaling link flow control procedures are initiated. The congested receiving node's MTP level 2 function notifies the remote transmitting node's MTP level 2 processor of the condition by means of a link status signaling unit. The receiving node's MTP level 2 function then withholds acknowledgement of all incoming message signaling units until the congestion abates. While the congested state exists the receiving node's MTP level 2 function periodically notifies the remote transmitting node of the condition. If the congested state continues for an extended period of time the remote transmitting node should take the link out of service marking it as failed.

5.1.4.1.3. MTP Level 3

MTP level 3 is responsible for transport functions and procedures that apply to the operation of signaling links as a group (i.e. the management of the signaling linkset). These functions fall into two distinct groups: signaling message handling functions and signaling network management functions. Signaling message handling functions (items 1 though 4 on the list below) are responsible for the actual transfer of messages to the proper signaling link or to the higher level function. Signaling network management functions (items 5 though 15 on the list below) control, based on a predetermined set of criteria about the status of the signaling network, the current message routing and configuration of the signaling network facilities. When the status of the signaling network changes MTP level 3 is responsible for the reconfigurations or other actions associated with the preservation or restoral of normal message transfer capabilities at the node.

1. Message Routing Function

The message routing function determines the outgoing link that is used for the transport of an outgoing message based on information in the routing label of a message. The routing label consists of the Destination Point Code (DPC), the Originating Point Code (OPC), and the Signaling Link Selection (SLS) Code. The point codes are the SS7 address for signaling points. The DPC is the signaling point code used in routing to the destination of a message. The OPC is the signaling point code for identifying the originating node that sent the message. The signaling gateway should have only one linkset connected to it, and therefore all messages regardless of DPC will use that A-linkset for message transport. All messages sent from the signaling gateway should use the signaling gateways point code as the OPC.

2. Message Discrimination and Distribution Function

Message discrimination is the determination of whether the signaling gateway is the destination for a received message. Because the signaling gateway interfaces with an SS7 network, as a signaling end point all messages received at the signaling gateway should be addressed to the signaling gateway (i.e., no signaling transfer function). The signaling gateway should examine each message that is received and determine if the message is addresses to it via DPC. If the DPC of a received message does not identify the signaling gateway, the message should be discarded.

If the DPC does identify the signaling gateway, the message distribution function is then invoked to deliver the message to the appropriate MTP user for further processing. The information required for message distribution is contained in MTP level 3 of the message in the Signaling Information Octet (SIO). There are three possible users for the MTP at the signaling gateway: ISUP, SCCP, or MTP network management. If the user part is MTP network management, the signaling gateway will process the message locally. If the user part is either ISUP or SCCP the message is transferred to the CCA or further distribution and processing using the interface discussed in Section 5.1.4.2.

3. Loadsharing

Once the signaling linkset for an outgoing message has been chosen based on the message routing function, a particular link within the linkset is selected based on the SLS field contained in the MTP level 3 portion of the message. The purpose of loadsharing is to distribute traffic evenly over the links within the linkset or links within a combined linkset, even during failure conditions when some of the links may not be available for transport of traffic. A combined linkset is a collection of one or more linksets. Because the signaling gateway should have a single set of combined A-links (an A-linkset between the signaling gateway and each STP in a mated pair), it will only need to support loadsharing of traffic over a combined linkset.

4. Message Sequencing

The SS7 signaling link protocol is designed to ensure that all messages sent over the same signaling link will be received at the destination point in the same order they were transmitted. Signaling network management procedures were designed with the intent that all messages sent by a node that have a common SLS code and DPC will be transmitted over the SS7 network through the same signaling nodes and use the same signaling links. This is done in order to assure that the order of transmission at the originating node is retained at the destination. Changes in link availability may

cause the different signaling links to be selected for routing of messages with the same DPC and SLS, but message sequence is still retained in these cases.

5. *Signaling Link Activation*

   Signaling link activation is used to bring a new link into service or restore a link that has failed. In order to activate a link, the signaling gateway will first perform the MTP level 2 procedures for signaling link initial alignment. Once initial alignment has been completed successfully, signaling link tests are then initiated (item 14 in this list). Once these tests have successfully completed, the signaling link is ready for the transport of signaling traffic. If the signaling link tests fail, the link activation process is repeated until either the link activation process is successful or manual intervention terminates the activation process.

6. *Signaling Link Changeover*

   Once a signaling link has been put into service and is carrying signaling traffic, it may be taken out of service (either automatically or manually) or may fail. If a link becomes unavailable because of failure or removal from service, a signaling link changeover procedure is performed to divert signaling traffic from the failed link to alternate links (within the linkset) as quickly as possibly, while avoiding message loss, duplication, or missequencing.

7. *Signaling Link Changeback*

   The signaling link changeback procedures are used to initiate the routing of traffic over a newly available link. The objective of the signaling ink changeback procedures are to ensure that signaling traffic is placed upon the newly available link as quickly as possible without message loss, duplication, or missequencing.

8. *Forced Rerouting*

   When a signaling route from a signaling gateway to a destination becomes unavailable due to remote failure, the signaling gateway should divert traffic to an alternate signaling route if one is available, by means of the forced rerouting procedures. The objective of these procedures is to restore the routing capability to a destination as quickly as possible to minimize the consequences of a failure.

   The term remote failure means that a failure is reported to the signaling gateway via network management messages and should be distinguished from a local failure such as loss of the linkset. Note that forced rerouting procedures are only initiated as a result of a remote failure of a route. If the failure is local (e.g., linkset failure) changeover procedures would be initiated.

9. *Controlled Rerouting*

   The controlled rerouting procedures are used to restore optimal signaling routing and to minimize message missequencing. These procedures are used when network management messages are received at the signaling gateway indicating that a previously unavailable route has become available or an available route is restricted. Controlled rerouting differs from forced rerouting in that there is a delay between the time when traffic is stopped on one linkset and started on an alternate linkset. This is because during controlled rerouting the signaling route is not lost, but being adjusted for optimal routing where in forced rerouting the signaling route is lost and the traffic must be redirected immediately.

10. MTP Restart

When a signaling point has been isolated from a network for some time it cannot be sure that the status of the routing information it maintains is still valid. Thus, problems could be encountered when the sending of user traffic is resumed because it does not have accurate status information, and therefore needs to perform many parallel activities while resuming transport of signaling traffic (e.g., link activation, changeback procedures, network management messaging). MTP restart allows a restarting node sufficient time to activate its signaling links, exchanging routing information with adjacent nodes, and recover from isolation in a controlled and organized manner.

These procedures may be optional for the initial signaling gateway implementation, but may be desirable because they allow a restarting node to gracefully recover from failure. Note that because the signaling gateway functions as a signaling end point, it would only need to support the adjacent node restart procedures, not the full restart implementation.

11. Management Inhibiting

Signaling link management inhibiting is requested by operations personnel when it becomes necessary (e.g., for testing or maintenance purposes) to make or keep a signaling link unavailable to user-generated signaling traffic. Note that while a signaling link is inhibited, the link is still operational at MTP level 2. Specifically, a signaling link that is inhibited (but active and in service) is capable of transmitting and receiving maintenance and test messages.

Inhibiting can be requested by management functions at either end of the signaling link and will be granted provided it does not cause a signaling route to become inaccessible or certain circumstances have not occurred (e.g., congestion).

12. Congestion Control

When a node experiences congestion (i.e., it receives traffic faster than it can process and transmit traffic), it must selectively discard some of the traffic in order to reduce the processing demand placed on that node. There are congestion control procedures defined in the MTP layer to relieve the congestion by performing discard of messages and forcing originating signaling nodes to cut back the volume of traffic they generate. The congestion control procedures defined in the SS7 protocol use a set of criteria to indicate which messages the congested node should discard and which messages the originating nodes should not generate until the congestion level has abated. All SS7 messages are assigned one of four different message priorities, 0, 1, 2, and 3. These priorities are not used to determine the order of message processing but rather to determine which messages will be routed in a congestion situation. The signaling gateway should be capable of initiating these procedures and processing messages from remote nodes that have become congested.

13. Signaling Route Management

The purpose of signaling route management is to ensure a reliable exchange of information between signaling points about the availability of signaling routes. The signaling gateway will be notified of signaling route set conditions by a set of signaling route management messages. These messages are sent between the signaling gateway and the STPs in the SS7 network to which it is connected in order

to provide information concerning the status and availability of signaling routes to other signaling points.

14. *Signaling Link Tests*

    The signaling gateway should be capable of periodically performing tests on the signaling links to ensure that the signaling link performance requirements are met. A signaling link test message should be transmitted when a signaling link is activated or restored or when a signaling gateway receives a request from maintenance personnel. Note that signaling link test and signaling link test acknowledgment messages are transmitted only on the link that is being tested.

15. *MTP User Flow Control*

    If MTP were unable to distribute a received message to a local user (e.g., ISUP, SCCP) because that user is unavailable, MTP User Flow control procedures would be initiated. In this case, MTP User Flow Control procedures would send a message to the originating signaling point indicating that the user part in unavailable. The originating node would not send any more user traffic to the node until the condition is resolved.

    According to current Bellcore requirements, these procedures are optional at signaling end points. The reason these procedures are considered optional is that depending on the signaling end point implementation, it may be unlikely that the MTP user part can fail independent of the MTP function. However, because the proposed VOP architecture is distributed and it is likely that the MTP user parts (located in the CCA and SA) can be isolated from the MTP layer (located in the signaling gateway), these procedures would be highly desirable.

5.1.4.2. Signaling Gateway Interworking with CCA

As mentioned previously, the signaling gateway is responsible for SS7 interconnection to the PSTN. As a result, the signaling gateway should support the MTP functions of the SS7 protocol and be capable of encapsulating the protocol user data within the received SS7 messages for delivery to the CCA. In addition to supporting message transfer between the CCA and the PSTN, the signaling gateway should also notify the CCA of flow control conditions and remote PSTN node isolation.

The protocol for communication between the CCA and signaling gateway has not yet been defined. While the protocol has yet to be defined, specific functions should be relayed over the interface between MTP (located at the signaling gateway) and the MTP "user" (the CCA). Furthermore, each function should provide the set of routing and status information necessary for the CCA and signaling gateway to process these functions correctly.

At a minimum, the following four functions should be included in the interface between the CCA and the signaling gateway:

1. *Transfer* – The transfer function is used between the signaling gateway and the CCA for the exchange of messages transported to and from the PSTN.
2. *Pause* – The pause function is sent from the signaling gateway to the CCA, notifying it that a remote PSTN node is inaccessible. The CCA should not send any more user traffic (either ISUP or SCCP) to the involved signaling gateway destined for the inaccessible node. This function would reduce the amount of traffic transported over

the VOP network to a signaling gateway that cannot successfully route the message to the PSTN.

3. *Resume* – The resume function is sent from the signaling gateway to the CCA, notifying it that it can resume sending traffic to the signaling gateway for a previously inaccessible PSTN node. This function cancels the pause function.

4. *Status* – The status function is sent from the signaling gateway to the CCA in order to notify the CCA that the signaling gateway is unable to provide complete message transport to a remote PSTN node. This function should account for at least two cases: signaling link congestion and remote "user" unavailability. These cases correspond to the MTP level 3 functions Congestion Control and MTP user Flow control, respectively, that are supported at the signaling gateway. The CCA should not send any traffic of the type (contained in the status message) to the affected signaling gateway until the condition has abated.

Table 5-2 shows a listing of the functions that should be supported in the interface between the CCA and the signaling gateway, as well as a listing of information that may be required in order to successfully process the function.

Table 5-2 CCA/Signaling Gateway Interface Functions

Function	Information Necessary for Processing
Transfer	Originating address, destination address, Signaling Link Selection Code (See 5.1.4.1.3, item 3), Signaling Information Octet (See 5.1.4.1.3, item 2), user data (i.e. ISUP, SCCP)
Pause	Affected destination address
Resume	Affected destination address
Status	Affected destination address, cause (either signaling link congestion and remote "user" unavailability)

5.2. Call Connection Agent Requirements

First, a call model is described to facilitate description of the CCA functional requirements.

5.2.1. Call Model

Call/service processing builds upon the current call processing infrastructure of existing digital exchanges using a generic abstract representation of call control functionality to process basic two-party calls and supporting service functionality to invoke and manage advanced services. The following call/service processing functions apply to the CCA call model:

- A call is either between two or more end users that are external to the network and addressable (via a directory number, combination of directory number and bearer capability, or another form of address), or a call is between one or more end users and a network entity.

- A call may be initiated by an end user, or by a Service Agent within the network on behalf of an end user. To supplement a call, service logic applications may either be

invoked by an end user served by a Call Connection Agent, or by the network on behalf of an end user.

- A call may span multiple networks. As such, each network only controls a portion of the call - call processing is functionally separated between networks. Service applications invoked in such an inter-network call are managed independently by each network.
- The CCA can be viewed as having two functionally separate sets of call processing functions that coordinate call processing activities to create and maintain a basic two-party call. This functional separation is provided between the originating portion of the call and the terminating portion of the call. This functional separation should be maintained to allow service applications invoked on the originating portion of the call (e.g., on behalf of the calling party) to be managed independently of service applications invoked on the terminating portion of the call (e.g., on behalf of the called party).
- It is desirable to allow multiple service applications to be simultaneously active for a given end user. It is also recognized that current supplementary services and other service features (e.g., toll-free service) will continue to exist. As such, service/feature interaction mechanisms may be required.
- The distributed approach and added complexity of call/service processing requires mechanisms for fault detection and recovery, providing graceful termination of calls and appropriate treatments for end users.

In the current circuit switched network, Call Models (Originating and Terminating) have been specified to support these call/service processing functions. A Call Model provides a high-level service and vendor/implementation independent abstraction of call and connection processing. For VOP, this abstraction would facilitate interoperability of systems (CCA, gateways, service agent and RTS) within a VOP network and interconnection between networks (VOP to VOP and VOP to PSDN/ISDN) by providing a common abstraction of call processing to all systems and networks involved in the call.

Calls are modeled to consist of originating and terminating call portions that are represented by Originating and Terminating Call Models which can be independently influenced by service applications. This is illustrated in Figure 5-6 for a basic two-party call (Party A calls Party B). The Originating Call Model detects a call set-up request on Party A's facility (i), and the Terminating Call Model detects a call completion request to Party B's facility (ii). If a call involves supplementary services or call features requiring assistance of a service agent, the Call Connection Agent (based on Call Model detection of the service request or call processing event) would communicate the request/event to an appropriate Service Agent. The Service Agent could then influence subsequent call processing based on the service application. Note that the CCA would not require assistance of the service agent for the completion of every call that involves a supplementary service or a special feature (see Section 5.3).

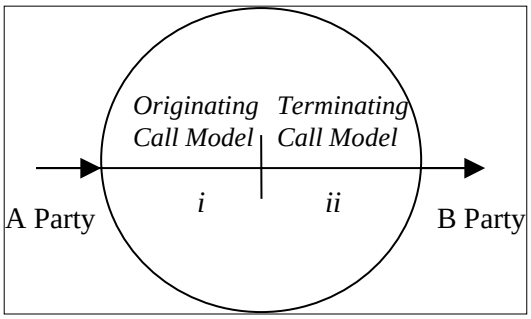

Figure 5-6 Originating and Terminating Call Models

The Call Model could also support a variety of access and network signaling protocols (e.g., MGCP, ISUP) and provide a common abstraction of this signaling information to service applications. The Call Model identifies points in basic call and connection processing when service applications are permitted to interact with basic call and connection control capabilities. In particular, the Call Model provides a framework for describing the following:

- Basic call and connection events that can lead to the invocation of service applications or that should be reported to active service applications,
- Points in call and connection processing at which these events are detected, and
- Points in call and connection processing at which call processing can resume.

The points in call, detection points, call processing transitions, and call processing events associated with the Call Model may be represented using Finite State Machines or using Object Oriented methodologies.

The CCA call processing is schematically shown in Figure 5-7. The CCA will initiate originating call processing based on the information received from the calling user (via the serving access gateway or a customer gateway), ISUP signaling from the PSTN/ISDN (via a signaling gateway), or another CCA. The CCA will process the call, potentially with the help of the service agent and the RTS based on the specific service features required for the call. Subsequently, the CCA will complete terminating call processing, possibly with the assistance of the service agent and RTS, instruct the appropriate bearer gateways (trunk, access and/or customer) to setup the connection, and send call related information to the called party (via the serving access or customer gateway) or towards the called party in the PSTN/ISDN (via a signaling gateway) or in the VOP network (via another CCA). The CCA will be capable of providing the traditional end-office as well as tandem switch functionality.

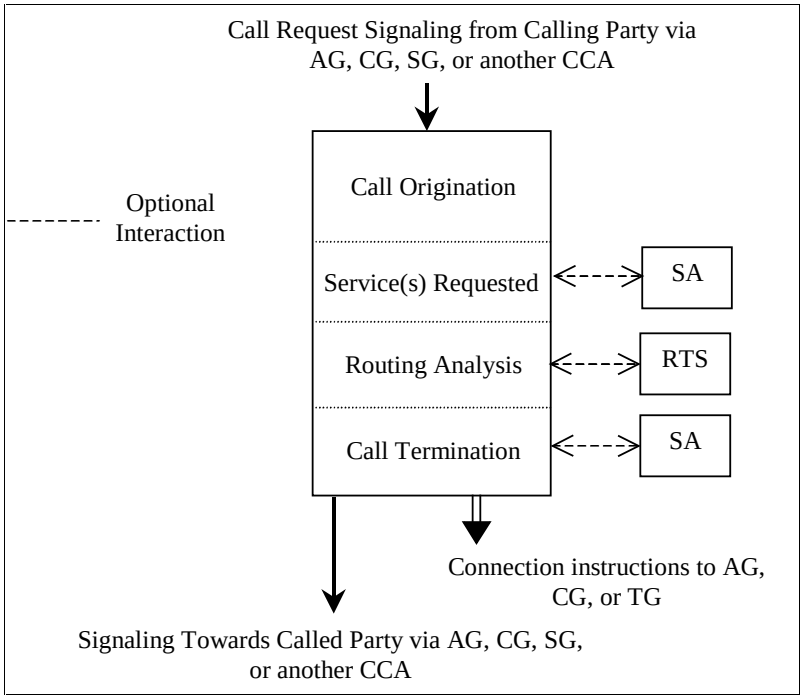

Figure 5-7 CCA Call Processing (Schematic)

A CCA provides a VOP network with most of its basic call and connection control capabilities. These capabilities can be divided into the three broad functional classes: bearer gateway (i.e., TG, CG, or AG) connection control, call processing, and network management interactions.

Bearer gateway connection control allows a CCA to alter the state of a bearer gateway's resources (e.g., connect a tone generator to an access line, connect two end-points to provide transmission path for user information through the gateway, etc.). In particular, the relationship between a CCA and a subordinate bearer gateway is assumed to be a master-slave relationship rather than the traditional peer-to-peer relationship that exists between PSTN switches. Given that assumption, the signaling between a CCA and a bearer gateway should emulate the messaging between call processing in a PSTN switch and the lower hardware layers in that switch.

In contrast, call processing in a CCA provides call and connection control and signaling to call processing entities in other nodes (e.g., a PSTN switch, another CCA or a CPE) as appropriate. It includes interworking with ISUP, which provides trunk management and supervision processes for circuit-switched trunks between VOP and PSTN/ISDN; interworking with other CCAs, which allows logical connections between bearer gateways and VOP networks controlled by different CCAs to be setup and released; interactions with bearer gateways, which enables a CCA to react to events on the user-network interface (e.g., an off-hook transition or a setup request on the user-network interface); and call routing, which ensures that calls are routed properly. Call processing also supports basic user features (e.g., routing to an IXC based on a pre-subscribed carrier identification code). The call processing in the CCA provides basic call control and some service features. To provide certain service features, it may take help of the SA or the RTS, while retaining overall control of the call (refer to Section 5.3).

Finally, network management functions enable a CCA to alter the state of a call in response to network abnormalities and to take appropriate actions for network protection and recovery. These abnormalities include the congestion or failure of a signaling link between the SG and the PSTN, management of bearer resources connecting the VOP network and the PSTN, the failure or congestion of a network node (including another CCA) that the CCA interacts with; and the graceful startup and shutdown of network elements that the CCA interacts with.

The remainder of this section describes these three functional groups in greater detail.

5.2.2. Gateway Connection Control

This section describes Bellcore's view of the functional elements needed in a CCA to manage connections within the CCA's subordinate bearer gateways. These functional elements allow a CCA to control the state of a bearer gateway's resources (e.g., access lines, trunks, check-loops, transponders, echo-control-devices, and logical connections), instruct a bearer gateway to watch for events (e.g., an off-hook transition), and request that a bearer gateway generate an inband tone or announcement.

5.2.2.1. Connection Model

This subsection describes a connection model that consists of endpoints, connections, and calls.

An endpoint is a user information (data) source or sink in a bearer gateway. It may be physical or logical, and it is associated with a unique Endpoint_identifier. Examples of endpoints include a TG interface terminating a PSTN trunk and an AG interface terminating an analog POTS connection from a phone.

A connection is an association between two endpoints in a bearer gateway. The purpose of a connection is the exchange of data between the endpoints. When a connection is created, it is assigned a Connection_identifier, which is unique within the bearer gateway. A call within a VOP network consists of a set of connections between endpoints and logical connection(s) through the core packet network. Each call is assigned a globally unique Call_identifier, and all connections involved in a call share that identifier. This identifier may be used for billing, connection control, or network management purposes.

5.2.2.2. Basic Connection Control Functions

Given this model, a CCA should be able to create and delete connections in subordinate bearer gateways (TG, AG or CG) and monitor endpoints in those gateways. In particular, the following generic connection management functions and commands are needed:

- Create Connection – to create a connection within a bearer gateway
- Modify Connection – to change the parameters associated with an established connection
- Delete Connection – to delete an existing connection or indicate that a connection is no longer sustainable
- Audit Connection – to audit the status of any connection.

- Notification Request – to instruct a bearer gateway to monitor an endpoint and watch for specific events (e.g., off-hook transition)
- Notify – to inform a CCA that an event has occurred
- Audit Endpoint – to audit the status of any endpoint
- Out of Service/Restart – to notify a CCA that a bearer gateway (or a group of endpoints within a gateway) has been removed from service or returned to service.

Additionally, a CCA should be able to limit the flow of data between the endpoints in some situations (e.g., prior to the Called Party answering).

Finally, a CCA and a subordinate bearer gateway should be able to exchange connection setup parameters. Some example parameters are: encoding method, packetization period, bandwidth, type of service, usage of echo cancellation, usage of silence suppression or voice activity detection, usage of signal level adaptation and noise level reduction or "gain control," usage of reservation service, usage of RTP security, and type of network used to carry the connection.

MGCP supports the functions described in this subsection.

5.2.2.3. TG Connection Control Functions

A trunk gateway provides a bearer interface between the PSTN and the packet network. In such a gateway, the endpoints are the trunk circuits, logical connections to the core packet network, and tone generators.

A CCA should be able to instruct a TG to apply the following call related signals to an endpoint: ringback tone, confirm tone, network congestion tone, intercept tone, preemption tone, and no circuit tone.

A CCA should also be able to instruct a TG to detect and generate the following tones: a 2010-Hz continuity check tone, a 1780-Hz continuity check tone, a 1000-Hz Milliwatt tone, a 1004-Hz Milliwatt Tone, and a Reorder Tone (120 impulses per minute). Furthermore, when such a tone is detected, the TG should notify the CCA.

Continuity check tones are used when a CCA wants to test the continuity of a trunk. There are two types of tests, single tone and dual tone. The CCA should be provisioned with information that describes which test should be applied to a given trunk.

Note that MGCP supports the functionality described in this subsection.

5.2.2.4. AG Connection Control Functions

The Access Gateway (AG) provides customer access to the VOP network from traditional network access interfaces supported in circuit switched networks. In providing this access, the AG is expected to support the following interfaces:

- Non-ISDN Analog line (Conventional 2-wire PSTN access)
- Non-ISDN PBX Trunk
- ISDN Basic Rate Interface (BRI)

- ISDN Primary Rate Interface (PRI).

Support for additional interface types beyond those listed there (e.g., Digital Loop Carrier [DLC] system interfaces, interfaces to wireless Radio Systems) is for further study.

The CCA instructs the AG to establish and release connections in support of calls that it processes. During the call establishment, the CCA may instruct the AG to provide the following: a tone or announcement to the local user or remote user; an indication of the type of circuit to packet conversion to be used; an indication of the remote gateway; an alert to the user about the presence of a call; and a bridge of two calls into a three-way call (e.g., for operator barge in). In addition, certain abnormal occurrences at the user interface may be reported to the CCA (user remains off-hook even after permanent signal has been applied).

The signaling to be used between the AG and the CCA for call and connection control may involve one of several options as described in Section 5.1.1. Depending on the option selected the CCA may need to support one or more communications channels to the AG and one or more protocols. The selection of which communication means are used requires further study.

5.2.2.5. CG Connection Control Functions

A customer gateway provides an interface between non-traditional CPEs (e.g., IP-phones) and the packet network. In such a gateway, the endpoints are the access lines, logical connections to the core packet network, and tone generators.

The CCA should be able to instruct a CG to provide a tone, an announcement or other appropriate call related indication to the user.

The CCA should also be able to instruct the CG to collect dialed digits from the Calling Party and detect off-hook transitions, on-hook transitions, flash-hook occurrences, and answer tones. The CG should be able to provide call related communication between the user and the CCA.

Note that MGCP supports the functionality described in this subsection.

5.2.2.6. Resource Management and Synchronization Processes

The connection model discussed in Sections 5.2.2.1 and 5.2.2.2 suggests that a master-slave relationship exists between the connection control procedures in a CCA and its subordinate bearer gateways. In other words, a CCA makes most (if not all) connection control decisions associated with a call, and a bearer gateway simply follows instructions from a CCA.

To make such decisions correctly, a CCA should track the state of various resources in its subordinate bearer gateways. In particular, a CCA should maintain a status map of those resources, and update the map whenever a resource changes state.

For a subordinate TG, a CCA should maintain a status map of the trunks terminating at the TG, and each trunk should be assigned one of the following states: “unequipped,” “transient,” “active,” “locally blocked,” “remotely blocked,” or “locally and remotely

blocked." Furthermore, a trunk in one of the last four states should also be marked "idle," "incoming busy," or "outgoing busy."

Similarly, a CCA should maintain a status map of the access lines terminating in a subordinate AG. In this case, the potential states include "in-service," "out-of-service," "off-hook," and "on-hook."

A CCA may also track the state of logical connections to the core packet network in a bearer gateway. Doing so may reduce unnecessary signaling between the CCA and the bearer gateway, but it is not necessary.

Note that the separation of a resource's state in a CCA from its actual state in a bearer gateway may cause a difficulty. Should the two states go out of sync, a CCA could make incorrect decisions and cause a reduction in call throughput in the bearer gateway. To keep these states in sync, the protocol between a CCA and a bearer gateway should be designed to minimize such synchronization errors. Including an "audit" message, which could be sent by a CCA to collect and return the status of a bearer gateway's resources, is one possible solution[2]. When the CCA receives an "audit response," it would update its status map according to the contents of the message.

Such auditing of a bearer gateway's resources, however, can corrupt an otherwise accurate status map in a CCA unless sufficient safeguards are devised. Appendix C on sample call flows provides one corruption example and discusses possible solutions.

5.2.3. Call Processing

This section describes Bellcore's view of the functional elements needed in a CCA to provide connection control between call processing peers in a network. These functional elements include interworking with PSTN/ISDN switches via ISUP, interworking with other CCAs, responding to call processing events in a bearer gateway, and call routing.

5.2.3.1. Interworking with ISUP

In the existing PSTN/ISDN, ISUP provides connection control procedures (e.g., call setup and release); circuit supervision processes (e.g., blocking and reset); and mechanisms to handle error conditions and abnormal events. To interface with the PSTN/ISDN via a TG, a VOP network must be able to correctly originate, process, and act on ISUP messages. In other words, it must be able to interwork with ISUP.

This interworking should occur in the CCAs because they control the TGs. To support ISUP signaling, a CCA should be able to decode and generate all ISUP messages, perform any function indicated by an ISUP message, create any suitable response (e.g., returning an RLC after an REL is received), and manage all appropriate ISUP timers. These functions, responses, and timers are defined in GR-317-CORE and GR-394-CORE for PSTN switches and TR-NWT-000444 for ISDN switches, respectively. A CCA that serves a TG should provide functionality similar to that found in these three GRs. This functionality is represented by the following three groups of ISUP messages:

1. Call setup and release is handled by the IAM, ACM, ANM, REL, RLC, RSC, SUS, RES, CPG, FAC, and CFN messages.

[2] In fact, MGCP has two such "audit" messages: Audit Connection and Audit Endpoint.

2. Circuit blocking and unblocking are managed by the BLO, BLA, UBA, UBL, CGB, CGBA, CGU, and CGUA messages.
3. Testing, maintenance, and error situations are handled by the CCR, COT, CQM, CQR, CVT, GRS, GRA, and UCIC messages.

The CCA should also be able to handle following errors: dual seizure, the receipt of unrecognized or unexpected messages (e.g., two IAMs for the same circuit), the receipt of messages containing unrecognized or inappropriate parameters, and the failure to receive a particular message (e.g., no ACM or ANM in response to an IAM).

To support this interworking with ISUP, a CCA should be provisioned with the following maps:

- OPC, DPC, and CIC to TG_address and Endpoint_identifier – used to identify a trunk from a TG's perspective when an ISUP message is received
- TG_address and Endpoint_identifier to OPC, DPC, and CIC – used to identify a trunk from a PSTN switch's perspective when an ISUP message is sent
- PC to SG_address – used to identify the SG serving a particular PC.

5.2.3.2. Interworking with Other CCAs

A CCA needs to signal another CCA when a call involves connection segments involving bearer gateways and VOP network system controlled by the other CCA. The CCA processing the incoming segment of the call needs to provide the following functionalities:

- Call Routing – The CCA performs call routing, possibly with the help of the RTS. As the result of the routing analysis the CCA will know which other CCA it needs to communicate with for the setup of the next connection segment.
- CCA-to-CCA Signaling – The CCA needs to signal the other CCA all the relevant call-related information so that the other CCA can proceed with the setup of the next leg of the call. CCA's need to exchange only the call and connection related information (e.g., service features, carrier selection, etc.). Only the information that is normally carried in ISUP call control messages need to be signaled between the CCAs. In other words, information needed for the setup and release (normal as well as failure case) of call and connection need to be exchanged. In general, this functionality is provided by the following ISUP messages: IAM, ACM, ANM, REL, RLC, SUS, RES, and CPG. A CCA should also be able to exchange supplemental call related information with other CCAs. Such information includes billing information, IAM parameters, and connection setup parameters (see the last paragraph in Section 5.2.2.2). Additionally, a CCA should be able to handle or prevent the following errors: the receipt of unexpected or unrecognized messages, the receipt of messages containing unrecognized or inappropriate parameters, and the failure to receive a particular message.

To support interworking with other CCAs, a CCA should maintain the following dynamic map:

- Call_identifier to Next_CCA_address – used to identify the next CCA in the signaling path if one exists.

For CCA-to-CCA signaling, ISUP call control messages with appropriate enhancements would be a good potential choice. Generally, ISUP maintenance messages (e.g.,

blocking) would not be needed. A CCA need not know the status of a bearer gateway controlled by another CCA.

5.2.3.3. Interacting with Bearer Gateways

The call setup signaling information between the CCA and the user flows through the AG and CG which will provide the necessary protocol mappings. It should be noted that the call processing will be under the control of the CCA. A CCA should be able to react to events that occur in its subordinate bearer gateways. In TGs, these events include the detection of a continuity check tone and the loss of a logical connection associated with a call. In AGs, these events include on-hook transitions, off-hook transitions, flash-hook occurrences, the availability of dialed digits, and the loss of a logical connection associated with a call.

When such an event occurs, the Bearer Gateway (BG) should notify the CCA. Depending on the event and the state of the call affected, the CCA may then instruct the bearer gateway to perform a subsequent action (e.g., collect digits after an off-hook transition) or alter the state of the call by signaling another CCA or PSTN/ISDN switch (e.g., release after an on-hook transition).

To support these interactions with a subordinate bearer gateway, a CCA should maintain the following dynamic maps:

- Bearer Gateway_address and Endpoint_identifier to Call_identifier – used to identify which call is affected by an event.
- Call_identifier to BG_address and Endpoint_identifier – used to identify the endpoints involved in a call.
- Call_identifier to BG_address and Connection_identifier – used to identify the connections involved in a call.

5.2.3.4. Call Routing

The CCA shall be able to route calls based on information in an IAM (e.g., called party number), in a "setup message" from another CCA (e.g., "joe@home.org"), or received from a AG/CG (e.g., dialed digits).

The routing may be done using internal routing tables, using the help of the RTS or SA, or some combination of all these.

The routing may be influenced by vertical services (e.g., call forwarding) or intelligent network features such as toll-free service.

If routing tables in an RTS are used, the CCA shall be able to query an RTS for the routing information.

5.2.3.5. Message Routing

The CCA receives messages from the SS7 network via the SG. The CCA also sends messages to the SG to be routed over the SS7 network. This signaling relationship between the CCA and SG exists for both ISUP based and SCCP based (i.e., TCAP) SS7

signaling exchanges. The CCA initiates ISUP based message exchanges while the SA is responsible for initiating SCCP based message exchanges. SCCP based message exchanges between the SG and SA are routed through the CCA because the SA and SG do not have a direct signaling interface in this architecture. Therefore, the CCA needs to support a message distribution function to determine where a received message (from either the SG or SA) should be sent.

The message distribution in the CCA should be based on the information contained in the message received from the SG or SA. In the case of messages received from the SG, the CCA should be capable of determining if the message should be processed locally (e.g., an ISUP message), forwarded to the SA (e.g., an SCCP message), or in some cases both (e.g. remote SS7 users become unavailable). Likewise, the CCA should be capable of identifying whether messages received from the SA should be processed locally or forwarded to the SG for routing over the SS7 network.

5.2.3.6. User and Service Information

The information that is provisioned against a user's line, access or DN in a traditional switch is expected to be stored in the CCA. Examples of such information are pre-subscribed carrier code and the user subscription information for services such as caller ID (see Section 5.3).

5.2.4. Network Management

5.2.4.1. SS7 Network Management

The CCA will detect abnormal events in the interconnected CCS network via information received from the SG. It will need the functionality to handle the following events:

- CCS link congestion
- ISDNUP flow control
- PSTN/ISDN node isolation.

5.2.4.2. Congestion or Failure of the Logical Signaling Links

The CCA will need the functionality to handle congestion or failure of the following logical signaling (control) links:

- Link between a CCA and a subordinate SG
- Link between a CCA and a subordinate TG
- Link between a CCA and a subordinate AG or CG
- Link between a CCA and an RTS
- Link between a CCA and a SA
- Link between a CCA and another CCA.

5.2.4.3. Congestion or Failure of Nodes

The CCA will need the functionality to handle congestion or failure of the following nodes it either controls or interacts with:

- An SG
- A TG

- Bearer gateways (AG, CG)
- An RTS
- An SA
- Another CCA
- Possibly, nodes within the packet network.

5.2.4.4. Node Startup and Shutdown

The CCA will need the functionality to handle the startup and shutdown of the following nodes it either controls or interacts with:

- An SG
- A TG
- Bearer gateways (AG, CG)
- An RTS
- An SA
- Another CCA
- Possibly, nodes within the packet network.

The CCA will also need the functionality to ensure the consistency of resource status and other information between the CCA and the affected node.

5.2.4.5. Management of Bearer Resources between VOP Network and PSTN

This section gives a high level view of the functionality needed in the CCA to provide maintenance control functions to manage bearer resources between the VOP network controlled by the CCA and the interconnected PSTN. The maintenance control functions include reset of resources, blocking of circuits, signaling of congestion control, etc. The CCA should be able to process an ISUP maintenance control message received from the PSTN or in case of a failure within the core network, it should be able to generate an ISUP maintenance control message towards the PSTN.

5.2.4.5.1. Action on Receiving ISUP Maintenance Messages from the PSTN

In the existing PSTN, ISUP provides maintenance control procedures (e.g., reset and blocking) to handle error conditions and network abnormalities. To interface with the PSTN, the CCA must be able to decode and process the ISUP related maintenance control messages. In other words, it should be able to provide the interworking function for the ISUP maintenance control messages.

Upon receiving an ISUP maintenance control message due to an abnormal event in the PSTN, the CCA should be able to do the following:

- Process the received information
- Perform any function indicated by the maintenance message
- Instruct the involved bearer gateways (i.e., TG, CG, or AG) and/or another CCA of the appropriate action to be taken
- Generate an ISUP maintenance control response message towards the interfacing PSTN.

In some cases, if appropriate, the CCA receiving the ISUP maintenance control message may also need to instruct other involved CCAs of the appropriate action to be taken. For example, if an ISUP Reset Circuit (RSC) message is received from the PSTN, the CCA shall process the information and send the release message(s) towards the involved bearer gateway(s) for the affected connection segment. It shall also generate an ISUP Release Complete (RLC) message towards the PSTN. The CCA my also send release messages towards other CCAs (if multiple CCAs are involved in the call path). It should be noted that when a PSTN switch sends an ISUP maintenance control message towards the VOP network, the latter has to provide the functionality to appear as another PSTN switch.

5.2.4.5.2. Generation of ISUP Maintenance Messages Towards the PSTN

In case of the failure in the core network (e.g., TG failure) controlled by the CCA, the CCA should be able to generate the ISUP maintenance control messages (e.g., blocking message, reset circuit message) towards the interfacing PSTN. In addition, it should also be able to instruct other involved bearer gateways (i.e., TG, CG, or AG) of the appropriate action. In some cases, if appropriate, the CCA may also need to instruct other CCAs (if multiple CCAs are involved in the call path) of the appropriate action. For example, if a CCA suffers memory mutilation it will not know the status of the connection, e.g., idle, busy incoming, busy outgoing, etc. and therefore, identifiers and logical connections at all the involved nodes should be reset to idle condition. The CCA should be able to send an ISUP Reset Circuit (RSC) message towards the PSTN to invoke reset of the affected circuit at the interconnected PSTN switch. In addition, it shall also send release message(s) towards the involved bearer gateway(s) for the affected connection segment. If multiple CCAs are involved in the call path, the CCA may also need to send release messages towards the other involved CCAs.

5.3. Service Agent Functions

The Service Agent (SA) should provide the logic for vertical services such as toll-free and LIDB calls. One way an initial line of distinction could be drawn between the services performed by the CCA and the SA would be that any current ISDN/PSTN service that requires the use of TCAP would be supported in the SA, including non-traditional services that are not currently offered in ISDN/PSTNs. According to these criteria, a call involving call forwarding or caller ID service will be processed by the CCA without the help of the SA. However, the CCA will invoke the assistance of the SA in processing a toll-free call. The functionality of the SA can be broken down into two operations; the execution of service logic for a transaction that occurs completely within the VOP network and the execution of service logic that requires signaling to an external SS7 signaling end point (i.e., an SSP or SCP).

Figure 5-8 presents an example of Service Agent Interaction. This example architecture will be used to describe the operation of services in a VOP network. The signaling interface between the SA and CCA has not yet been defined, but may be based on TCAP depending on the division of functionality between the CCA and SA and on the services offered in the VOP network.

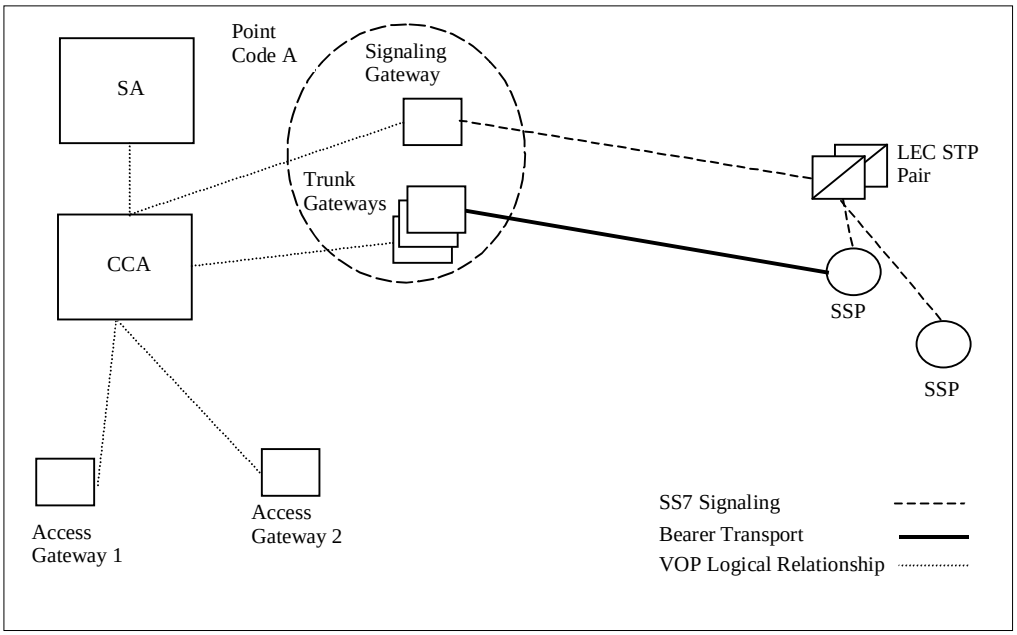

Figure 5-8 Example Service Agent Interaction

When an intranetwork service is performed in the VOP network, an access gateway or customer gateway signals the CCA with the user entered information (i.e., dialed digits). The CCA then "triggers" on the user entered information, recognizing that further processing of this information is required at the SA. The CCA should then signal the SA with the user entered information, as well as information relating to the originating customer, if necessary. The SA would then process the user entered information, identifying the service required and executing the service logic for that service. The SA then signals the CCA with instructions for execution of this transaction with the customer. An example of an intranetwork VOP service requiring the SA could be an Automatic Callback transaction between two VOP customers. In this example, a customer at Access Gateway 1 in Figure 5-8 attempts to setup a call to a customer at Access Gateway 2. The customer at Access Gateway 2 does not answer the call (i.e., a voice call is not setup between the customers). The customer at Access Gateway 2, then, enters an activation code for automatic callback at their CPE (e.g., *69 in many traditional SS7 networks). Access Gateway 2 signals the CCA with the user entered information and awaits further instructions. The CCA examines the user entered information and recognizes it as a service activation code, at which point the CCA signals the SA with the necessary information. When the SA receives the information, it identifies that the user has invoked Automatic Callback and signals the CCA with instructions for completing the transaction. In this case, the SA signals the CCA with instructions to poll the status of the last incoming calls line (the Customer at Access Gateway 1) and setup a call between the customers at Access Gateways 1 and 2 if possible. If the customer's line at Access Gateway 1 is not idle, the CCA should instruct the Access Gateway 2 to play an announcement notifying the customer that the call cannot be completed at this time and to try again later.

Services that require signaling to an external SS7 node may require the SA to formulate the TCAP and SCCP information (as well as perform the processing) associated with that

service. In these cases, the CCA "triggers" on user entered information and signals the SA for further processing, or the CCA receives an SS7 message (via a signaling gateway) or the CCA receives a message from another CCA which requires processing at the SA. In the latter case, the CCA could identify that further processing is required at the SA by information contained in the message. Once the SA receives the information from the CCA, it identifies the service that needs to be executed and performs the service logic related to that service. Depending on the service, the SA may need to signal the CCA with call processing instructions (e.g., checking line availability of a customer), and await a response from the CCA. Once the SA has executed the required service logic, it will formulate the SCCP and TCAP layers of an SS7 message, as well as provide routing information and send this message (via the CCA) out to the appropriate signaling gateway. If a response is required, the SA will receive the SS7 response message (via the Signaling Gateway and CCA), process the response, and signal the CCA with call processing instructions. One example service that could involve external SS7 signaling is a toll-free service call (e.g., dialed as 800) using an SS7 based toll-free database. In this example, a customer at Access Gateway 1 in Figure 5-8 dials an 800 number. The access gateway signals the CCA with the user entered information. The CCA "triggers" on the user entered information, recognizing service processing is required at the SA and signals the SA with the necessary information. The SA recognizes that the service that has been activated is the toll-free service and identifies that it needs to query an SS7 toll-free database in order to complete the service processing for this call. The SA determines the routing information necessary for delivering the message in the SS7 network (this could be done with the aid of the Routing and Translation Server), and formulates the SCCP and TCAP portions of the query message. The message is routed to the Signaling Gateway (via the CCA), where the MTP layer is added to the message and sent out to the SS7 network. Once the response message is received at the SG, it is sent to the SA through the CCA. The SA then uses the information contained in the response to obtain the routing number for the call. The SA then signals the CCA with call processing information that indicates the DN to be used for call setup.

5.4. Core Network Functional Requirements

Voice is a very distinct type of traffic. Voice connection does not require a lot of bandwidth, however it is very sensitive to delay and jitter. Core network should be designed with this traffic characteristic in mind. In this section some high level requirements associated with core network design will be addressed and open issues will be introduced. Packet networks were designed for multiple services, not just for voice. Voice will be incorporated as just one of the many services.

5.4.1. Internet Protocol Networks

IP networks gained universal recognition during the last decade. IP is simple and cheap. Up until very recently all the traffic on the Internet was a best-effort service. For voice, best effort service is not an acceptable alternative. The network has to provide at least some quality of service and traffic classification. For example packets carrying voice should be given higher priority than the ones carrying E-mail messages. Also for voice, a more advanced mechanism of transport is necessary. In this section QOS schemes available for IP networks are discussed, compared, and related to voice. Also transport protocol designed to carry multimedia traffic is introduced and compared to traditional transport protocol, TCP.

5.4.1.1. IP Quality of Service

Network services (such as ATM, Frame Relay, SMDS), that were designed from the beginning for the service provider environment, provide formally defined and enforced Quality of Service (QOS) mechanisms addressing such key performance issues as bandwidth, loss, delay and delay variability. In contrast, Internet technology has existed for two decades with (until very recently) only minimal emphasis on service quality issues – promising only a "best effort" service.

The recent surge of interest in finding workable solutions for providing QOS in IP networks is being driven by a number of factors. In this report we are only interested in factors associated with real-time applications, such as Voice Over IP (VOIP), with traffic characteristics and performance requirements dramatically different than traditional data applications.

Given the diverse set of applications that have already been targeted for IP network services, we can anticipate a diverse set of user requirements to emerge in this area. QOS mechanisms are designed with no specific application in mind. We describe these approaches generically and then point out how they are applicable to VOP. Voice is going to be transported over a packet data network, though it may not be the main emphasis in QOS mechanism design. At a minimum, QOS mechanisms must be able to provide:

- Service models, which provide an unambiguous way of describing an application's traffic characteristics and associated performance requirements
- The ability to support differentiated levels of service, allowing non-real time critical applications such as e-mail to receive lower priority than applications with more stringent delay requirements
- The ability to support real-time services, such as voice and video conferencing, with strict, quantifiable requirements for delay and delay variability
- The ability to request specific QOS treatment either via service provisioning or in real-time, using a signaling protocol
- The ability for VPN customers to receive a guaranteed, quantifiable, verifiable level of service as they would receive in a private network environment
- An approach that is scalable to national and international carrier deployment.

All routers in the core IP network should implement at least one of the standard QOS mechanisms.

5.4.1.2. Resource Reservation Protocol

The Integrated Services (intserv) Working Group of the IETF defines its charter as expanding the Internet service model to accommodate the transport of audio, video, real-time as well as "classical" data, thereby transforming the Internet into a robust, integrated-service communications infrastructure. The work of this group has focused on defining the services that must be provided, requirements for network elements to support these services, and the signaling used to request specific QOS treatment. Much of the

attention in this area has been focused on the Resource **Re**s**er**vation **P**rotocol (RSVP). RSVP is a signaling mechanism that allows an application to request specific QOS treatment from the network and for the network elements along the transmission path to reserve the resources needed to satisfy the QOS request (see Figure 5-9). Use of RSVP as the QOS mechanism for VOP is for further study.

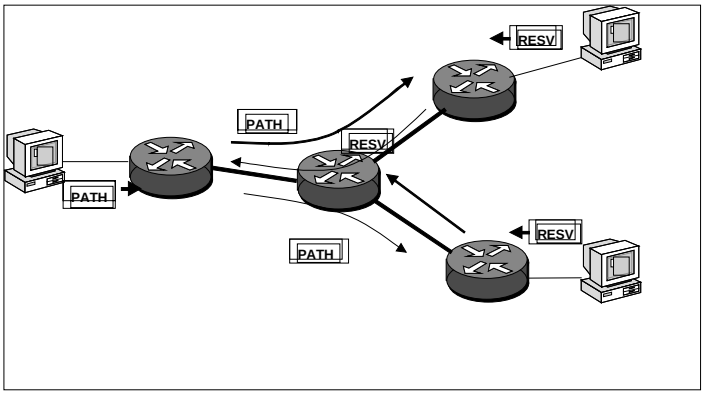

Figure 5-9 RSVP

The Integrated Services model includes the following three classes of service:

1. A **guaranteed service** for real-time applications requiring a bandwidth guarantee and upper bound on delay, with no loss due to queue overflows. It does not attempt to provide an explicit guarantee of delay variability or "jitter".
2. A **controlled load service** provides a service that emulates best effort service on a lightly loaded network. Thus, it is a "better than best effort" service, with low loss and delay, but without quantified guarantees. The service is aimed at "adaptive, real-time applications". These applications are known to perform well under lightly loaded conditions, but are highly sensitive to overload conditions.
3. A **best effort service**, similar to today's Internet service, with no guarantees.

Guaranteed Service is most appropriate to be used for VOP.

The operation of RSVP is illustrated in Figure 5-9 above. An RSVP-aware application communicates its QOS requirements to the host operating system via an API. This triggers the creation of a PATH message, which is sent from sender to receiver. The **PATH message** includes various information items, including the Sender Template, the Sender Tspec, and the Adspec. The Sender Template consists of a Filter Spec, which identifies the sender's flow. The Sender Tspec characterizes the traffic that will be sent. The Adspec is updated by intermediate routers along the flow's path to record resource information. For example, if the Adspec specifies a QOS service that is not supported by an intermediate router, this is flagged in the Adspec to inform the receiver.

As the PATH message travels from sender to receiver, resources along the path required to satisfy the application's QOS request have not yet been reserved. Instead, the resource reservation is requested by the receiver. If the receiver agrees to communicate with the sender, the receiver sends a **RESV message** upstream, along the same path traversed by

the PATH message. The RESV message includes a Flowspec, which includes a description of the flow requiring the reservation (Receiver TSpec) and the QOS service that is required (Receiver RSpec). As the intermediate routers receive the Flowspec, they reserve the resources needed for the reservation.

Some key characteristics of the RSVP process are as follows:

- QOS requirements are requested of the network by the application explicitly, in real-time. The network evaluates its current ability to provide the needed resources, notifying the application if it cannot satisfy the request.
- As the diagram indicates, RSVP reservations can be made for multi-cast communications. In fact, there are a number of design considerations for multicast (e.g., the ability to share reservations, merging upstream RESV messages) that make it efficient for this environment.
- Reservations are made for each application flow, identified by sending/receiving address, port, and protocol. The intermediate routers providing the resource reservation must track the reservations on a per-flow level of granularity[3]. In addition, the priority treatment given to non-"best effort" traffic is typically implemented through sophisticated queuing algorithms implemented on the router's links – another potential capacity bottleneck.
- Unlike ATM, where successful VCC setups reserve resources for the duration of the connection, the RSVP reservations must be refreshed periodically through the transmission of additional PATH messages. While this approach has additional overhead, it provides a mechanism for re-establishing resource reservations around link failures.
- Unlike ATM (with PNNI routing), where QOS capabilities are considered explicitly in the routing of a VCC, RSVP functions independently of the internal routing protocol (IGP). That is, RSVP attempts to satisfy the reservation request along the normal path determined by the IGP. The request may fail, even if sufficient resources are available on an alternate path.
- The successful use of RSVP as a mechanism to achieve explicit per-flow QOS guarantees still requires that the network is properly engineered – it is not a panacea. This is true of *all* QOS approaches.

5.4.1.3. Differentiated Services

It is worth noting that the early design work that went in to the development of RSVP can be traced back to the early 1990s – predating the explosion of the Web, the commercialization of voice on the 'net, and the current emphasis on *scalability* as a fundamental requirement for carrier-scale IP networks. Given the present business need to provide predictable service for commercial applications (VPNs, extranets) and to support voice and video, there is an urgent need for a scalable QOS approach for IP networks.

In 1997, various proposals were made within the IETF for such a coarse-grained approach that would allow the provision of one or more premium services that could be

[3] It has been estimated that each flow reservation requires roughly 1 kbyte of memory in each router along the path.

offered in a shared IP network environment without the need for detailed, per-flow state information/reservations in the core of the network. Examples of premium services that have been proposed and simulated so far include the following:

- An ***assured service***, which guarantees a user a specified amount of network bandwidth even in the face of network congestion
- A ***virtual leased line service***, which provides a low loss, low latency, low jitter, assured bandwidth end-to-end service.

It must be emphasized that the proposed implementations of these services do not require the detailed, per-flow resource reservations as would be done with RSVP. This suggests that it may be possible for service providers to offer such "better than best effort" services in a carrier-scale deployment. Although it is premature to conclude that this is feasible on a full production basis, the following is encouraging evidence that this may be possible:

- Recent simulation studies of the assured service by Bellcore suggested that such bandwidth guarantees can be provided on properly provisioned networks and were found to be robust to various traffic scenarios.
- Studies of the virtual leased line service by Van Jacobson at LBNL have yielded similar encouraging results. Furthermore, they report that such a virtual leased line service has been successfully prototyped (using Cisco 7000-series routers implementing weighted round-robin queuing) on the DOE ESNet.

Pursuing this opportunity to develop scalable, differentiated services via a coarse-grained approach, the IETF has recently chartered the Differentiated Services (diffserv) Working Group. The focus of this effort is to develop "relatively simple and coarse methods of providing differentiated classes of service for Internet traffic, to support various types of applications, and specific business requirements". Abandoning the fine-grained, per-flow resource assignment approach associated with RSVP, the Differentiated Services approach (see Figure 5-10) is described below.

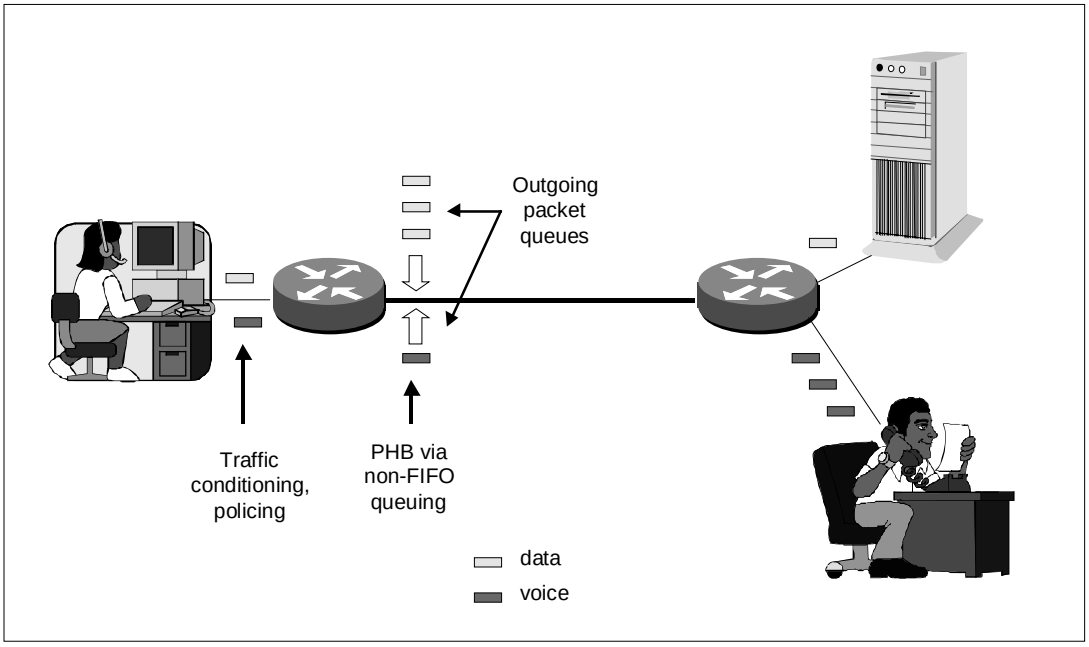

Figure 5-10 Diffserv

- A one-byte "DS byte" field within the IP packet header (the IPv4 TOS byte or the Traffic Class byte in IPv6) marks each packet to receive a particular forwarding treatment (referred to as **per-hop behavior** (PHB)) at each network router. The DS byte can be set by the user application or at the network ingress node, based on QOS policies negotiated with the customer.
- At the network ingress, traffic conditioning is performed. For example, applications requesting more than "best effort" service will typically have their data rates and burst sizes constrained; adherence to these constraints will be policed at the network ingress, with "out of profile" traffic marked (by downgrading the DS field) to receive only "best effort" service. By marking out-of-profile traffic as such and forwarding this traffic on a lower priority basis, congestion in the higher priority queues can be avoided.
- A small number of Per Hop Behaviors (PHBs) will be defined and used as building blocks from which a variety of Internet services can be defined. These PHBs are performance characteristics (such as expedited forwarding) that can be implemented in network routers via non-FIFO queuing and congestion control algorithms (e.g., Weighted Fair Queuing, Random Early Detection (RED), RIO).
- The specialized or differentiated treatment given to certain classes of traffic (as signaled via the DS byte) is obtained by applying the PHB processing to traffic aggregates (i.e., all packets with the same DS value), not to individual flows.
- The resulting services will have different performance characteristics appropriate for different types of traffic (voice, video, data), and can also be used to support multi-tiered pricing for premium versus "best effort" service.
- As in any QOS approach, the Service Provider is responsible for provisioning the network so that it is properly engineered. That is, the Service Provider maintains a

quantitative understanding of the subscribers' traffic characteristics and service requirements. The Service Provider provides sufficient network capacity such that, in conjunction with the PHBs implemented by the routers, the customers' requirements are met.

Use of diffserv as a QOS mechanism for VOP is a candidate for further study.

5.4.1.4. Diffserv and RSVP

It is important to note that, although the diffserv approach is fundamentally different (and more scalable) than that associated with RSVP, there are elements of RSVP that can be used in conjunction with diffserv. Specifically, RSVP includes a mechanism and API that allows an application to request specific QOS treatment in real time. Such a dynamic signaling mechanism is complementary to the static, provisioned approach described above. It can be used at the edge of a diffserv network to allow an application to dynamically request specific QOS treatment.

The combined use of diffserv and RSVP for VOP is for further study.

5.4.1.5. Real-time Transfer Protocol

Real-time Transfer Protocol (RTP) is a protocol designed to transfer multimedia traffic over the Internet. It provides necessary timing functionality, which IP lacks. Real-time Transfer Control Protocol (RTCP) is a companion protocol for controlling the RTP session. RTP provides for all the necessary timing and sequencing. Currently it seems like a natural choice for voice transport in IP networks. TCP may and already used for audio and video transport (e.g. Netscape). However there are some fundamental problems with TCP, which do not allow it to be used for this purpose. Three main problems are as follows:

1. TCP is a reliable protocol. Packets will be retransmitted if not properly received. This is not desirable for voice. In fact it will create distortion, echoing and other problems. That is why RTP uses UDP as its underlying protocol.
2. TCP cannot support multicast. Multicast support is a necessary attribute of VOP network
3. TCP congestion control is not suitable for voice. Once TCP detects congestion, it will decrease its window size. For time-sensitive application as voice it is not permissible since the receiver may suffer from starvation.

In addition TCP has a relatively large header and does not contain any timing information. RTP takes care of all of these problems. While it is not reliable, the room is left for this reliability to be added if necessary. RTCP can scale the session up to 2000 participants and provides intelligent bandwidth allocation depending on the age and participation of the party. Another useful feature of RTP is that it will work with IPv6 and ATM, specifically with ALL-2 and AAL-5.

5.4.2. ATM Networks

Asynchronous Transfer Mode (ATM) networks were designed to provide any service. There are numerous functions and layers associated with ATM. That allows *guaranteed* QOS, something that regular IP networks cannot provide. In this section some issues

related to voice over ATM are described. It is safe to assume that ATM network will support SVCs. An issue of ATM multicast is for further study and will be addressed in the upcoming GRs.

5.4.2.1. ATM Adaptation Layer

In order for ATM to support many kinds of services with different traffic characteristics and system requirements, it is necessary to adapt the different classes of applications to the ATM layer. This function is performed by the AAL, which is service-dependent.

AAL-1 will keep reserved bandwidth constantly. Voice is digitized using pulse code modulation (PCM) techniques, specified by ITU recommendation G.711. This type of traffic has burstiness equal to 1; it is therefore natural that AAL-1 was designed to carry CBR traffic. It provides clock synchronization, sequencing and forward error correction. While providing for a circuit switch like quality, AAL-1 has a serious drawback. It is expensive. Silent periods are transmitted with the same pick rates as active periods, and reserved bandwidth is almost never utilized to its full capacity. Transmitting voice with AAL-1 proves to be inefficient and most probably will not be adopted for VOP.

AAL-5 can be used for CBR and VBR traffic. Unlike AAL-1, AAL-5 will generate a cell to send only when there is enough data to fill 48-Byte payload. If there is not enough data, the cell will wait for it to send a cell or until a corresponding timer expires. AAL-5 is very well suited for signaling transport. Also the fact that AAL-5 does not introduce any additional per-cell overhead makes it attractive. AAL-5 becomes the default adaptation layer.

Another alternative is VBR traffic with AAL-2. Transmitting voice as VBR traffic requires that a different coding technique, adaptive differential PCM (ADPCM) is used, as specified in ITU Recommendation G.721. In CBR source, traffic is always generated transmitting active periods as well as silent periods, which is an inefficient way to use network resources. To achieve higher resource utilization speech activity detection may be used at the VBR voice source so that voice packets are generated only when the source is active thereby increasing the transmission efficiency. Transmitting cells generated only at active periods and using ADPCM coding a compression ratio of better than 4:1 can be achieved without noticeable degradation in voice quality. AAL-2 is a compromise between AAL-1 and AAL-5. In AAL-1 the cells are going to be transmitted independently of the presence of the data. In AAL-5 the cells are going to be transmitted only when there is enough data to fill them completely. With AAL-2 a cell is going to wait util it has 24 bytes of useful data and will be transmitted half filled if necessary. ATM forum (VTOA) is currently working on AAL-2 specification for narrowband services, and it is possible that VBR with AAL-2 will be a choice of VOP traffic. This issue requires further study and ATM Forum participation.

Because of the variety of services supported by core ATM networks AAL-1, AAL-2, and AAL-5 should be supported. The choice of QOS, bit rate and adaptation layer is for further study.

5.4.2.2. ATM Addressing

Currently there are two types of addresses, which are widely used on the ATM networks: E.164 and ATM End System Address (AESA). E.164 addresses are basically regular

public phone numbers. They are referred to as ATM public addresses. They are recognized by the ATM networks. Local Exchange Carriers (LECs) are responsible for the distribution of E.164 addresses and they are assigned according to the geographic location. The ATM Forum defined a private ATM address format. It is 20 bytes long. It is designed to encompass a number of different numbering plans and to allow internal administration and control of the addressing space. AESA currently has three different formats. One of them is E.164 AESA; it has public E.164 address embedded. This format is critical for the calls between regular phone and other devices over ATM networks. Core ATM networks designed for VOP should utilize E.164 AESA addresses, and all address translation should be done before the core network. In other words, the ingress switch should get E.164 AESA; none of the switches between ingress and egress should perform any address translation.

Another way to categorize the addressing space is by ownership. Any type of address can be split into service provider addresses and customer owned addresses. The idea is to be able to route based on the service provider addresses only. This reduces the number of entries in the public ATM switches routing tables. Once the call has been routed to a gateway or private network, the full address will be needed in order to route to the end station. This is called hierarchical routing. There is still an open issue on how many of the 20 bytes should be allocated for providers and customers.

5.4.2.3. ATM Internetworking

What happens when the call has to leave one network and go to another one? There are a number of issues associated with this. We are only going to introduce them briefly and mention the solution where appropriate.

Two ATM networks may not have identical classes of services. Therefore the call leaving one network and entering another network may undergo QOS negotiation. The usual procedure is to pick the closest service, which still complies with the desired QOS of the originating call.

An ATM network has to be able to negotiate QOS parameters with another network in general. However voice traffic, with very well known characteristics, should have a universal QOS for each bit rate and adaptation layer.

The issue is even more complicated with routing and signaling. There may be two cases: (1) a call going through transit network, and(2) not going through transit network. If the call does not go through a transit network, there is an interface between them. Choice of the protocol used on the interface will depend on the routing protocols, which the networks use themselves. If at least one of the networks uses PNNI, then the logical choice for the interface protocol is AINI. If both networks use B-ISUP, then the choice for the interface protocol is BICI. For transit internetworking configuration there are several possibilities depending on the protocols used by all three networks, PNNI peering and the transit network representation. This discussion is beyond the scope of this report and will be addressed in generic requirements.

Transit network should not disclose internal topology of communicating networks unless they are PNNI peers, in which case topology should be exchanged for proper routing.

5.4.2.4. IP over ATM

ATM is a backbone technology. However it is not universally accessible technology, unlike IP. Virtually every desktop computer now has IP protocol suite in its OS. Therefore it makes sense to take advantage of the IP accessibility and ATM services. This solution is called IP over ATM.

Fundamental problems, which should be resolved when doing IP over ATM, are as follows:

- Address Resolution
- IP multicasting
- Security.

All of these problems are candidates for further study.

There are several approaches to IP over ATM, in this section we are only interested in the following schemes, which perform transport exchange in the core network:

- Classical IP over ATM (CIOA)
- The IETF Multiprotocol Label Switching (MPLS)
- The ATM Forum's multiprotocol over ATM (MPOA).

Technique of IP over ATM is for further study and will be determined during GR process.

5.4.2.4.1. Classical IP over ATM

Refer to Figure 5-11 for easy follow up. In Classical IP over ATM, IP routers are attached to ATM backbone networks. Switches in the ATM network are treated as devices of IP sub-networks. Each sub-network has ARP server attached to it. IP hosts are not able to do address resolution directly, so the usage of these ARP servers is necessary. ARP servers contain mapping information between IP and ATM addresses. Through the established PVCs, an ARP request is sent from the IP host through ATM backbone to ARP server. The ARP response travels back, but instead of the MAC address; The IP host receives an ATM address. Having obtained ATM address, the host can initiate ATM call setup with the desired destination. In this approach, unless some IP QOS mechanism is used, ATM QOS is utilized.

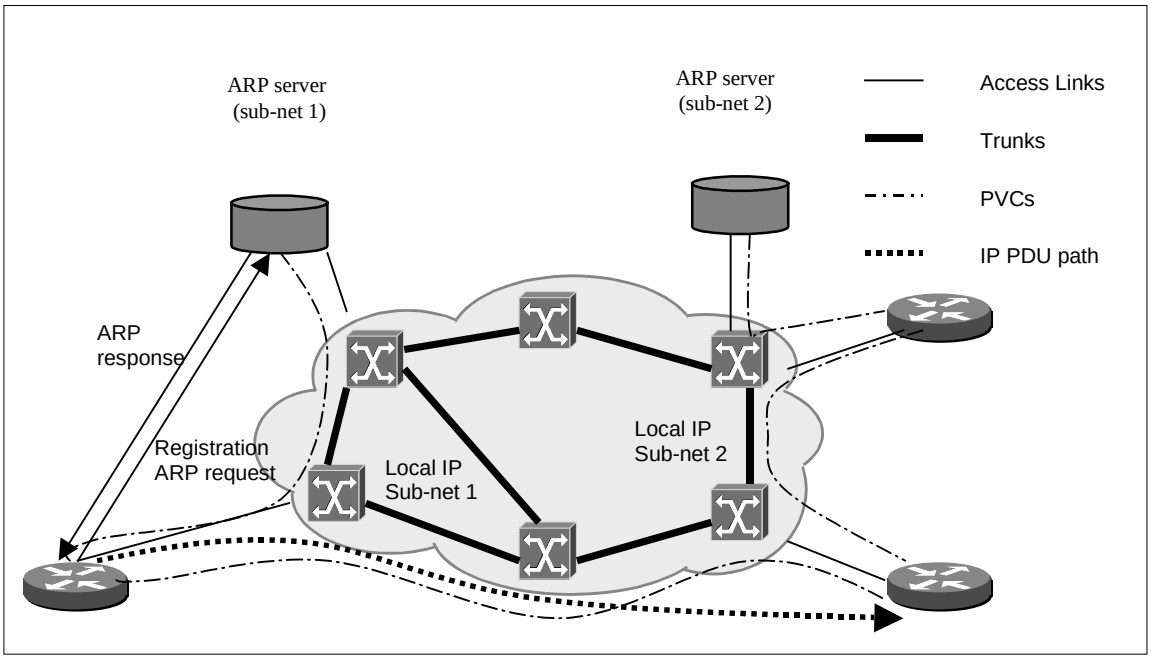

Figure 5-11 CIOA

To resolve multicast it is necessary to translate a class D IP address into a collection of ATM addresses. This functionality is provided by Multicast Address Resolution Server (MARS). Communication with MARS is done over Internet Group Multicast Protocol (IGMP). Multicast Servers (MCS) retransmit packets on point-to-multipoint, or multiple point-to-point VCs. MARS is connected to MCSs by point-to-multipoint connection.

CIOA has been proposed back in 1994. Since then superior methods of IP over ATM transport have been introduced (see Figure 5-11). In the next two sections, two new approaches, which take advantage of the underlying backbone, are described.

5.4.2.4.2. MPLS

In traditional IP routed networks, packets are forwarded toward their destinations on a store-and-forward basis. At each router, a routing table is consulted to determine the best next-hop for the packet. This is accomplished by searching the IP forwarding table for the most-specific (longest) address prefix that matches the packet's destination address. In addition, other layer 3 processing (such as address filtering for security purposes) may be performed.

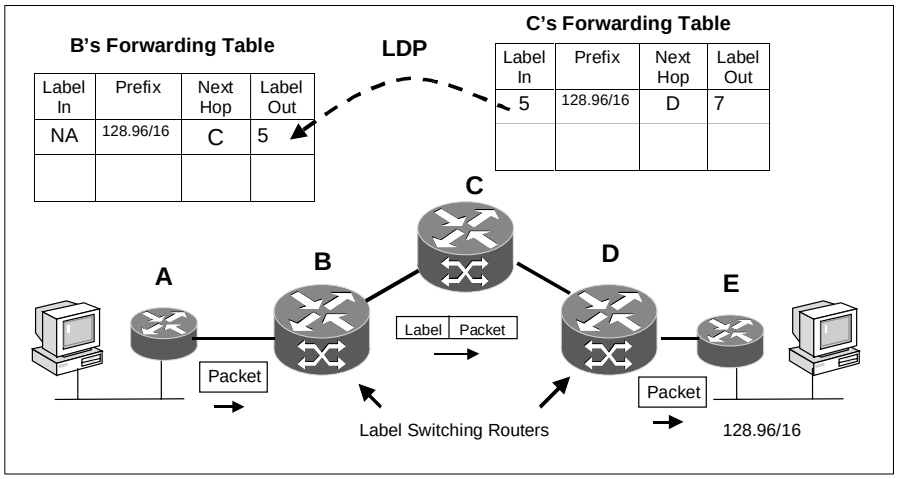

Figure 5-12 MPLS

An MPLS network consists of a network of Label Switching Routers (LSRs). The LSRs distribute destination-based routing information among themselves using standard IP routing protocols, such as OSPF or BGP-4. At the ingress to the MPLS network, the first LSR in the packet's path performs a longest prefix match on the destination address to determine its next hop and outgoing interface. Before forwarding the packet across the interface, the LSR attaches a short (20 bits), fixed length label to the packet. Subsequent LSRs along the packet's path make forwarding decisions by consulting a table that maps incoming labels to outgoing labels, rather than normal longest prefix match searching. Before transmitting the packet over the outgoing link, the incoming label is replaced with the outgoing label found in the table ("label swapping"). The associations between incoming and outgoing labels are communicated among the LSRs via a Label Distribution Protocol (LDP). In most cases, each LSR assigns incoming labels from a local pool of available labels, and receives outgoing labels from the "downstream" next hop router for the outgoing packet. The resulting Label Switched Path (LSP) through the MPLS network is typically the same path that is defined by the network's internal routing protocol (IGP). Consider the network shown in Figure 5-12 above. Router B (a LSR) has established a route to prefix 128.96/16 via the network's IGP, with Router C designated as the next hop. Being a LSR, Router A has to populate its Forwarding Information Base (FIB) prior to performing label switching of packets to 128.96/16. It requests an outgoing label for this prefix from Router C, which has already established an incoming label for this prefix. Because Router B is the first LSR in the path, it does not expect to receive labeled packets to this destination, hence does not require an incoming label. The creation or modification of a LSP is triggered by the network's routing protocol (e.g., OSPF) as IP forwarding tables are created and modified within routers. Thus, when a router creates an entry in its forwarding table, it must also create label bindings via LDP. Thus, the creation of LSPs is "topology driven", not "flow driven" as in certain other IP switching approaches (Ipsilon's IP switching, MPOA). It is generally acknowledged that this topology-driven approach is more robust and therefore preferable for carrier-scale implementations. When the packet reaches the egress LSR at the edge of the MPLS network, the label is stripped off and the standard IP packet is passed to the host or non-LSR router.

In practice, the Label Switching Router (LSR) is typically an enhanced ATM switch, though other transport technologies (SONET, Frame Relay) are also applicable. The label information is encoded in the VPI/VCI field of the ATM cell – so "label swapping" corresponds to the normal cell-relay forwarding technique used in ATM networks. The major difference with Label Switching across an ATM core is that the VCC carrying the IP packets from source to destination is established by the IP routing and LDP procedures, *not* by the normal ATM control plane. Because the LSR must run standard IP routing software as well as the LDP, a significant upgrade to the ATM switch's control software is required to turn it into a LSR.[4]

5.4.2.4.3. MPOA

MPOA is an alternative approach that has been defined by the ATM Forum for utilizing an ATM network to carry IP traffic (as well as other network layer protocols) efficiently. The main thrust of MPOA is to provide an architecture that extends the previously defined LAN Emulation (LANE) approach to carry IP traffic efficiently via a campus or wide-are ATM backbone, as well as providing interworking between ATM and non-ATM attached hosts. The efficient transport of IP traffic across an ATM backbone is accomplished by detecting traffic flows, and then establishing "cut through" ATM SVCs to forward IP packets across the network. Although significantly different in approach, it accomplishes a similar goal as MPLS, in that forwarding is accomplished via efficient ATM cell-relay/label-swapping, rather than by traditional IP forwarding.

In Figure 5-13, IP hosts (Host A and Host B) are attached to legacy LANs (Ethernet, Token Ring) separated by a wide area. In general, the two hosts belong to different subnets. At each location, an *edge device* (a router or LAN switch) on the local subnet is connected to the ATM WAN and assists local hosts in communicating across the ATM WAN via MPOA.

Assume that Host A wishes to communicate with Host B via a TCP connection. Initially, no ATM VCC has been pre-established across the ATM network to support such communications, so Edge Device A forwards the IP packets toward B using traditional IP forwarding. That is, the packets travel hop-by-hop through a sequence of connected routers, toward Host B.

[4] Cisco Systems' pre-standards version of MPLS, called "Tag Switching", has been implemented as an upgrade to their BPX multiservice ATM switch, as well as their LightStream1010 campus switch.

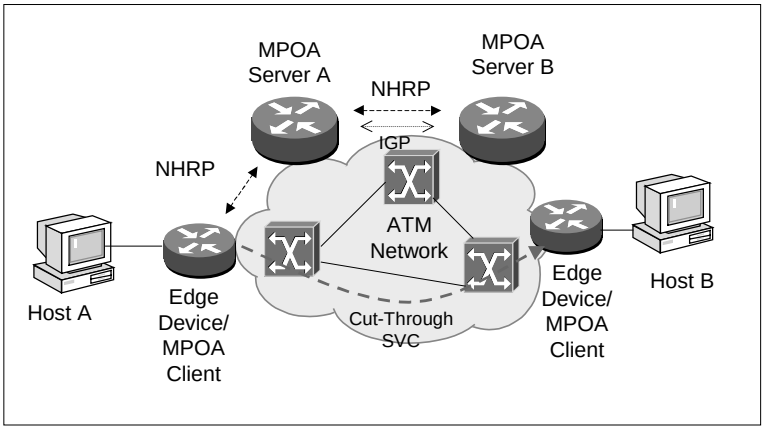

Figure 5-13 MPOA

After monitoring the flow of traffic from Host A to Host B and noticing that a relatively long flow may be in progress, Edge Device A decides improve the efficiency of data transfer by establishing a "short-cut SVC" through the ATM network. Unfortunately, Edge Device A only knows the IP address of the destination (Host B), not the appropriate egress point on the ATM network. That is, Edge Device A needs to resolve the IP address in an ARP-like manner. This is accomplished by querying location A's MPOA Server, which uses the Next Hop Resolution Protocol (NHRP) to obtain the target ATM address from MPOA Server B. Once the destination ATM address is obtained via NHRP, Edge Device A establishes a SVC to Edge Device B, forwarding all subsequent traffic (for this flow) through the ATM network without the further intervention of IP routers.

The following key characteristics of MPOA should be noted:

- Like MPLS, MPOA offloads (much of) the IP packet forwarding function from the IP routers, forwarding the traffic via the ATM switches via label-swapping/cell-relay.
- Unlike MPLS, where the Label Switched Paths (LSPs) are determined a priori (via the routing protocol), MPOA is a flow-driven architecture. That is, the detection of long-lived flows triggers the establishment (and subsequent teardown) of the forwarding paths (SVCs).
- Unlike MPLS, where the ATM switches are required to implement IP routing protocols, MPOA utilizes standard ATM control plane functionality.
- In the MPOA architecture, the role of the IP routers is diminished but is still required. They continue to run their normal routing protocols, which are still required to support their NHRP server function, as well as for default forwarding of IP packets.
- The fact that an ATM network is being used for transport is invisible to the legacy LAN-attached hosts, which require no change in communications protocol stacks or hardware.

5.5. Support for End User Services

5.5.1. Scope of VOP Network Services

VOP Network Services encompass traditional residence and business end user services such as Three Way Calling and Call Waiting as well as Calling Number associated services. However, VOP Network Services also include network based services for Centrex Users and ISDN Users. In addition, network services for PBXs in both conventional POTS and ISDN Primary Rate environments are to be supported. Intelligent Network based Services such as 800 service and virtual private networking also are within the scope of VOP Network Services. See Appendix A for a more complete list of traditional services and their definitions

The provision of such services in a conventional network applies not only to speech, but within ISDN to additional types of circuit switched calls (3.1kKz audio, 56kbps, 64kbps). In a VOP network that supports ISDN, VOP services shall apply to more than speech calls as well, since the “Voice” in Voice over Packet for Next Generation Networks encompasses these other types of circuit switched calls.

VOP Network services will be provided to users with conventional POTS and ISDN interfaces through the Access Gateway in conjunction with the Call Connection Agent and the Services Agent. The VOP conventional and ISDN services functionality must be partitioned among the Call Connection Agent, the Access Gateway and the Services Agent. To the extent a private network or AIN based service may require communication or control over a Trunk Gateway or an interface to an Intelligent Peripheral, those control and signaling elements also need to be identified and partitioned. A listing of some of these potential service components including ones common within call control is found in Appendix B.

These same VOP Network services will also need to be provided to users that have direct packet access to the VOP network through the Customer Gateway. Such users will need services that are available over conventional interfaces in addition to new Next Generation Network services that will evolve in the VOP network. New Next Generation services are beyond the initial scope of this SR. Whether the Customer gateway will require conventional service for other than speech type voice calls, and possibly analog modem calls, is to be determined.

5.5.2. Protocols for Network Service Control

Providing end users the ability to dial and control calls with services will be accomplished by signaling between the Service Agent, the Call Connection Agent and the Access Gateway. The MGCP protocol and extensions are being considered as a candidate for the protocol to support calls and services. The use of ISDN based DSS1 protocols such as Q.931, Q.932 and Q.921 are also being studied. When considering services for the Customer Gateway, ATM protocols based on DSS2 including UNI and PNNI are also being studied.

In addition, SS7 protocols such as TCAP and ISUP to support AIN type network services between the Service Agent and Network data bases for 800/888 services and Calling

Name type services are also planned. See section 5.2 and 5.4 for descriptions of the Service Agent and Trunk Signaling Gateway functionality.

The decisions and utilization of protocols for specific services will be addressed as part of the Generic Requirements work on the VOP Services Framework GR.

5.5.3. Documentation of VOP Network Services Functionality

A Framework GR for VOP Network services is planned to 1) document the philosophy of decomposition of conventional network services across the VOP network elements, 2) identify the common signaling protocols among network elements to allow for the provision of services to end users 3) serve as a common reference for subsequent GRs documenting the specifics of groups of network services and 4) serve as an updateable repository of all protocols used to support all VOP network services.

However, since most network services are call associated, the preparation of philosophy and protocols for services must be dependent upon and consistent with the approach for signaling for call set up and completion. Therefore, the work on VOP services must be delayed in time to allow progression of the work on call establishment.

Individual Service GRs would follow the guidelines set in the Framework GR to create consistent and coherent VOP service requirements. Following are examples of VOP Service GRs that may be prepared:

- Calling Number Identification Services
- Calling Name Services
- Call Waiting/Additional Call Offering Service
- Automatic Call Back
- Selective Call Screening Services
- Call Forwarding Services
- Multiline Hunt Group Services
- Three Way/Six Way/ Flexible Call Management
- Fundamental Basic Business Group Services
- Call Pick-Up Services
- 800/888 (Inwats and Outwats) Services
- Private Network Services
- Network Services for PBXs
- ADSI Services
- Voice Activated Dialing Service
- Voice Message Service.

5.6. End-to-End Performance Requirements in Packet Based Networks

This section presents the need for specifying End-to-End Performance Requirements for Packet based networks and in particular the Voice over Packet Network architecture proposed in this document. Section 5.6.1 presents the general considerations for performance in packet based networks like IP, ATM and IP over ATM carrying voice traffic. Section 5.6.1.1 discusses the importance of end-to-end performance in the VOP architecture by means of examples and brings out the various components that contribute

to performance degradation. Section 5.6.1.2 provides a framework to the end-to-end performance generic requirements. Sections 5.6.2 and 5.6.3 present the issues related to QOS and Reliability, respectively.

5.6.1. Performance Considerations for Voice Over Packet Networks

There are several candidates for transport technologies to be used in Next Generation Networks. The choice of technology is expected to be performance-driven, beside other factors. The following packet based technologies are expected to be the major candidates:

- Internet Protocol (IP)
- Asynchronous Transfer Mode (ATM)
- IP over ATM.

A comparison of these technologies is presented in Section 4.1.1. The following discussion is focussed on performance issues with these technologies.

IP and other network layer protocols, in their present form, provide a best-effort and yet unreliable, connection-less packet delivery service. Packets may be lost, duplicated, delayed, or delivered out of order. The service is connection-less because each packet is treated independently from all others. These could have different implications for different applications. Under consideration here is a special case of Voice traffic being carried by packets. The following packets are intended to play a two-fold role in the current VOP architecture:

- Signaling traffic transport
- User information/Data transport.

Signaling traffic refers to call processing message flows between the various elements/nodes of the VOP architecture. User information refers to the transfer of user data, in this special case, voice packets between the elements/nodes in the VOP architecture. The end-to-end requirements imposed by these two functions translate into corresponding end-to-end requirements at the network layer. For example, it is important to have comparable call setup and teardown times to meet the requirements for reasonable quality of service. This means that signaling messages have delay requirements. Therefore, packets carrying these signaling messages have corresponding delay requirements imposed on them. Similarly, voice connections have end-to-end delay, loss and jitter requirements, which translate into corresponding Packet-level requirements.

The first step then is to define appropriate Packet-level performance parameters that reflect the application level performance parameters. Application, in this context, refers to either the signaling or call processing layer or the user data/information layer. The IETF and standards bodies like the T1A1.3 subcommittee are in the process of defining IP performance parameters ([1] - [6]). The second step would be to specify objectives for these parameters for each type of application supported by the Packet transport service. This would involve deriving mapping between the performance parameters at the application layer and the Network/Packet layer performance parameters. The derived mapping can then be used to calculate objectives/requirements for the end-to-end packet performance parameters. For ATM, such performance parameters have already been defined in [7]. Quality of service classes have been defined such that each of the classes has the capability to support at least one application, for example, voice, video, data etc.

These QOS classes are specified by setting numerical objectives to each of the performance parameters relevant to the application traffic supported by the service class.

The general performance parameters for data and signaling transport are as follows:
- Delay
- Latency
- Loss Ratio
- Delay Variation.

Delay, Loss Ratio and Delay Variation are typically specified for data transport and especially in case of voice. Signaling transport is primarily concerned with delay, which translates into Latency, and Loss Ratio. We will discuss the importance of these performance parameters specifically with relevance to the VOP architecture and end-to-end QOS in the following section. One other performance parameter, which needs attention and will be discussed in the next section in detail, is "Availability or Blocking Ratio".

5.6.1.1. VOP Architecture Specific End-to-End Performance Considerations

It is imperative to examine the end-to-end network layer requirements in the light of the specific architecture proposed in Section 4.2. It is necessary to focus on the performance impacts of the proposed architecture on the underlying transport network and specify network level/packet level requirements that cater to the specific requirements of signaling protocols outlined in Section 4. Performance requirements for each of the network elements (Call control agent, Trunk Gateway, Access Gateway etc.) are also important for the architecture to be successfully implemented.

Acceptable end-to-end performance is important for the success of the VOP services because the users are ultimately affected by end-to-end performance. Therefore, it is necessary that the desired end-to-end performance is achieved for all types of VOP service. A good starting point for analyzing the performance issues in the VOP network is to examine the various services offered and the types of calls supported by the network. From section 3.1.3, the following calls are to be supported:

- VOP network subscriber-to-VOP network subscriber
- VOP network subscriber-to-PSTN/ISDN subscriber (and *vice versa*)
- PSTN/ISDN subscriber-to-PSTN/ISDN subscriber, via VOP network.

This is one broad classification of calls from a performance perspective. The interface to a subscriber may or may not be packet-based. Before voice is packetized, it is transported to the gateway that performs packetization. This may be at the customer premises in some cases or at some point in the network in other cases. Under such varying scenarios, the voice call may experience different performance degradation. It is necessary to consider the types of access networks and the elements in these access networks in order to assess its performance impacts. The types of calls that can be established include the following:
- Voice calls
- Circuit switched data calls (perhaps via circuit emulation)
- Packet switched calls.

The performance requirements for each of these types of calls needs to be carefully specified in order to provide acceptable service.

The VOP network supports analog line terminations, ISDN line terminations and other types of packet based access like ADSL and IP phones. It supports voice calls between subscribers that have such a variety of interfaces. As an example, we may consider a voice call made from a simple analog telephone set to a subscriber with an IP phone. For simplicity, it is assumed that the VOP network serves both the subscribers. Figure 5-14 presents the overall network diagram. The various network segments and network nodes that contribute to performance degradations is then listed.

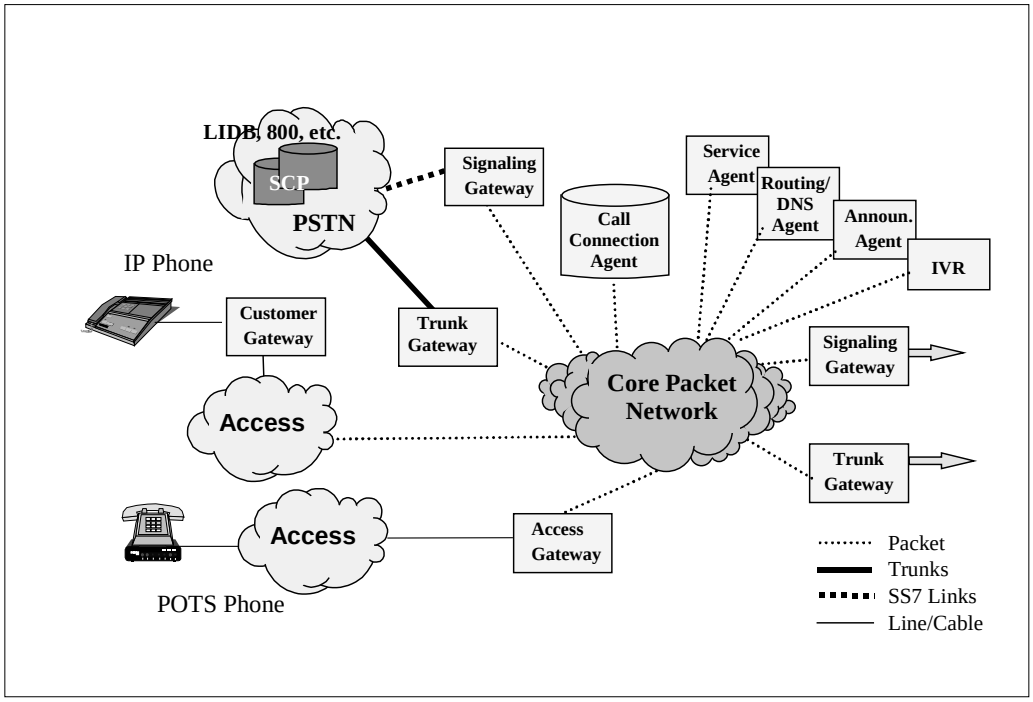

Figure 5-14 Example Call in the VOP Network

The Access Gateway provides the dial tone and performs the function of collecting digits etc. Once all the information required to establish the call is obtained at the gateway, it communicates with the Call Connection Agent to establish communication with the IP phone connected to the Customer Gateway in some other part of the VOP network. For simplicity again, we may assume that the Customer Gateway shown is the gateway to which the IP Phone is connected. In reality, the customer gateway could be connected to one of the following access clouds off of a different core network.

- The subscriber using the analog POTS phone goes off-hook to make a call.
- After collecting the information necessary to set up the call, the Access Gateway communicates with the Call Connection Agent to establish the call.

- The Call Connection Agent communicates with the Customer Gateway connected to the IP phone to request a connection with the Analog phone connected to the Access Gateway.
- A communication channel is established between the Analog phone and IP phone through the Customer Gateway and the Access Gateway respectively.
- Voice is packetized at the Access Gateway and transported over this communication channel to the IP phone through the Customer Gateway. Voice packets are then de-packetized.
- One of the parties involved in the connection indicate a call termination (on-hook) to their respective gateways.
- The Gateway requests that the connection be terminated to the Call Connection agent and a series of events similar to call setup is performed in order to terminate the call.

During both Call Setup and Tear-down, messages are sent back and forth between the Gateways and the Call Connection Agent. These messages have certain delay constraints. A very long call set up time, beyond a certain limit, may not be acceptable. We assume here that the Call does not need to cross an administrative domain and hence only one Call Connection Agent is involved. The following elements contribute to the performance of this call:

- The Core Network
- The Access Network to which the IP phone is connected.
- The Access Gateway, Customer Gateway and the Call Connection Agent depending on their individual capacities and load.
- The type of Voice encoders used in the Gateways and the IP phone.

The above listed elements contribute in various ways towards the End-to-End Performance parameters for this example call.

- Core Network – Contributes to Throughput, Delay, Loss and Delay Variation.
- Access Network – Also contributes to Throughput, Delay and Delay Variation.
- Gateways – Contribute to Throughput, Delay, Loss and Latency.

  Delays within the gateways include the following:

  – Algorithmic delay: Example, G.711 has no compression so there is no algorithmic delay. G.729 on the other hand encodes a 10 ms compression frame before it can present it for packetization. In addition, on the decode side, the G.729 algorithm requires that the decode DSP maintain a 5 ms look-ahead buffer.

  – Packetization delay: The number of samples collected and placed in a packet is somewhat arbitrary for G.711. For G.729, the minimum potential payload is the size of a compression frame.

  – Processing and queuing delays within the gateway

  – Delay Variation or Jitter in gateways - A jitter buffer is maintained in the receive gateway to take into account delay variations across the network.
- Call Agent – Contributes to Latency. This directly reflects in call setup and tear down time.

- Voice encoders – Contribute to Delay. Although these are part of gateways, it is listed separately since they can have a significant impact on Delay Performance apart from the Delay contributed by the gateways due to other factors.

The above example assumed that the VOP network served both the subscribers. In cases where either or both subscribers are served by the PSTN the call setup and the information transfer phase of the voice call will experience performance degradations due to other elements like the Signaling Gateway, the Trunk Gateway and the PSTN network etc. Also, if the Voice call traversed multiple administrative domains, more than one Call Agent will have to be involved. This is another factor that needs to be incorporated into a Call reference Model used to assess end-to-end performance. Several Call Reference Models need to be built to account for all possible types of calls and any performance impacts these models have on the Network. Therefore, in arriving at the performance requirements for each of the network elements and network portions, it is necessary to take into account the various types of calls that may need to be established. These Call Reference Models can then be used to apportion the end-to-end performance requirements to each element (Network Node or Network Segment) in the Call reference Models.

5.6.1.2. Framework for End-to-End Performance Requirements

The end-to-end VOP network performance considerations are influenced by the following three main factors:

1. Performance requirements for each of the VOP network elements (Call control agent, Trunk Gateway, Access Gateway, Customer Gateway, etc.)
2. Performance requirements for the transport network
3. End-to-end connection/call types.

Based on the proposed architecture of the VOP network, a brief framework for End-to-End Performance Requirements/specifications is presented here. The following is a set of issues that the suite of performance requirements needs to deal with:

- Call Reference Models for various types of calls supported by the VOP Network
- Network Segment Performance – The Performance requirements for various network segments in the Call reference Models, e.g., the Core Network
- Network Node Performance – The Performance Requirements for the following Network Nodes:
  - Call Connection Agent
  - Access gateway
  - Customer Gateway
  - Signaling Gateway
  - Trunk Gateway
  - Service Agent.

Requirements need to be specified for the following performance parameters for each of the above Network Elements (Gateways, Call Control Agent, Core Network etc.):

- Delay
- Latency
- Delay Variation

- Loss Ratio
- Availability.

The goal of this suite of Performance requirements is to provide acceptable end-to-end performance to the customers of the VOP Network by specifying the individual performance contributions of each of its elements.

5.6.1.3. Latency and Delay Requirements

Call processing/signaling messages are to be transported back and forth between various nodes in the VOP architecture. These messages are encapsulated in packets and transported over the underlying network. Call processing is delay and loss sensitive. Also, the Call processing state machine or the call model, which is responsible for call setup, management and teardown is sensitive to both message delay and loss. The delay sensitivity arises from the user perception of call setup and call teardown times. The loss sensitivity is attributed to the increased latency resulting from the need to retransmit lost signaling messages. An in depth analysis of the dependence of the call flow model parameters/timers on the packet performance parameters is needed in order to specify the requirements on packet performance parameters relevant to signaling transport.

Latency control is also important for audio/voice data. It is more important than loss control. For voice encoding, loss of data packets results in either small noise glitches or periods of silence. Delay can have two effects on voice performance. First, it increases the subjective effect of any echo impairment. Second, even when echo is controlled, delays above 300ms round trip can interfere with the dynamics of voice conversation, depending upon the type of conversation and degree of interaction. ITU-T Recommendations G.114, G.131 and G.173 (Annex A) give additional information regarding effects of delay and echo. Therefore, for a voice connection, where end-to-end delays as short as possible must be maintained, it may be necessary to declare a “very late” voice packet as lost in order to achieve acceptable delay. The tradeoff between long delay (which may result in higher speech transmission quality, but will increase the difficulty of conversation) and dropped packets (which will result in lower speech transmission quality, but will ease the ability to have an interactive conversation) must be given careful consideration when designing VOP services.

The concept of delay variation tolerance is sometimes useful to introduce in this context. In simple words, delay variation tolerance specifies the maximum and minimum delay or the delay window of a packet that can be tolerated on a voice connection in order to achieve a desired level of speech transmission quality.

The impact of such performance parameters on the relevant network segments and network elements in the VOP architecture need to be examined. It may be required to specify allocations of the performance objectives to the various network segments and network elements/nodes. In the special case of Packet delay, the apportionment of delay in the core network, in the access network and in the network nodes (e.g., Gateways) is important in order to insure that all network segments and elements have a fair burden of the end-to-end Packet delay requirement. Similar details apply to other performance parameters like Packet loss, etc.

5.6.1.4. Loss Ratio Requirements

In simple terms, Loss Ratio is the ratio of the total number of lost packets to the total number of packets sent over a connection or virtual circuit between two peer network layers. Loss occurs in a network due to various reasons including limited physical resources (buffers) and network congestion. Different applications have different loss sensitivity. A voice circuit/connection can afford to experience loss of voice samples to a certain extent. Therefore, the transport of voice using packets places demands on the end-to-end packet loss ratio. It is essential to specify requirements on the acceptable end-to-end packet loss ratio for VOP calls. Since the Access Gateway, Trunk Gateway and the Customer Gateway can potentially contribute to this Loss Ratio, it is necessary to specify loss requirements for each of these gateways. The contribution of the Core Network to the Loss Ratio can be significant and needs to be specified. Similarly, each network involved in completing the voice call has to be allocated a portion of the end-to-end loss ratio contribution.

5.6.1.5. Availability Requirements

As mentioned in the previous sub-section, “Availability or Blocking Ratio” is also a performance parameter that needs to be specified for a network service. The performance of the network is also judged on its availability at any given time or over a period of time. A clear definition of this parameter and a numerical objective for this parameter needs to be specified for the VOP network services. A definition similar to that for “Blocking Ratio” for telephone trunks may be a starting point for defining this parameter and to set numerical objectives.

5.6.2. Quality of Service

Quality of service provides a competitive mechanism to provide a more distinguished service. It is a mechanism used to treat traffic preferentially. In the present scenario we have primarily two types of traffic flowing through the network: signaling traffic and user information/data traffic. It is essential to provide mechanisms in the network to be able to distinguish between these two types of traffic and treat them differently. Typically, the volume of user data traffic far exceeds the volume of signaling traffic in a network. Signaling traffic can experience congestion due to a high load of user data traffic. This could result in increased latency for the signaling messages. Signaling messages need to be given priority over data traffic or need to be provided with separate channels that do not compete with data traffic. Some types of calls may be given precedence with respect to others. This may be called Feature related QOS. For example, an E 911 call may need to be processed with higher priority than other calls and may need to have better voice quality than other calls. Either the Gateways or the Call Connection Agent may indicate/modify the QOS for such calls. QOS may also be required to treat, for example, voice calls separately from voice band data calls. In order to accommodate the above service differences, it is necessary to do the following:

- Define a set of service classes (QOS classes) based on application performance requirements or service requirements.
- Set objectives for the Packet performance parameters relevant to each service class. This may result in requirements on both Gateways, Call Connection Agent and the Network segments in order to achieve the desired overall performance.

In the circuit-switched world of telephony, methodologies are in place for echo, loss and noise Grade of Service (GOS). These methodologies allow prediction of changes in engineering on user perception of quality. It is necessary, therefore, to develop similar mappings between user perception of quality and the Quality of Service (QOS) offered by the network in terms of the end-to-end network performance parameters. Results from subjective testing experiments conducted to derive the above mapping could be used to develop such methodologies.

5.6.3. Reliability

This sub-section addresses the need for reliability requirements for each element of the VOP architecture as well as the VOP network as a whole. A common aspect of reliability for an individual element of a network is its availability. The availability of a system is the probability that the system performs a required function at a given instant of time. Unavailability (i.e., the complement of availability) is commonly expressed as the long-term fraction of time that the system fails to perform as intended. In many applications, unavailability is expressed as cumulative downtime per year, which is the long-term average amount of time (e.g., minutes) during a year that a system is unable to provide service. Unavailability can also be weighted, typically (though not exclusively) by the number of customers affected by the loss of service. In this way, reliability models may include the effects of service demands that vary by time-of-day or by geographical location.

Since a network failure rarely results in a total loss of service by the network, an aspect of reliability of particular import to networks is survivability, which quantifies the performance capabilities of a network under network failure conditions. Measures of impact of service loss on customers may be developed based on failure attributes such as duration and number of customers affected.

A comprehensive reliability model needs to be developed specifically for each of the functional elements in the VOP architecture. Based on this model and reliability requirements for the element, reliability requirements for various components of the element may be specified. While reliability requirements on individual elements go a long way to managing overall network reliability, separate reliability requirements for network segments and the network as a whole must also be established. Network reliability requirements may be based on failure frequency, measurable impact attributes, or an index calculated from various impact measures. Reliability requirements may establish thresholds for various measures of service loss in order to define when failures are serious enough to be counted as a service outage.

Reliability requirements should consider carefully the various failure modes to be encompassed. The decision of which failure modes to include may depend on perceptions of potential customer expectations for reliability. If it is expected that customers will use the VOP network as a replacement for existing wireline voice networks, it is probable that customers will expect reliability comparable to that delivered currently by the wireline networks. However, if the VOP network delivers price or service advantages beyond those of existing wireline networks, customers may be willing to relax their reliability expectations to obtain those advantages. For example, it is important to emphasize that the reliability objectives of existing voice networks are intended to include network reliability during natural disasters such as earthquakes or hurricanes. Designers of the VOP networks must decide whether the VOP network will

be designed to achieve this level of reliability or whether its customers will not expect this level of reliability. If this level of reliability is to be delivered, models for the frequency and impact of such events on the VOP network should be developed. In addition, reliability analyses should incorporate repair and maintenance models to represent the mitigating effects of best practices and proper network support.

Additional element reliability may be achieved through the introduction of redundancy to the VOP network. Redundancy is of particular value for elements with a central position in the VOP architecture. The element at the heart of the VOP architecture is the Core Network. This element is too large to be duplicated for the purposes of reliability. However, its reliability is augmented by its robustness through the creation of a high density path structure within the Core Network.

Of greater concern is the Service Agent. Only one Service Agent exists for the entire VOP network. Its functional elimination or isolation would make vertical services such as 800 and LIDB unavailable throughout the VOP network. For this reason, the Service Agent is a prime candidate for paired duplex systems capable of assuming the roles of one or the other if one system is not capable of fulfilling its function.

Each VOP network may have multiple Billing Agents. In any case (although with differing consequences), the effects of failure of one or multiple Billing Agents should be modeled.

The VOP network also has multiple Call Connection Agents. However, in this case, it is clearly planned that specific gateways (Access Gateways, Customer Gateways, Signaling Gateways, and Trunk Gateways) are associated with each Call Connection Agent. The failure of a CCA would not bring down the VOP network but could impose total loss of service to a substantial fraction of the customer base. Modeling the reliability of this element is of great importance in establishing reliability requirements. It is also crucial to traffic engineering for establishing the number of Call Connection Agents in the VOP network. For example, reliability considerations may require more Call Connection Agents than their traffic capacity constrains.

Because of their position at the lowest level of the VOP architecture hierarchy, the various gateways (Access Gateways, Customer Gateways, Signaling Gateways, and Trunk Gateways) have the least import in reliability requirements with respect to survivability of the network for a single failure. However, because of their multiplicity throughout the VOP network, frequent (though less critical) failures can still produce customer perception of unreliable service. For this reason, it is no less important to model their characteristics and modes of failure as input into the analysis of reliability requirements.

Separate reliability models should be constructed for hardware and software components of each element. The models for failure of hardware element components may be based on estimates provided by Bellcore's Reliability Prediction Procedure (RPP). The increasing dominance of modes of failure beyond physical failure of hardware components requires the consideration of additional models for failure.

Of particular concern is the effect of human interaction on reliability of individual systems and the network as a whole. Recent studies indicate that failures resulting from procedural errors in existing voice networks are increasing. The rapid roll-out of new

technologies and services to meet customer needs constantly introduces new equipment and processes into developing networks. The new equipment and the processes needed to manage them demand the consideration of a learning curve as technicians learn correct operations. New architectures such as the VOP network are particularly susceptible to this reliability problem. Consequently, reliability models for the VOP elements must capture the frequency and impact of procedural errors in their estimates.

Of course, failures may result from intentional as well as unintentional human interactions with network elements. Failure modes should also include the effects of sabotage and vandalism on network elements. Robustness in network design may reduce the impacts of such failures as well as their frequency.

Besides the reliability of individual elements, failures may result from interoperability design errors between network elements. Even when standards are established, equipment suppliers to the VOP network may have incomplete or incompatible interpretations. This problem is exacerbated by the likelihood that equipment from multiple vendors will be needed to make the VOP architecture a reality. Interoperability testing will eliminate most of these errors but it is likely that some will remain especially in the early stages of the network's existence. Models for such errors should be developed and allowance for early reliability problems should be considered in the implementation phase of the VOP network life cycle.

Proper functioning of any telephony network places a heavy responsibility upon the software controlling its network elements. Over the years, this has become increasingly true of wireline networks and can only be even greater in a VOP network. Consider that in a wireline network, no software involvement is necessary to support most calls between the completion of call setup and the initiation of call release. However, a VOP network must provide software support to every call throughout the duration of the call. Software must control the correct creation, routing, delivery, and sequencing of each voice quantum packetized. Software reliability prediction models should be developed to predict failure rates from design and implementation faults in software. The substantially greater reliance on software makes the VOP network especially susceptible to failures resulting from computer viruses; such a virus could have a potentially devastating effect on the VOP network through its widespread dissemination via the network itself. Reliability analyses would need to model such a virus and its effect in order to understand potential impacts on requirements.

The packetization of voice provides new failure modes from the customer's perspective. In wireline voice telephony, outside of transmission quality, there is little that can go wrong from the customer's viewpoint once the call is setup. Packetization creates a host of new possibilities. Packets can be misrouted or lost creating gaps in speech. Packets may be placed out of sequence creating confused speech or conversation without logical flow. The most likely problem would be delay of packets which could make conversation unacceptably painful. Such delay occurs when a portion of the network is overloaded by traffic. Assuming proper traffic engineering has been performed, such overloads have the greatest likelihood of occurrence when a portion of the network has failed. Thus, VOP networks are susceptible to a type of reliability service loss not seen in wireline voice networks. Reliability requirements must establish thresholds for delay and loss of speech packets to identify when service quality is sufficiently poor that service may be considered lost from the customer's perspective. Reliability models for the

frequency and impact of failures of network elements must be created to encompass these effects.

5.6.4. Performance Aspects of Coders and Decoders

Transmission in Packet networks is characterized by periods of relatively error-free transmission, punctuated by occasional bursts of lost frames. These lost frames occur when packets are lost in transit or are discarded due to late arrival as part of a delay management strategy at the destination. Thus, speech coders for VOP applications must be evaluated in terms of their performance when multiple sequential frames are lost or discarded. Some VOP applications are also likely to encounter high ambient acoustic noise at the sending end of the connection (e.g., when one of the end points is a personal computer). Hence, it is desirable that the speech coder shows robustness in the presence of acoustic background noise. The performance effect caused by lost or missing packets at the destination, and the associated effects on low bit rate speech coders, is of particular concern. In many applications, it will be necessary to include multiple frames of coded speech in a single packet. Thus, speech coders for VOP applications should be robust with respect to loss of multiple sequential frames. ITU-T Recommendation G.700-series codecs have been shown to have good quality and to be robust in their performance under wide range of conditions. The use of speech coders that are already in wide use in digital wireless systems may be considered for use in VOP systems. While the transmission characteristics of wireless channels and those of Packet-based systems may differ, speech coders for wireless applications are designed to be robust with respect to coded frames that have been corrupted and declared unusable. Hence, they exhibit properties that are desirable in a speech coder for VOP applications.

The contribution to one way delay of certain ITU-T G.700 series voice codecs are provided in Table 5-3. This gives an idea about the impact of the codecs on end-to-end delay performance.

Table 5-3 Delay Contribution of ITU-T G.700 Series Speech Codec to One Way Delay

Speech Codec	Contribution to One way delay in (ms)	Bit Rate (Kbits/s)
G.726	0.25	32
G.728	2	16
G.729	35	8
G.723	97.5	6.3

In some calling scenarios, the speech signal will be subjected to encodings by more than one speech codec. The transmission path may traverse two gateways. Hence, speech will be encoded and decoded two times by the speech codec. In these cases, the ability of the VOP codec to function well in tandem with the other codec must be given proper consideration.

5.7. Billing Usage Measurements Requirements

The term *billing usage measurements* refers to information that is collected in association with the use of network capabilities and/or services. This information is initially captured in *raw* form in the network (i.e., in direct association with the actual usage) for subsequent processing for customer billing and perhaps other corporate uses (e.g., fraud detection).

This section describes high-level functional requirements necessary for capturing and processing billing usage measurements in the VOP architecture.

5.7.1. Overview

The following premises are assumed with regard to the high-level functional requirements related to billing usage measurements:

- The goal of the required functionality is to capture and process billing usage measurements in the VOP environment in a manner equivalent to the billing usage measurements functionality in place in the traditional Public Switched Telephone Network (PSTN) environment. Although the underlying architectures of these environments are fundamentally different, the types of services offered to (and used by) customers are assumed to be equivalent. Hence, the associated usage measurements needed to account (i.e., bill) for use of the services should also be equivalent.
- A service provider will likely want to use an existing billing system to process the billing usage measurements produced in the VOP network, rather than deploying completely new applications. Producing billing usage measurements similar in format and content (to the extent practical) to the measurements processed today by billing applications would minimize modifications to these systems.
- Given these premises, existing standard formats (e.g., Bellcore AMA Format [BAF]) are assumed to have the capability to accommodate the new environment, perhaps with modifications.
- Generation, formatting and outputting of billing usage measurements for use in downstream processing is assumed to be performed by the combination of the CCA and the BA.

Despite the commonality between architectures with regard to billing usage measurements, certain challenges are inherent in paralleling the PSTN usage measurement functionality in Next Generation Networks. These challenges primarily stem from the distributed nature of network functionality, in contrast to the traditional PSTN environment in which, as a rule, a single element (i.e., the switching system) has the capability to collect, format and transmit the required usage information.

5.7.2. Billing Usage Measurements Architecture

Figure 5-15 depicts key elements in the VOP network that affect the billing usage measurements process. In comparison to the PSTN model, in which the switching system is generally responsible for generating, assembling and formatting usage measurements, the VOP billing usage measurements architecture is more distributed (i.e., more elements are involved in the process) and thus more complex. In the VOP

architecture, "raw" billing usage measurements are generated by the CCA and transferred to the BA. Communication between the CCA and BA can occur over the Core Packet Network. After receiving the raw usage measurements from the CCA, the BA performs the processing needed to create a formatted record that can be subsequently transmitted to the downstream corporate billing system (and/or other applications) for processing.

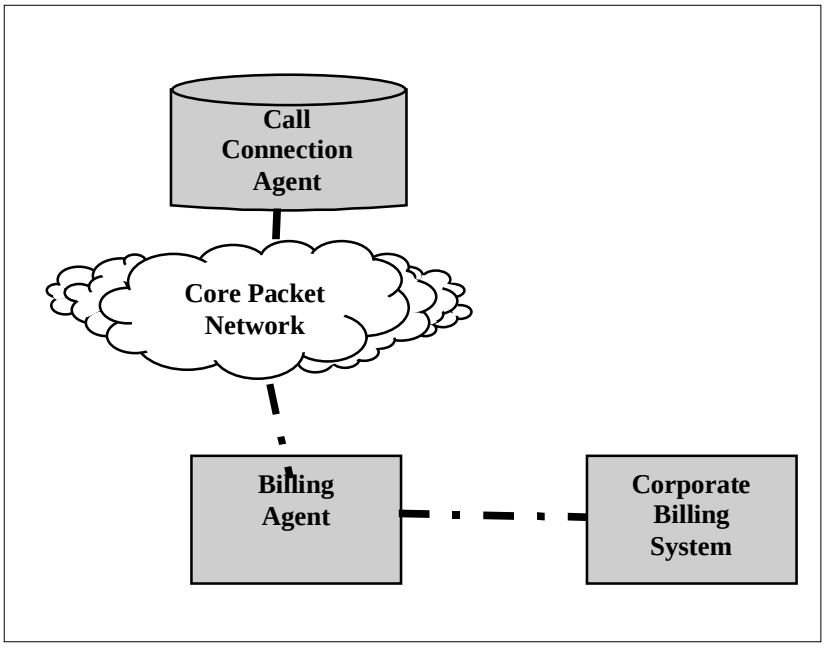

Figure 5-15 VOP Billing Usage Measurements Architecture

This architecture will accommodate billing usage measurement functionality for initial VOP implementations. Future capabilities are expected to be introduced which will build upon this architecture to provide additional services and features not available in initial implementations (e.g., interactive billing, direct communication between the BA and VOP Gateways). Section 7 of this Special Report describes potential future capabilities such as these that can be added to the initial VOP implementations.

5.7.3. Billing Usage Measurements Core Functionality

This section describes the fundamental processes in the CCA that are involved with billing usage measurements.

5.7.3.1. Accounting Administration

Accounting administration is a process through which the administrator provisions information used by the CCA to manage accounting. Based on provisioned information, the CCA determines under what conditions it is to capture billing usage measurements. In the CCA, this process is used to establish the following information:

- If usage is to be recorded for a particular service (e.g., vs. flat rate billing)

- If usage for a given service might be recorded for a particular customer or set of customers (e.g., for local measured service)
- If usage is to be recorded for conditions other than completed, billable events (e.g., attempts).

Accounting administration in the CCA also encompasses determining and recording the type of event with which the usage is associated [5]. This process also entails determining other information needed to manage communication between the CCA and BA (e.g., how often usage information is transmitted to the BA, time-out lengths for individual events).

5.7.3.2. Usage Measurement Recording Decision-Making

Usage measurement recording decision making entails the CCA's determination of applicable recording logic based on the specific network and customer configuration in effect when service or feature usage is taking place. Included in this process is the CCA's determination of what service or feature was invoked (e.g., a toll-free service, based on an 800 or 888 prefix being dialed). Based on this determination, the function then determines whether or not usage is to be recorded. Based on this decision, and if a recording is to be made, the CCA can then determine what information needs to be captured and in what format (e.g., detail vs. aggregate). In addition to determining the nature of the recordings, this process also determines how many recordings will be needed for a given event (e.g., one for a call and one for a feature that was invoked, such as call forwarding).

5.7.3.3. Usage Measurements Recording

Usage measurements recording performed by the CCA entails the actual capturing of raw, detailed information in association with service or feature usage. It encompasses the determination of what structure will be used to capture the information and the full details of the usage (e.g., calling number, called number, start time, Quality of Service [QOS]) for subsequent transmission to the BA.

5.7.3.4. Usage Measurements Storage - Temporary

Temporary usage measurements storage by the CCA refers to the capability needed to retain usage measurements until they can be purged. This function includes storage rules, such as for how long the data needs to be retained and when to flush the data from storage. This process has two components:

1. Storing (i.e., maintaining) usage data while an event is in progress, and
2. Storing usage data after it has been packaged and successfully transmitted to the BA.

5.7.3.5. Usage Measurements Outputting

Usage measurements outputting refers to the transmission of usage data from the CCA to the BA. It is composed of two primary functions:

1. "Packaging" the usage data into the form in which it is delivered across the CCA/BA interface. This entails translating the data from the CCA's internal representation

[5] This is commonly referred to as the "Call Type", and is a key field in determining how a given service or feature is billed.

into a form that is recognized by the BA (i.e., using raw usage details to create a *usage data record*).

2. Physically transferring the data (i.e., the usage data record) from the CCA to the BA across the CCA-BA interface. These usage data records might include either complete event details or partial details (e.g., call connection data in a *beginning* record and call disconnect data in a subsequent *end* record), and can be transmitted either individually or in files.

   This process also encompasses managing communication between the CCA and the BA to ensure that the data transmission process is reliable. It includes features for how and when the triggering of usage data record transmission is accomplished (e.g., by polling or initiated by the BA at regular intervals). The process also includes acknowledging receipt of the usage data recording (e.g., if the BA acknowledges that the usage data records were successfully received, the CCA can then delete its copy from storage; or if unsuccessful, resend).

5.7.3.6. Usage Measurements Report Generation

The *usage measurements report generation* function reports various information to the BA to ensure the integrity and completeness of the usage measurement process. For example, given that the BA will be responsible for "long duration" call processing[6] (see Section 5.7.4.4), the CCA will need to report information regarding what connections are active to the BA on a daily basis. Reporting from the CCA to the BA will also be necessary for exception processing, such as when there is a failure in the CCA usage measurement functionality (i.e., to alert the BA that all expected usage data records might not be received).

5.7.4. Billing Usage Measurements Core Functionality (Billing Agent)

This section describes the fundamental processes in the BA that are involved with billing usage measurements.

5.7.4.1. Accounting Administration

Accounting administration performed in the BA is similar to the equivalent process in the CCA, particularly with regard to managing communication between the two elements. In addition, accounting administration in the BA encompasses the following additional functions:

- Record data administration, including establishing and maintaining parameters needed to populate certain fields in formatted usage records (e.g., Billing Agent Identifier)
- Record and file handling administration (e.g., file size parameters, file transfer initiation procedures)
- System interface communications administration (e.g., to initiate communications between the BA and billing systems)

[6] A *long duration* call is a call that was active upon reaching a particular time-of-day (typically midnight) a second consecutive time. Long duration calls trigger the creation of formatted usage records for each subsequent twenty-four hour period for which the call is still active.

- Systems operations administration, including administration of the BA system configuration and storage thresholds
- Log administration, which encompasses the ability to perform basic administration of the various logs that will be supported by the BA.

5.7.4.2. Usage Data Massaging

Usage data massaging refers to performing additional processing on information in the usage data record in order to produce a correctly formatted usage record. Examples of usage data massaging include rounding input data to conform to requirements and computing the elapsed time associated with a call.

5.7.4.3. Usage Data Correlation

The need for *usage data correlation* is premised on the notion of multiple (i.e., two or more) records being produced in association with a single event, none of which contain all the information needed to produce the applicable formatted usage record. The need for usage data correlation in the BA is one of the fundamental differences between the VOP billing usage measurement process and the analogous PSTN process. In the PSTN, no correlation of distinct pieces of information is necessary for a typical voice call. In the VOP architecture, however, multiple usage data records (i.e., a beginning record and an end record) will typically be produced by the CCA (at the outset and completion of a call, respectively) and transmitted separately to the BA. This processing is primarily driven by the need of the BA to correctly process call connection information in association with long duration calls. The BA must therefore possess the capability to correlate (i.e., associate) these separate usage data records so that it can produce one formatted usage record associated with the call. The BA may also need to correlate usage data records for use of other services or features (e.g., for the activation [beginning] and deactivation [end] of a customer's call forwarding capability).

In addition to the need for the BA to perform long duration call processing, a secondary driver for performing usage data correlation in the BA rather than the CCA is based on the philosophy of offloading as much data (and processing) as possible as soon as possible after the usage takes place.

5.7.4.4. Long Duration Call Processing

As noted in Section 5.8.3.5, the CCA will produce daily reports listing active connections, which are used by the BA to perform long duration processing. The BA initiates *long duration call processing* upon receiving the active connection report from the CCA, using it to ensure that resident usage data records for the beginning of call events are still valid (i.e., for active events). Assuming both beginning and end records are transmitted from the CCA to the BA for each call, the BA can use the information in the active connection report to track calls that are still in progress (i.e., by matching its active beginning records with those indicated on the report). Mismatches can then be addressed through exception processing; those beginning records that correspond with active connections for two (or more) consecutive midnights will trigger creation of a long duration call record (and one or more subsequent continuation records, depending on how long the call is in progress).

5.7.4.5. Usage Record Generation Decision-Making

Usage record decision-making in the BA encompasses determining when to produce the formatted usage record (e.g., when an end record is received, correlated and processed in conjunction with a previously received beginning record). It also determines which type of record is to be produced.

5.7.4.6. Usage Record Generation and Formatting

As previously indicated, in the absence of any business driver to utilize a new format for usage records produced by the BA, an existing standard (e.g., BAF) should continue to be utilized for *usage record generation and formatting*. For future VOP-specific services or features for which no current record formats exist, either the current approach could be extended or a new type of format created. The advantage of utilizing an existing format (either with or without modifications) is to take advantage of existing billing systems rather than requiring new billing applications to be developed.

5.7.4.7. Usage Record Validation and Error Correction

Usage record validation and error correction refers to the functions in the BA that verify the correctness and completeness of usage data. Quality and reliability requirements of the BA functionality are assumed to be equivalent to those in the PSTN environment. Since this usage information is directly associated with a substantial portion of revenues for a typical service provider, validation of the accuracy and completeness of the usage records that are generated is of paramount importance. Usage record validation requirements, therefore, are expected to equate to those associated with the traditional PSTN environment. Usage record validation in the BA may encompass the following facets:

- *Record Completeness* - ensuring that all required data within each record is included.
- *Data Validity* – verifying that the data in the record contains valid values.
- *Record Formatting* – ensuring that the record is properly formatted before being output.
- *User Interface for Error Correction* – specifying a capability for a user interface to be able to process (and perhaps correct) records determined to be erroneous and/or invalid.

5.7.4.8. Usage Record Outputting

Usage record outputting is the processing necessary to successfully output formatted usage records in the form of *usage record files*. These usage record files are subsequently transmitted to the downstream billing system (or other application). This function includes specifying how and when to create the file itself (e.g., periodically [daily, hourly, etc.] or as requested by the billing system).

5.7.4.9. Usage Record File Storage

Usage record file storage in the BA refers to the capability needed to retain usage measurement files until they can be purged. Usage record file storage requirements are likely to correspond to those in the PSTN environment (e.g., the capacity to store a

minimum of five days worth of usage record files). BA requirements for usage data storage include storage rules, such as for how long the data needs to be retained and how (and when) to flush the data from memory. Analogous to the CCA usage record storage process, this process has two components:

1. Storing (i.e., maintaining) usage data files while they are being created, and
2. Storing usage data after it has been packaged and successfully transmitted to the billing system or other downstream application.

5.7.5. Supporting Functionality and Features

Functionality and features that will be needed in support of billing usage measurements include security, auditing, system management, storage and removable media.

The BA supports security mechanisms in the following areas: authentication, access control and confidentiality [7]. Security in the BA is critical due to the importance of the data handled by the component. The goals of this security are preventing intrusion from access to the BA to avoid corruption, alteration, or disclosure of usage data. Interface security is addressed in Section 5.8.7.

The CCA and BA together effectively equate to a switching system from a usage measurements perspective. Accordingly, these elements require auditing of usage measurement events that is equivalent to switching systems. Auditing is needed to ensure the ongoing integrity of billing usage measurement functionality in both the CCA and BA. Auditing is performed to support the recording of information such as number of formatted usage records produced, number of formatted usage records output and number of formatted usage records flagged due to error conditions.

System management refers to supporting the local or remote overseeing of the operation and integrity of billing usage measurement functionality, including the following:

- Generating local alarms and/or protocol notifications upon detecting abnormal conditions (e.g., the BA can output a protocol notification when a file transfer to a billing system fails)
- Providing statistics to network management systems for performance monitoring (e.g., for data volumes vis-à-vis capacity)
- Providing statistics to network management systems for load balancing (e.g., between CPUs, storage devices and/or BAs).

Removable media refers to the management of physical devices that contain billing usage measurements, including their archiving, transport (e.g., to billing systems) and backup/retention.

5.7.6. Constraints

As previously indicated, stringent requirements will be needed to help ensure that the BA and CCA usage measurements functionality operates as expected. These requirements address the following:

[7] Security requirements for the Call Connection Agent are not addressed here since such requirements will presumably be established for reasons other than usage measurements and will also apply to usage measurement functionality.

- *Availability of billing usage measurement hardware and software*

  This refers to the required availability of the component (i.e., allowable down time, both scheduled and unscheduled).

- *Data accuracy (including timing accuracy, aggregation accuracy, etc.)*

  Accuracy requirements are expected to be equivalent to those for the PSTN billing usage measurement functionality.

- *Integrity*

  This refers to monitoring the performance of the functionality in comparison with established quality benchmarks (e.g., loss rates over time, one-time losses of data and misproduction of data) in the recording, formatting and outputting of billing usage measurements).

- *Performance/Timeliness*

  This refers to the ongoing monitoring of the functionality with regard to availability (e.g., how soon after the completion of an event does the associated usage measurement data need to be available). Performance also addresses system throughput (i.e., how many records in a given time interval [e g., per second] can the element produce and transmit).

- *Environmental*

  Historically, billing usage measurements components have been required to be protected against certain environmental dangers (e.g., heat, humidity, earthquakes). Environmental constraints also address protection of the people who operate the equipment (e.g., from radiation), as well as structural requirements (e.g., size and weight requirements).

5.7.7. Interfaces

This section describes the characteristics and capabilities that will be needed for interfaces between components of the VOP billing usage measurements architecture.

5.7.7.1. Call Connection Agent to Billing Agent Interface

The Call Connection Agent/Billing Agent interface is expected to have the following capabilities and characteristics:

- Highly reliable delivery of data (which is its key characteristic)
- Secure delivery of data (at a minimum, to prevent data alteration; perhaps also to ensure confidentiality)
- Flexibility to easily support transmission of enhanced or modified data content over the interface
- High performance and efficiency, which are needed to support the transport of expected high volumes of data associated with use of telecommunications services
- Implemented using a standard industry solution.

The CCA/BA interface can be deployed via one of many protocols. Potential candidates include Remote Authentication Dial-In User Service (RADIUS), Diameter and Common Object-oriented Request Broker Architecture (CORBA).

5.7.7.2. Billing Agent to Billing System Interface

The Billing Agent/Billing System interface is expected to have the following capabilities and characteristics:

- Highly reliable delivery of data (which is its key characteristic)
- The ability to transport large volumes of data, typically in large "packages" to billing systems. In the future, this interface might also support smaller packages of formatted billing records (e.g., in support of real-time billing)
- Secure delivery of data (i.e., at a minimum, to prevent data alteration; perhaps also to ensure confidentiality)
- Flexible, to easily support transmission of enhanced or modified data content the interface
- Implemented using a standard industry solution.

The Billing Agent/Billing System interface will likely be implemented using File Transfer Protocol (FTP).

5.8. Security Requirements

5.8.1. Introduction

The Voice over Packet network will be viewed as an attractive target for hackers, foreign adversaries, terrorists, corporate saboteurs, disgruntled employees, and others who might attempt to bring down parts of the network for reasons of espionage, mischief, or vengeance. Because of the potential for disruption, and because the network is a crucial component of the PSTN in general, strong and effective security measures should be in place, and security should be a high priority of service providers. The physical locations of elements and the operations, maintenance, and testing facilities need to be protected from unauthorized access and determined attack. The associated software must also be given ample security during its operation, maintenance, configuration, and upgrades. Both the hardware and software must be protected from insider and outsider tampering.

The network and its protocols are attractive targets for the following reasons:

- The cost (in terms of money, effort, and risk) to an attacker can be low. Intruders have a wide array of sophisticated tools and techniques at their disposal. These are obtainable from a variety of sources including publications, electronic bulletin boards, and Web sites. These sources provide a great deal of accurate and detailed information regarding how vulnerabilities in telecommunications systems and network elements can be exploited.
- The chances of getting caught are low. As networks become increasingly connected, intruders are able to attack remotely from more and more locations, including locations outside national boundaries.

- The return can be high. An intruder has the potential to gain access to customer information such as calling card numbers and calling patterns, and to degrade or interrupt service by attacking the network through the protocol.

Because the network links all elements and other non-call control network components, an intrusion into the network could lead to assaults on elements of the network. Thus, the network may unintentionally offer an intruder a path to a great number of potential targets within the PSTN. An intruder having access to the PSTN at that level could mount any number of assaults ranging from simple theft of data to tampering with the operations and functioning of telecommunications components, which might conceivably halt voice and data service over large geographic areas.

For the foreseeable future, all VOP elements used for public telephone service will be interconnected with and be considered part of the PSTN. Therefore any requirements for VOP telephony must include interconnected PSTN elements. As such, security requirements for the VOP network should be presented from the following three points of reference:

1. The Network (unauthorized access from outside the network)
2. The protocols (e.g., IP, SS7 etc.) that drive the network
3. Individual network elements, both within the VOP and the PSTN, that control and deliver public telephony (e.g., Call Agent, Trunk Gateway).

The scope of this section is to assess the security issues for implementing a VOP network including the following:

- Network Security
  - Unauthorized access from outside the VOP network.
- Transport and Communication Protocols Security
  - ATM
  - IP
  - Routers
  - SS7.
- Functional Element Security
  - Access Gateway (AG)
  - Billing Agent (BA)
  - Call Connection Agent (CCA)
  - Operations Support Agent
  - Routing and Translation Agent (RTA)
  - Signaling Gateway (SG)
  - Service Agent (SA)
  - Trunk Gateway (TG).

5.8.2. Network Security Issues

Because the network links all elements and other non-call control network components, an intrusion into the network could lead to assaults on elements of the network. Thus, the network may unintentionally offer an intruder a path to a great number of potential targets within the PSTN. An intruder having access to the PSTN at that level could mount any number of assaults ranging from simple theft of data to tampering with the operations

and functioning of telecommunications components, which might conceivably halt voice and data service over large geographic areas.

The classical protection against network attacks is to isolate the network that supports the critical application from outside networks using “firewalls”. These firewalls must be considered “first-stop” only defenses and should not deter network security agents from protecting the inner core of the network from intrusion. The most secure method of protecting the network from harm is by deploying security measures at each network element, transport and even in the transmission protocols.

At issue then is how to make firewalls as secure as possible so as to keep unauthorized access to a minimum and also to realize that all networks are penetrable and that protecting the inner core is just as important as protecting the outer wall.

5.8.3. Transport and Communication Protocols Security Issues

5.8.3.1. ATM

ATM vendors have been slow in providing the security services needed to perform identification, audit, system access control, resource access control, integrity, and security administration. The system is wide open and all of its vulnerabilities have been documented by the hacker community and are ready to be exploited. The VOP network must demand that the vendors provide the means to implement needed security features. There are many other security issues with ATM and should be explored.

5.8.3.2. Internet Protocols

IP networking, and equipment (e.g., routers) are well known and well understood by the intruder community. As a result, intruders using traditional and new IP hacking tools and techniques will attack IP telephony networks resulting in denial of service, eavesdropping, and theft of service. At the very least, IP will be vulnerable to the following problems:

- *Loss of confidentiality*

  If IP security features are not in place and messages traverse the IP network in the clear, then the contents of the messages will be readable as they pass through the IP network.

- *Loss of integrity*

  IP networks are managed using protocols that lack security features and provides a good potential source of exploitation by attackers who assault IP nodes through management channels.

- *Address spoofing*

  This is a common form of attack upon IP messages, which may also contribute to loss of integrity by causing messages to stray.

- *Loss of authenticity*

  Address spoofing may also cause a loss of message authenticity if an intruder is able to send counterfeit messages that appear to come from *bona fide* sources.

Deploying newly developed IP Security (IPsec) techniques may be one answer in protecting information, but it will not protect against denial of service attacks. The combination of multiple firewalls and IPsec can increase the level of security, but core network security features must still be deployed.

5.8.3.3. Routers

The security of the router is influenced by both the physical location of the router and the security of the software the router is running. Security issues must be addressed from two perspectives - 1) router access features and 2) data routing features. Traditionally router access features do not include identification, authentication, system access control, resource access control, auditing and alarms, system integrity checks or security administration.

Security of data routing should be analyzed based on routing of traffic, filtering of traffic, encryption of traffic and auditing of traffic.

5.8.3.4. Signaling System Number 7

As SS7's role in packet-based telephony and other new technologies increases, the potential downside of severe network outage as a result of tampering increases as well. Intruders, hackers, and other potential adversaries have more understanding of SS7 than ever before. They also have greater opportunity to intrude, greater incentive to intrude, and greater chance of success than they have had before. Furthermore, there may be powerful adversaries with money to spend on expertise that could be used to bring down the signaling network and with them the VOP networks ability to transport calls. This concern has prompted a number of in-depth studies to determine the nature of SS7 vulnerabilities. Some of these studies have been alarming in their tone and conclusions, triggering even greater concerns. To state the results of these studies in detail is beyond the scope of this report. However, these studies have concluded that the risks of greatest concern for the SS7 transport are the following:

- Theft of data from SS7 messages
- Alteration of data in SS7 messages
- Subversion of SS7 messages to alter the normal operations of the CCS network
- Subversion of operations messages (both SS7 messages and messages sent across other operations channels) to alter the configuration, performance or reliability of the CCS network
- Physical damage to or destruction of CCS nodes or CCS links.

These risks exist because the SS7 protocol lacks comprehensive security features, and because physical and operational security need to be stronger.

5.8.4. Functional Element Security Issues

All new and existing network elements must have the ability to block and or to audit unauthorized entry into the system or unauthorized use of system resources. Network Element security feature requirements can be categorized as follows:

- *Identification*: the process of recognizing a session requestor's unambiguous and auditable identity, such as userid.
- *Authentication*: the process of verifying the claimed identity of the session requestor.
- *System Access Control:* authorizes the establishment of a session (i.e., login) and continuation of a session until logoff.
- *Resource Access Control:* provides the capability of denying access to the network element resources in the absence of proper authorization (user privilege, channel privilege, etc.).
- *Security Log:* provides tools to establish an audit trail.

Therefore it is required that each listed VOP network element have the capabilities to implement these security features. Protecting the network elements from unauthorized access is most important but providing security for the data communicated by the elements is also important and is discussed in the following sections.

5.8.4.1. Access Gateway

The AG presents the line interface from the customer premises to the network. This line interface must allow line functions (i.e., dial tone, digit capture, etc.) but must function to block all other backdoor access to the connected network element. Line interfaces at the PSTN switch are an excellent example of how line interfaces provides protection from intrusion i.e., allows for line functions but has no linkage for access to the host processor.

5.8.4.2. Billing Agent

Unauthorized access to the BA has the greatest potential for fraud and possible destruction of billing data. There is little if any evidence that the unauthorized access will lead to network outages.

5.8.4.3. Call Connection Agent

The CCA element provides most of the call processing functionality to support voice on the packet network and therefore demands the most careful planning and engineering of security features. Based on existing PSTN engineering principles, all network elements and components are duplicated. This principle affords a measure of protection i.e., minimizes the risk of a total service outage. Any lack of engineered redundancy in new VOP elements must then be met with the greatest number of security features available. When the architecture of this elements is introduced it must be subjected to an expert security risk analysis; one that would recommend appropriate security features.

5.8.4.4. Operations Support Systems

Access into an OSS enables remote access, multiple access and widespread access in network elements. As has been shown, operation support systems have communication channel connection with network elements and transport elements that are, for the most part, always active. This leads to the following two considerations that require attention, especially since the potential consequences are so great:

1. Undetected or undesirable connectivity between the OSS platform and any other network, such as the Internet. If there are avenues of access and egress to the OSS from the network elements, then an intruder can accomplish any type of attack.
2. Allowing open access from in-house functions i.e., maintenance centers, provisioning centers, etc.

All “best” practice security features must be available in this new element to allow the administrator to do the following:

- Provide each user with a unique userid and password
- Authenticate each user
- Allow system access control
- Utilize resource access control such as user and channel command privilege
- Implement security log files to provide audit trails.

5.8.4.5. Routing and Translation Agent

The RTA provides the software for the routing of calls over the packet network. It also provides the line, feature and profile information for direct connect line customers. Unauthorized access to this element can result in fraud, disruption of service and message routing errors.

5.8.4.6. Signaling Gateway

The SG provides the interface between the Call Agent and the SS7 network STP for ISDN-User Part messages. Unauthorized access to this element could result in network disruption due to the impact on trunking i.e., trunk set-up and disconnect messages are disrupted.

5.8.4.7. Service Agent

The SA provides service logic for calling features. The logic software could located at the SA or an SS7 SCP. Unauthorized access to this element could result in the illegal use of network service free of charge. Disrupting this element would result in lost revenues due to feature unavailability.

5.8.4.8. Trunk Gateway

The TG converts circuit switched voice to packet and provides additional trunk functions, such as DTMF transport, tones and announcements, and transmission measurements testing. The trunk connection to the switch does not present any vulnerabilities to the switch but continues to be a source of concern for illegal monitoring and fraud.

6. Operations and Management Architecture

6.1. Introduction

Competitive VOP offerings must have an effective and efficient Operations and Management (O&M) architecture realized through processes and systems that scale with service features provided, and network size and complexity. The business needs of Service Providers dictate that service be provided quickly and easily, that operations and management support a Quality of Service (QOS) comparable to that of PSTN, and that the operations costs are competitive with current services. These needs must be satisfied in the face of major new challenges. For example, the VOP network typically involves a variety of new elements from multiple suppliers. New customer service fulfillment models are needed to reflect customer expectation ranging from traditional telephony service activation to Internet Service Provider web activation.

The operations and management architecture needs to effectively span the following domains:

- Multiple network layers: transport, ATM, IP, signaling and control
- Varied customer premises equipment arrangements including both those purchased by customer and those provided by a Service Provider
- Numerous technologies including gateways of various types, call and service agents, ancillary servers, routers, and management systems
- Multiple suppliers
- Interfacing with other networks: circuit switched, Internet, ATM, fast packet
- Interconnecting with other service providers: ILECs, CLECs, IXCs, ICPs, and ISPs.

In addition, the operations and management architecture needs to have the flexibility to be able to support future services and service features, and the Next Generation Network (NGN) through a straightforward evolutionary path.

6.1.1. Business Drivers

The correct operations and management strategy and architecture are critical to business success. In particular, the operations and management approach for VOP must satisfactorily address the following business drivers.

- *Service Quality*

  To maintain customer loyalty it is expected that VOP will require a Quality of Service (QOS) as measured in the following dimensions at the service access point:

  – Ease of access and use, e.g., simple subscription and call management consistent with the look and feel of today's services

  – Support for a QOS comparable to that provided by the PSTN dial tone delay, voice transmission quality, reliability, survivability, Mean Time To Repair

(MTTR); in sum, customer perception of signaling delay and sound, video or data transmission quality

- Maintaining different levels of QOS, reliability and congestion control for differentiated services across multiple transport technologies, end-to-end across the network
- Reliability and availability of service features, e.g., low call failure rates and high service feature availability. This includes achieving 24x7 availability through network design and engineering, during network augmentation, and in the face of installing new hardware and software releases.
- Customer Care, e.g. Web-based customer interface supporting access to billing and performance information (e.g., Service Level Agreement - SLA), and other customer care functions such as submitting a trouble report, placing an order, checking their status, and quick service restoral.
- Alerting business customers of network detected problems to enable them to better manage use of alternative communications paths

- *Efficient Network Management*

  Reduced operations cost and higher responsiveness have been realized by telecom companies over the last decade. To be competitive, VOP service providers will require the following:

  - Operations using appropriate automation and flow-through to achieve current cost levels and avoid the need for scarce technical support
  - Easy customer access that supports service differentiation, e.g., flexible Web-based customer interfaces
  - Increasingly integrated operations support for circuit switched and packet switched service platforms
  - Common operations for bundled services (e.g., voice and Internet access).

- *Scalability*

  The dynamics of the market and the anticipated rapid emergence of innovative use of the network will require the following VOP operations capabilities:

  - Support of customer growth and network expansion
  - Applicability to large and small volume business environments
  - Support for rapid deployment of successful new services.

- *Flexibility*

  VOP operations will need to support the introduction of the rapidly changing technology base that will be the platform for emerging businesses. This implies support for the following:

  - Traditional telephony services over the data portion of the hybrid network, while providing the basis to supporting a new generation of IP, Internet and multi-media services in the future
  - Customer mobility

  - NGN through a straightforward evolutionary path.

- *Security*

  Customer confidence in service security wherever the user is located will be a continuing critical element to success. This implies the following:

  - Mechanisms for administration and management of network access authentication and access control
  - Use of appropriate security mechanisms (e.g., encryption, digital signatures) for data confidentiality, data integrity, and non-repudiation
  - Appropriate security features on operations interfaces
  - Secure access to network management systems.

- *Flexible Billing*

  New pricing strategies will be developed as new services and service packages emerge. This, along with new alliances among emerging companies, will require the following:

  - Flexible billing mechanisms to support varied pricing strategies and special offers including usage-based billing, and discounts for service packages or volume usage
  - Standards for billing usage measurements formatting and transport for both the PSTN and packet services; this is essential for interconnection of autonomous service providers.

- *Operations Support Systems*

  The rapid emergence and introduction of new systems and network technology to deliver VOP services will require the following:

  - Appropriate system framework for integrating critical in-place systems with platforms and applications from multiple suppliers
  - Inter-domain systems that manage multiple services and customers across technology domains
  - Ability to operate across multiple vendor-specific network elements, element management systems and account for already installed infrastructure, new or recent infrastructure, and emerging infrastructure.

Standards bodies and industry forums are starting to address a number of the VOP operations needs and issues (see Section 3). Currently, vendor products offer proprietary solutions to some of these needs, but fall short of providing a suite of O&M applications that fully address all of these issues.

It is important to provide some structure to the Operations and Management (r)evolution. Sufficient progress has been made to identify comprehensive O&M requirements that drives the next generation of products that would provide an orderly integration of multi-vendor equipment and circuit and packet technologies. This effort complements custom solutions that are needed given the current diversity of products, business situations, and legacy operations environments.

6.1.2. Scope and Approach

The Operations and Management Architecture Section provides a framework architecture for addressing VOP operations and management. It identifies operations and management needs for VOP emphasizing new challenges that VOP introduces beyond that faced for existing services and networks. Accordingly, it "dimensions" the operations challenge, but does not give solutions to it.

This section develops the framework in terms of business issues and needs of the next one to three years. This section is structured as follows:

1. First, the impact of VOP on operations processes and associated functions is discussed. Key processes will be used to organize the functional impact and relate the analysis to business drivers.
2. Next an overview of information needs and issues for VOP is given based on a comparison with information needs of POTS.
3. Finally, a framework to structure solutions is given that describes the activities and considerations in planning and designing a VOP O&M solution.

The solution framework provides a methodology to apply to choose among the various alternatives for realizing an operations solution for VOP services. It includes discussion of the use, role, and value of industry management models and protocols. It encompasses TMN layering, multi-domain management, application implementation architectures and the use of common computing/communications Middleware, operations interfaces, and protocols. A protocol neutral approach is taken to maximize consideration of solving business needs with existing and emerging products. Recent Network Management (NM) concepts must be assessed for feasibility and timeframe, rather than immediate adopting and advocating an "ultimate" architecture that might have merit sometime during the 21st century

The architectural framework proposed for the operations and management of VOP networks is the ITU-T recommended Telecommunications Management Network (TMN). The Bellcore proposed solution is based on a number of industry TMN-based specifications and requirements documents, most notable the following:

- GR-2869-CORE
- ITU-T Recommendation M.3010, Principles for a Telecommunications Management Network (TMN), 1996.
- ITU-T Recommendation M.3400, TMN Management Functions, 1996.
- GB910, SMART TMN™ Telecom Operations Map (TOM), Version 1.0, (TeleManagement Forum, October 1998).

The scope of this section excludes detailed requirements, implementation packaging, specific Operations Support Systems (OSSs) (would need to be addressed on an individual SP basis), and the Information Technology (IT) platform environments.

6.1.3. Organization of Section

The organization of the remainder of this section is as follows:

- Section 6.2 – Business Processes and Functions
- Section 6.3 – Information Architecture
- Section 6.4 – Framework to Structure Solutions

6.2. Business Processes and Functions

The VOP service initiatives must be built on efficient end-to-end business processes to be cost competitive and operationally consistent with current best practices. Accordingly, this section is organized around the three key processes, namely, service fulfillment, service assurance, and billing. Following is a brief description of each of these processes:

1. Service fulfillment involves the establishment of a network, the planning and creation of services on that network, and the offering (sales and ordering) and configuring these services to paying customers.
2. Service assurance involves all activities required to maintain and assure the quality of service promised to the customer. This can be accomplished proactively and reactively.
3. The billing processes or accounting management processes involve the timely collection of usage data, rating and distribution of billing event records, credit validation, and timely invoicing and handling of adjustments and collections.

The impact of VOP is illustrated by discussion of some affected aspects of each of the processes, and the functions needed for VOP. This is not meant, however, to be a comprehensive treatment of business processes and functions for VOP. For example, some of the issues associated with the Business Management Layer will not receive full treatment but will be addressed in the context of the processes identified above.

6.2.1. Service Fulfillment

The Service Fulfillment business processes most affected by VOP are Customer Interface Management, Sales, Ordering, Service Configuration, and Network Provisioning.

6.2.1.1. Customer Interface Management

Centralized customer care capabilities for VOP service providers need to include Web interfaces as well as automatic routing of personal voice transactions. These customer interfaces need to support corporate marketing approaches, e.g., branding, and new billing options. The customer interfaces may have global aspects for international providers; e.g., language selection may be needed for screens and announcements.

6.2.1.2. Sales

The sales process will involve special personnel training. Account executives and service representatives will need to understand not only voice services, but also how these may be affected by their being offered over a packet network (such as being aware of QOS issues). They will also need to understand the benefits of VOP over PSTN. If voice services are offered as part of a package with data services, the personnel will need to be aware of data service issues and potential interactions with voice services. More sophisticated customers may want information on the networks involved in an end-to-end

voice path. The personnel will also need to present billing implications of service bundling options.

6.2.1.3. Ordering

The following key operational characteristics of the order handling processes are considered necessary to support the VOP user:

- Support for service ordering for multiple geographic areas of use including the information needs of business partners
- Service ordering that enables customer controlled security; especially important with third party sales channels
- Separation of customer credit assessment from immediate activation of service
- Service feature templates to enable simple and consistent methods for ordering voice and billing service features for the non-expert and third party sales channels
- Standard order templates and identification codes for internal and inter-company ordering of services. A key requirement will be service codes for QOS parameters.

6.2.1.4. Service Configuration

Configuring of customer-specific information in the appropriate systems for VOP includes the following:

- Provisioning access information in the access network, e.g., ISDN terminals and cable boxes represent potential new service configuration and security requirements for activating voice features
- Provisioning customer service configuration information in the Call Connection Agents and Service Agents
- Provisioning the underlying packet services in packet NEs (e.g., IP addresses in DNS servers)
- Provisioning of voice service parameters in the NEs responsible for the configuration of the CPE (if applicable)
- Configuring mobility management parameters to enable users ability to access from various locations.

Activation of the customer service involves the coordination and sequencing of remote software service activation, including the following activities:

- Installation and testing of the CPE (if any)
- Configuration of the CPE (if any), e.g., via software downloads
- Activation of the service in Call Connection Agents and Service Agents
- Electronic interfaces between business partners for consistent activation of services.

Some of the above activities represent a departure from PSTN needs and practices. The Internet Service Providers applications, ISDN terminals and cable boxes represent

examples of potential new service configuration and security requirements for activating voice features.

6.2.1.5. Network Provisioning

The Network Provisioning process includes the engineering, installation and administration of the VOP network including its voice service control infrastructure as described in Section 4. In provisioning the network, special attention needs to be paid to the following:

- Relationships between Call Connection Agents and trunk groups
- Relationships between Call Connection Agents and Trunk Gateways
- Relationships between Call Connection Agents and Billing Agents
- Relationships between Call Connection Agents and Voice Feature Servers
- Digit analysis information
- Routing information within the Call Connection Agents.

Major aspects of the VOP network and service environment will influence the engineering processes. The service provider initiatives will likely involve alliances and partnerships of the various players in the business model. Engineering activities will involve the network design using new NEs and routing associated with Packet Networks and their interconnection.

Voice services will be implemented largely by incorporating service logic in the Call Connection Agents that will handle all connectivity required, and in peripheral NEs, such as the Voice Feature Servers and Service Agents. This is not unlike the deployment of SS7 services in the PSTN. However, new capabilities will need to be supported, e.g., some of these services may make use of the underlying transport network (e.g., packet broadcast services), and thus, new procedures will be needed that recognize new parameters and functionality.

In addition, the transport packet network will need to support the provisioning of new categories of information on some of these services. In particular, some peripheral NEs on the packet side will need to handle the configuration of the CPE, and hence, they need to be provisioned with the CPE-resident service functionality.

These characteristics of the Network Provisioning Process imply a new emphasis on the following:

- A framework for introducing rapidly emerging technologies and services
- Implementation of Business Level Agreements among the service providers, network operators and the third party suppliers
  - Software and interface release and implementation management among the system platform, Middleware and service application providers
  - Centralized network and service planning (e.g., Release planning) and distributed software implementation management (e.g., service configuration and network provisioning)

  - Testing of new capabilities involving multiple providers: product testing, integration testing, First Office Applications and user testing.
  - Documentation management (e.g. interface specification, system practices).
- A “signature” or “brand” look and feel for services with the large variety of customer expectations (potentially around the globe)
- New network elements and the traffic sensitive design to the customer interface
- Service design coordination for multiple network and service providers to meet the traffic and processing demands
- Feature interaction management between existing PSTN services and packet network-based services introduced by other suppliers
- Engineering systems and procedures that support significant outsourcing of many of the engineering as well as operations functions to software and hardware suppliers
- Key engineering processes to support:
  - Network infrastructure design (e.g., for ATM and IP networks)
  - Access infrastructure design (e.g., Hybrid Fiber Coax, xDSL)
  - Facility infrastructure design (e.g., PDH, SONET/SDH)
  - Routing design for IP networks
  - Numbering plan development and management for interworking of the Telephone Number and IP addresses under the assumptions of user mobility and number portability.

6.2.2. Service Assurance: Fault and Performance Management

The VOP Service Assurance Process must be able to address new types of network elements, a network architecture that includes packet-based and circuit-based networks and their interconnection, new quality parameters, new customer manifestations of degraded performance, new failure modes, and increased focus on Web-based trouble reporting and status information. Since troubles can be identified by multiple sources (e.g. customer, service provider, network operator or third party service providers), the service provider must have a network and service status advisory process that supports customer notification and avoids unnecessary maintenance and trouble shooting activity.

The key operational characteristics of the service assurance process that are considered necessary to support the VOP service provider are as follows:

- Help desks and call center access to status of the transport and service capabilities to handle customer calls
- Customer trouble report management that is consistent with Service Level Agreements (SLAs)
- Mapping of new network performance characteristics to the SLA QOS measures, e.g., packet loss impact on voice control and call audio quality
- New trouble shooting approaches that recognize the customer VOP symptoms in terms of the IP packet or ATM cell relay network behavior

- Training of skilled network operations staff to maintain the network performance and network elements
- Consistent service performance measures that can be meaningful to partners of a VOP initiative, e.g., dropped calls as observed by the service provider and the troubles that occur as a result of an intermediate transport provider problem.

Considering the need to offer voice services over packet networks and be successful relative to traditional PSTN providers, assuring a high quality of service (QOS) becomes a critical priority for a VOP SP.

For service assurance, a seamless status and control management process between the service provider alliance and the sophisticated VOP customer becomes critical. Network maps, for example, must represent both sides in common views, in order for troubles to be easily traceable.

The following sections provide additional discussion of service assurance subprocesses.

6.2.2.1. Proactive Service Assurance

This represents a set of activities geared towards the detection and resolution of troubles before they affect the customer (or at least, before they are noticed by the customer), as well as the avoidance of troubles before they even occur.

Alarm surveillance, fault localization and performance monitoring and traffic management play the key roles here.

6.2.2.1.1. Alarm Surveillance

In the area of alarm surveillance, the SP's network management functionality will have to handle a new set of alarms, from the VOP NEs. Alarm correlation across the diverse technologies of voice service control, signaling, and packet transport represents a major challenge for VOP providers.

6.2.2.1.2. Fault Localization

Fault localization is another major area of concern for similar reasons. Procedures must be developed to manage the following:

- Interfaces to customer networks
- New NEs that separate call control from switching and routing
- Increased involvement of third party service providers.

SP automation and personnel charged with the detection and resolution of faults must be familiar with both sides of the VOP puzzle: voice service workings and packet networking.

6.2.2.1.3. Performance Monitoring and Traffic Management

Monitoring the performance of the VOP network is another area critical to the success of the VOP SP. This involves defining and using the right types of measurements. Some such measurements will be monitored mostly in the packet world, and yet they must

address voice needs. Other measurements will be on trunks, and they can be typical of PSTN, except that they concern transitions between the VOP and the PSTN worlds, which represent a major source of QOS degradation. The importance of these factors cannot be overemphasized.

Performance monitoring also involves the selection of the proper thresholds for threshold crossing alerts (TCAs) – a process that will require extensive VOP experience. The monitored parameters and selected thresholds have a very broad impact because they impact report generation, engineering systems, and Service Level Agreements.

The network performance measurements, of course, ultimately target the proper application of traffic management functions, which allows the SP to circumvent problems. PSTN types of traffic controls, for example, cannot be reused in the VOP world. Rather, traffic management policies will differ from PSTN, since instances of performance congestion may be due to packet congestion, and not voice nodal congestion. Moreover, these policies will differ from PSTN due to the differences in traffic behavior between the underlying transport mechanisms.

QOS is expected to be very closely tied with billing. Thus, reporting mechanisms for customer service performance may need to be introduced to the SP's network and service management structure.

6.2.2.2. Reactive Service Assurance

Reactive service assurance involves all activities required to resolve troubles reported by the customer or other sources.

Customer Care personnel will be called to handle customer calls with a variety of complaints, some of which will be unique to the VOP world. The proper methods and procedures, and well-designed training will be critical to the success of VOP service assurance.

Comments on fault localization mentioned in the previous section apply here also. When a customer calls in with a trouble, the resolution of the trouble will require knowledge of both sides of VOP. For example, a voice service problem, such as low quality, may be due to packet network failures or other causes.

Typically, the resolution of a voice trouble will involve more activity by the Customer Care and Repair personnel than is typical for PSTN, as there are many more variables that contribute to the customer's service, and hence that can affect it.

6.2.2.3. Fault Correction and Testing

The correction of faults will require new methods and procedures, as VOP involves new NE types. This holds true for both software correction (such as remotely resetting parameters) and physical correction (such as part replacement). Customer mobility, i.e., use of service features at access points outside the home area, will require extending capabilities to coordinate fault management procedures with foreign networks. Training will also be key for rapid, efficient and successful fault correction.

Similarly, there are new NEs to test, and new testing procedures and tools must be developed and/or acquired. VOP may also require the establishment of some novel types of tests that normally do not belong in the typical PSTN test suite.

6.2.2.4. System Management

The VOP system and NE management hardware and software including the call connection function create a more distributed environment that must be managed. The PSTN, on the other hand, tends to feature highly concentrated applications relative to the VOP environment. VOP system management thus involves the management of the following key elements:

- Topology of the VOP components
- Status and control of VOP distributed applications
- Status and control of computing platforms, Middleware, resources, processes, devices, services, etc.
- Load balancing
- User and system access security.

6.2.3. Accounting Management: Billing Process

This area represents a critical challenge for a SP newly offering voice service. SPs that do not provide voice service may not have the necessary billing mechanisms to measure and bill for voice usage. These mechanisms must be defined and established.

The billing process has to enable easy evolution from service development and trials to commercial delivery. The following key operational characteristics of the billing process are considered necessary to support the VOP user:

- Management of billing usage to enable flexible call settlement processes (e.g., revenue sharing arrangements with third party vendors or settlement of mobile usage charges)
- Remittance management for various call handling and transport problems
- Rapid availability of billing usage measurements information from network elements necessary to support VOP for service resellers
- Interfaces between VOP subscriber databases and existing service provider subscriber and billing databases.

As described in Section 5.7, billing measurements associated with voice calls and usage of associated services will need to be collected from new NEs and subsequently correlated and output before being transmitted to downstream billing systems.

In addition, as QOS issues enter the picture, the SP will need to establish new billing policies and set up the necessary functionality to carry them out. For example, billing inquiries may involve the verification of low quality (via QOS reporting) and the issuing of the necessary billing adjustments

6.3. Information Architecture

6.3.1. Introduction

One of the critical areas in the introduction of VOP in a service provider's network is information management. This section provides an analysis of the information needs of a VOP provider, and juxtaposes these against information in the framework of POTS.

To accomplish this, this section organizes information in several key categories. For each category, the analysis proceeds to discuss the information needs of VOP, and how they might differ from POTS information.

The intent here is not to provide an information architecture solution for a Service Provider, as such a solution strongly depends on the provider's existing information environment, business practices, services to be offered, and operation migration strategy. Hence, it would require a more detailed analysis of the provider's needs. This section provides instead a roadmap of information needs and issues that would be encountered.

6.3.2. The Information Roadmap

Bellcore typically uses a variety of information frameworks in analyzing the needs of a SP. This SR uses an information roadmap abstracted from a Bellcore model of the information management for a typical SP. The model itself provides substantial detail, and such detail will be needed for a more thorough analysis. But for the purposes of this discussion, the abstracted view will suffice to provide the VOP information roadmap.

The information needs can be classified in the following key categories:

- Activity Management
- Accounting
- Corporate Environment
- Customer
- Customer Account and Contracts
- Equipment Inventory
- Connectivity Inventory
- Access Inventory
- Finance
- Designs and Plans
- Location
- Products
- Resource Utilization
- Routing
- Support Material
- Surveillance
- Service Instances
- Work Force.

Information needs for the business of VOP fit under these categories.

6.3.3. Voice Over Packet Information Needs and Impacts

6.3.3.1. Activity Management

The collection of formal operating procedures of the SP will have to be augmented by a set of new methods and procedures involving potentially a new transport medium, if applicable. More critical, however, will be the management of procedures pertaining to the interaction between voice services, with which the SP may already be familiar, and the entirely new transport medium on which they will ride. New, interdisciplinary methods and procedures must be developed and associated training plans must be formulated to address the new needs of the business.

6.3.3.2. Accounting

The SP will have to develop new billing strategies. Depending on these strategies, the SP's accounting system may be affected. The SP may have to manage new types of call detail records, generated by the new VOP NEs in the SP's network. For example, the new policies may call for billing sensitive to the quality of service (QOS) during each specific call, a substantial departure from the typical POTS practices. Service representatives may need access to QOS information on a per call basis, in order to address customer complaints and billing inquiries. Such issues will affect the accounting information management needs of the SP.

6.3.3.3. Corporate Environment

Managing the SP's VOP business may bring a new set of variables. Present and future government mandates (e.g., the requirement to provide 911 service and lawfully authorized electronic surveillance) will require the SP to develop the data structure to keep track of compliance. Regulatory filings may also enter the environment. These issues are no different than POTS per se, but the implementation from a technical perspective may affect the SP's information needs.

6.3.3.4. Customer

The customer's identity and associated information will not be affected by the introduction of VOP per se. However, how the customer information is categorized may be affected, particularly for SPs who have not offered voice services before. The majority of the impact will be in the customer service configuration arena, which is covered under the Service Instance category.

6.3.3.5. Customer Account and Contracts

The introduction of VOP in the SP's suite of services will affect the contract and account information the SP maintains. The account information may be affected by the introduction of new billing mechanisms. Contracts may require new options, particularly for SPs that never offered voice services before.

6.3.3.6. Equipment Inventory

The introduction of a new series of VOP NEs will require the addition of new data entities in the SP's information structure. These will be entirely new types of NEs, and hence, the new entities will have their own new sets of attributes. This may impact the SP's equipment and software inventory databases.

6.3.3.7. Connectivity Inventory

The inventory of the entire connectivity infrastructure will be impacted by the new technology that the introduction of VOP brings to the SP's environment. Some examples include the following:

- The inventory of new transmission media, if the SP does not already have such media in the network
- The need to inventory circuits (e.g., PVCs in an ATM environment) set up as part of customer service configurations or for the needs of the SP's own business
- All transport connectivity supporting VOP. This may contain multiple layers of transport.

The termination points of such circuits will involve potentially new addressing schemes, which may impact the way connectivity is inventoried in the SP's existing environment.

6.3.3.8. Access Inventory

The POTS model for access to customer service locations involves a variety of loop, port identifiers and telephone numbers. VOP is no different, except it adds a new set of variables in identifying ports on the customer side. Some examples are as follows:

- Hardware identifiers on the CPE
- Connectivity address(es) on the CPE, such as IP addresses for voice over IP
- Additional addressing schemes, such as symbolic domain addresses for voice over IP
- Underlying transport equipment identifiers supporting access to the customer.

All these elements need to be associated with each other and with the access to the specific customer. This typically involves, and hence impacts, multiple databases in the SP's environment.

6.3.3.9. Finance

The impact identified in this category is limited to the new types of accounting events that the SP may have to log and track, particularly for a SP that has never offered voice services before.

6.3.3.10. Designs and Plans

VOP will introduce a new set of session control mechanisms, and may introduce a new transport medium. These will require the SP to develop new plans and engineering designs. Whereas this does not constitute a new type of information, these plans and

designs will contain variables that will be new to the SP and may need additional data structures with which to be managed.

6.3.3.11. Location

This category contains data for the identification and attribution of sites, routes and geographic locations pertaining to the network infrastructure or the customer service locations. Much of this type of information is probably already covered in the SP's information structure. However, new attributes (data details) may need to be introduced, which will affect the SP's location databases. Managing VOP CPE, for example, may require the addition of new data entities (such as CPE location and physical access requirements) in the SP's databases.

6.3.3.12. Products

The SP's product catalog will have to be augmented with a new suite of voice services and features. This may involve the generation of new data entities, particularly if the SP has never before offered voice services.

6.3.3.13. Resource Utilization

The need to provide POTS quality on packet makes this a critical area to the success of the SP. Thus, measuring the performance of resources, such as infrastructure components, many of which will be new to the SP, and connectivity, is an area where VOP will have a major impact. As a result, the following new types of performance measurements will have to be managed:

- Trunking performance, for trunks to connect to the PSTN
- Voice call performance, which may involve measurements unique to the packet world
- Session control performance
- Overall QOS for plain voice calls and added service features.

In addition, the associated traffic management will involve new types of traffic controls, unique to VOP.

6.3.3.14. Routing

VOP will require new routing methodologies, resulting in new routing models and new data structures to store and manage routes. For example, unlike PSTN, VOP will make use of the unique characteristics of packet routing (e.g., IP routing and ATM SVCs), such as the ability of a node to reach any other node "directly."

6.3.3.15. Support Material

This category involves data necessary for the management of the SP's VOP network and services. New tools, test sets, spare material, documentation, etc. are bound to enter the business. Some of these will be unique to the VOP world, as opposed to POTS.

6.3.3.16. Surveillance

This is another category critical to the success of the VOP SP. The types of new information the SP will have to manage include the following:

- New fault types associated with the new NEs
- New alarm information
- New trouble report and performance exception types
- New fault localization procedures.

Compared to POTS, VOP will involve new NEs, its own routing methodologies, and its own failure types. This assures that all items in the list above will contain elements that go well beyond POTS.

6.3.3.17. Service Instances

VOP involves its own service descriptions and configuration requirements. Data capturing VOP service configuration information will involve parameters that are unique to VOP. Thus, this category of information will also be impacted by VOP in a major way, potentially affecting multiple distinct elements within the SP's data management structure.

6.3.3.18. Work Force

VOP will require new skills in the work force of the SP. These new skills may require the establishment of new work management algorithms, which may have an impact on the SP's work force administration software.

6.4. Framework to Structure Solutions

This section provides a framework to structure an operations and management solution for VOP networks. As described in Section 4 (Technology and Architecture Framework), VOP networks introduce a number of new Network Elements (NEs) and other aspects such as NE distribution, signaling and control, voice transport, internetworking with the existing PSTN, and Quality of Service, which all need to be managed from a telecommunications perspective. The purpose of the Operations and Management Framework Architecture, addressed here, is to provide the reader with a structured approach to addressing operations and management issues associated with offering Voice Telephony Services over emerging packet-based data networks. Although the scope of this operations and management framework addresses VOP, the proposed solution approach is extensible to - but does not explicitly address - the operations and management of other network services that may be offered over the Next Generation Network, e.g., Internet Access, Cable TV, Virtual Private Networks (VPNs), multi-media.

This section integrates material presented in the previous Operations and Management sections and describes some of the steps, activities and considerations in planning, designing and/or procuring an operations and management solution for VOP. The framework to structure an operations and management solution for VOP networks encompasses the following:

- Business goals, strategies, objectives, and policies
- VOP network architecture, services, and technologies needed to support the business
- A TMN-based architecture for VOP networks
- A functional architecture
- Operations process scenarios
- A data/information architecture
- Management domains and targeted integration levels
- A physical architecture framework that includes packaging of functions, data, and interfaces to be supported by OSSs
- System interface options.

6.4.1. Business Goals, Strategies, Objectives and Policies

A key aspect in framing the operations and management solution for VOP networks is to decide on certain business goals, strategies, objectives and policies. Depending on whether you are a Network Operator (NO) for VOP networks, a Service Provider (SP), or supplier of VOP network elements, your business goals, strategies, objectives and policies may vary. These business decisions need to be articulated because some of them impact the operations and management architecture for VOP networks. For example, a Network Operator may decide that packet-based data networks and off-the-shelf voice telephony gateways provide the cheapest capital investment and quickest way to deploy a voice grade telecom network. In this case, the operations and management solution may need to address the integration of multi-supplier NEs that have pre-defined operations capabilities and system interfaces.

A SP must decide whether a VOP network provides the required voice services and Quality of Service (QOS) needed to retain and/or increase market share. Service Level Agreements (SLAs) are key service differentiators today, but the VOP criteria used to define SLAs need to be backed up by available measurements, reporting capabilities, and selected pro-active corrective actions (e.g., customer contact, protection switching, billing credits, etc.).

A goal to provision service within a specified time frame may require a certain level of process automation. Customer Care services and access may also be a key service differentiator that helps the SP establish a name brand.

Suppliers of VOP NEs may want to sell off-the-shelf NEs and bundle in an Element Management System (EMS) that provides operation and management capabilities for this supplier-domain of NEs. This EMS may then need to be integrated into a larger Operations Support System (OSS) environment to address overall VOP network operations and management.

The following is a sample list of considerations that should be reviewed for applicability to one's business goals, strategy, objectives, and policies. Many of these items are key design aspects in framing the operations and management solution for VOP networks.

- Service management and network management approaches that are independent of underlying network element technology as much as possible
- Cross-technology domain management
- Use of multi-supplier network elements and their element management systems
- Element management layer approaches that support supplier independence to network and service management layers
- Use of the network as an ultimate source of inventory data
- Management domains based on functions, geography, technology and/or supplier equipment, etc.
- Engineered business processes with automated and manually-assisted flow-through as a key to lower/reduced operations and management expenses
- Increased service quality and customer satisfaction
- Reuse and integration of existing or off-the-shelf Operations Support Systems (OSSs) as much as possible
- Use of open standard interoperable interfaces where appropriate and practical
- Design and/or procurement of new OSSs consistent with TMN architecture principles and concepts
- OSSs built on specified/approved computing platforms
- Separation of OSS user, processing and data layer concerns
- Rapid service fulfillment business processes
- Corporate data as an asset and information management
- Proactive maintenance via performance monitoring, network event correlation
- Reporting to customers, and integration with maintenance and repair processes
- Electronic communications interfaces to other carriers and customers to support electronic commerce, and
- Integrated customer contact and customer care services.

6.4.2. VOP Network Architecture, Services, and Technologies Needed to Support the Business

VOP network architecture alternatives, available services, and deployable technologies are addressed in the previous sections of this SR. Characterizing the VOP network architecture, services, and technologies that will be used to realize the business goals and strategy are key inputs in the design of an operations and management architecture.

6.4.3. TMN Architecture for VOP Networks

As mentioned above, the ITU-T recommended TMN architecture is proposed as the operations and management framework for VOP networks. Although the regional and international standards bodies are just beginning to address operations and management

for VOP networks, existing generic specifications like Bellcore GR-2869-CORE and ITU-T Recommendations M.3010 and M.3400 can be applied to VOP network operations and management.

In the following subsections, the TMN architectural viewpoints, i.e., functional, information, and physical will be explained; and it will shown how this framework can be used to structure an operations and management solution for Voice Over Packet (VOP) networks.

6.4.4. Functions, Operations Process Scenarios, and Data

6.4.4.1. Functional Architecture

The TMN functional architecture addresses two dimensions, i.e., logical layering and management functional areas/groupings. The first dimension defines five logical layers, i.e., the TMN Logical Layer Architecture (LLA) [M.3010]. Each layer encompasses functions that provide a specific type of management view or level of abstraction to other functions in the same or other layers. The five logical layers and their applicability to VOP operations and management are as follows.

- *Business Management Layer (BML)*

  Contains the functions used at higher management levels within the organization, e.g., goal setting, finance, and budgeting. VOP planning and product definition activities are logically associated with this layer, as are activities detailing agreements between jurisdictions.

- *Service Management Layer (SML)*

  Functions associated with this layer provide support for pre-order inquiry, service-order negotiation, billing, and trouble reporting. A VOP SP needs to decide whether customers can access the functions of the layer through a provider's service representative or by means of automated, self-service mechanisms (e.g., Web-based Customer Care Call Centers). Specialized support capabilities can be established for specific groups such as residential customers, business customers, etc.

- *Network Management Layer (NML)*

  *P*rovides information about network topology and connectivity, and network reserve availability, performance, usage, and outages. This layer also supports control and coordination of the network by providing a global end-to-end view of the network elements and physical transmission links that make up the VOP network. It also facilitates configuring and monitoring network equipment and transmission facilities, and managing network-activation and restoral activities. Given the different types and distribution of NEs that make up a VOP network, the level of cross-domain integration is a key design decision for SPs.

- *Element Management Layer (EML)*

  Facilitates configuring network elements both by sending messages to them and by recording updates from their software memory. This layer stores information about network performance and outages that are collected and reported by the network elements, as well as information about the amount of bandwidth currently available in the network. It manages the switching, signaling and control, and transport

functions necessary to deliver voice over packet-based data networks. Functions in the element management layer can also aggregate portions of the network — subnetwork domains — that may require specialized knowledge to operate, such as supplier-specific NEs or a technology-specific feature.

- *Network Element Layer (NEL)*

  Contains the operations and management functions that reside in VOP NEs. "Operations and Management Agents" collect and disseminate information about the ongoing state of network elements by gathering data from NE plug-in components, transport interfaces, etc. The functionality to respond to configuration instructions (subscriber line service activation) and to operate within a local view of the configuration is in this layer.

The second dimension in the functional architecture is the TMN Management Functional Areas (MFAs) of Fault, Configuration, Performance, Accounting, and Security, and functional groupings within each of the MFAs.

Together, the five logical layers and the five management functional areas form a matrix into which management functions may be assigned (see Figure 6-1). A decomposition of these TMN Logical Layers and Management Functional Areas/Groupings is defined in Bellcore GR-2869-CORE. Together Bellcore GR-2869-CORE and ITU-T M.3400 also define the Management Application Functions (MAFs) that reside in each cell of this matrix (see Figure 6-2). This functional "decomposition" serves as a template for describing and organizing functions and for studying management activities to identify each function performed and the data and connectivity needed to accomplish that function. A description of some of the key relevant processes and functions for VOP service, network and system management is given in Section 6.2.

Further differentiation may be assigned as necessary to reflect how operations processes work (see Section 6.2) and what data flows (see Section 6.3) may be needed to support the operations and management of VOP networks.

	Configuration Management	Performance Management	Fault Management	Accounting Management	Security Management
Business Management Layer					
Service Management Layer					
Network Management Layer					
Element Management Layer					
Element Layer					

Figure 6-1 The TMN Functional Matrix

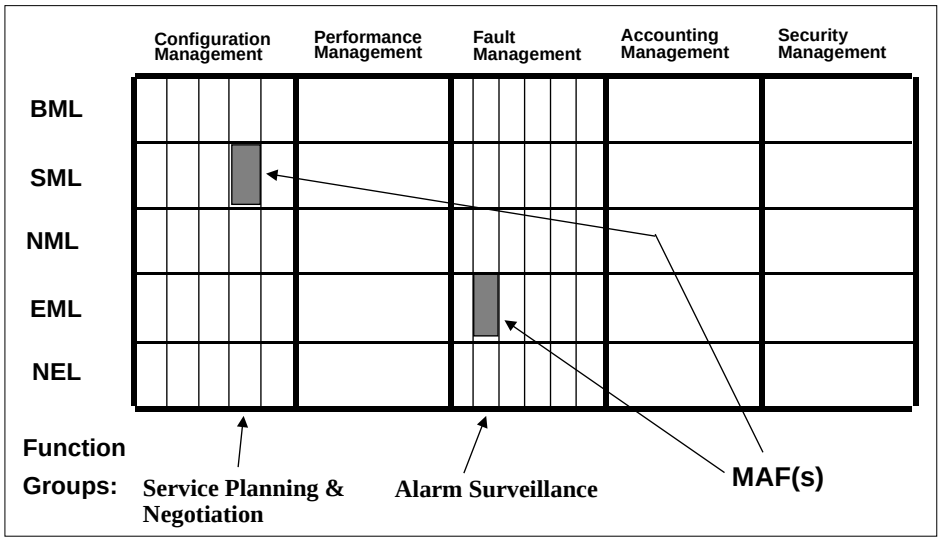

Figure 6-2 TMN Management Application Functions

6.4.4.2. Operations Process Scenarios

The TMN matrix is a useful way to describe and categorize management functions, but it is not a requirement for how functions are physically placed in systems. It's an organized framework — part of an effort to understand the intricacies and future growth requirements of a complex system of systems. The identification of management functions through decomposition doesn't always imply that replacement software and hardware systems will fit into neat little categorization cells. The management processes that involve the management functions are conceptually viewed as a matrix to aid in understanding relationships, but in practice, processes may have several functions, and functions may be associated with multiple processes.

Operations process scenarios are the means by which an entire end-to-end process, such as establishing new service, is analyzed and specified. During an operations process analysis, it's possible to see when a function often interacts with another function. The function affinities that are identified may lead to further optimization of the network. Perhaps functions with strong affinities could be best served by residing on the same computer system, or by being part of the same network management application. By reviewing the input and output interactions that the affinity group has with other groups and availability/constraints where data is stewarded, detailed data/information models and interface definitions can be identified.

As an example, typical business processes for VOP needs to address Service Fulfillment, Service Assurance, and Billing (see Section 6.2). To fully define these processes, operations process scenarios need to be defined. The Service Fulfillment process flows for VOP networks may need to address a variety of scenarios such as the following:

- Service availability inquiry
- New subscriber line connection, purchased Residential Access Gateway, new Telephone Number (TN) assigned

- New subscriber line connection, Residential Access Gateway installed by Telco, new Telephone Number (TN) assigned
- New subscriber line connection, Residential Access Gateway installed by Telco, Local Number Portability (LNP)
- Disconnect of voice telephony service, with and without Residential Access Gateway retrieval, with and without LNP
- Cancellation of order
- Change of order
- Change in subscriber line feature set.

6.4.4.3. Data/Information Architecture

The data/information architecture includes the definition of data types/entities, their characteristics, relationships, and behavior, etc. The operations process flows assist in determining information (i.e., input/output) interactions and interaction paradigms between functions, data stewardship, data location, redundancy and consistency management, and levels of data abstraction that may be needed for operations and management of VOP networks. Furthermore, VOP NEs and management systems may already support certain industry-standard or vendor-specified operations interfaces that may also dictate or constrain the data/information architecture design (see Section 6.3).

The point here is that even though the functions associated with a process flow may be the same, different data items may be required. For example, in Ordering Handling, a pre-order inquiry that lists service availability on a VOP network may need to distinguish what types of service are available, e.g., Plain Old Telephone Services (POTS), Hunt Group, PBX-DID, Centrex, etc. For each of these service types different features may be supported, e.g., custom-calling features, dialing plans, E911, hunting types, group features, etc.

Data assignments, for example, may also occur at different times during the process flow. For example, a Customer Gateway purchased at a department store may get registered for pertinent information (such as equipment serial number and MAC address) at the time and place of the sale. Whereas, a Customer Gateway that is installed on the customer premise may not be known until the technician installs and tests the device from an inventory on his or her truck.

6.4.4.4. The Target Functional, Information, and Operations Scenario Views

By analyzing the operations and management functions and data definitions and "threading them together" to support the customer's business process requirements, the target functional architecture, information architecture, and operations process scenarios can be defined and validated for completeness and sufficiency. Based on the results of this analysis, it may be necessary to revise the functions and data, client business processes, or the decision to deploy. See Figure 6-3 for an illustration of this methodology. Note that this is an iterative analysis and design exercise.

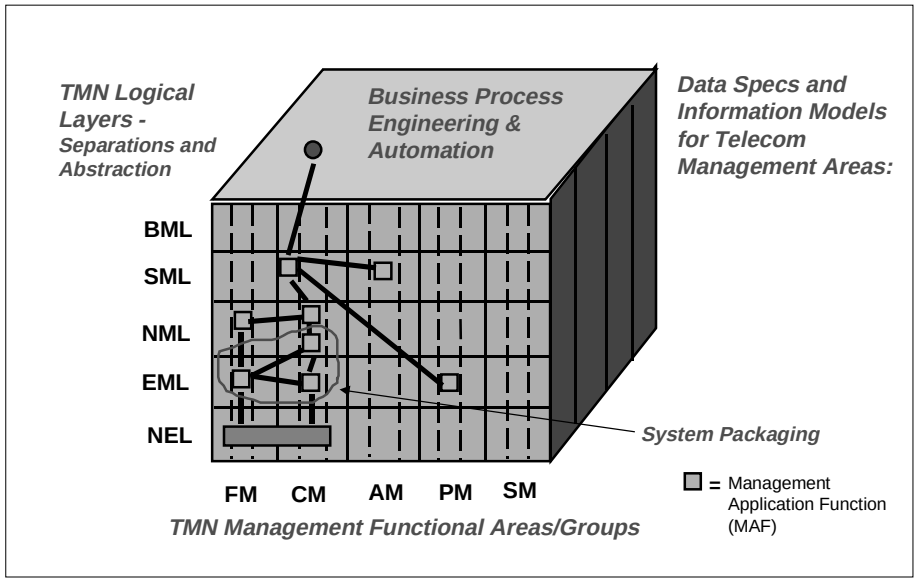

Figure 6-3 Bellcore TMN Analysis/Design Methodology

6.4.5. Management Domains

Another aspect in designing an operations and management solution for VOP network is to identify the management domain requirements and constraints. Example management domains include the following:

- Administrative
  - Types of Customers (e.g., residential, small business, large business)
  - Other Network Operators
  - Other Service Providers
  - Wholesalers/Retailers
  - Suppliers.
- Geographic layouts
- Organizational/Work Centers
- Functional domains (e.g., memory administration, network traffic management, etc.)
- Supplier-specific NE and EMS domains
- Network technology-specific domains
- Layer Network Domains (Voice Signaling and Control, IP, ATM, SONET, WDM, etc.).
- Network partitioning (e.g., networks, subnetworks, NEs)
- Interdomain management.

6.4.6. Physical Architecture Framework and Packaging

Given the target functional architecture, information architecture, operations scenarios, and management domains, the physical architectural alternatives can be determined. The physical architecture includes the packaging of functions, data, and system interfaces to be supported by Operations Support Systems (OSSs), Work Stations (WSs), Network Elements (NEs), mediation devices, Q-adapters, interconnection gateways, and/or work centers. Considerations typically include the identification of functions and data packaging, such as the following:

- Functional and data components to be supported by multi-supplier NEs
- Functional and data components to be supported by supplier Element Management Systems (EMSs)
- Functional and data components to be packaged into higher tier OSSs, e.g., Network Management Systems (NMS) and Service Management Systems (SMSs)
- Functional and data components to be packaged into Work Stations, (WSs), mediation devices, Q-adapters, and gateway components
- Use of common computing platforms, databases, Middleware, etc.
- Use of existing/deployed OSSs (may require migration strategy to supplement or surround)
- Use of off-the-shelf OSSs or OSS applications, as is
- Use of off-the-shelf OSSs or OSS applications, with customization
- Specification and procurement/development of new OSSs.

6.4.7. System Interfaces, Adaptation and Mediation

Another aspect of the physical architecture is the system interfaces to be supported. A common goal of many Service Providers (SPs) and Network Operators (NOs) is the use of open, standard, interoperable interfaces. This strategy provides SPs and NOs with the option to buy NEs and OSSs from multiple suppliers and eases the procurement and system integration issues. As illustrated in the network architecture section of this SR, however, VOP networks can be constructed of many different types of NEs, e.g., CPE, access network technologies, core transport network technologies, signaling and control servers, other general purpose computing servers, edge devices/gateways. The operations interfaces to these NEs in some cases are being designed by industry standards groups/forums and include protocols such as SNMP, FTP, CMIP, CORBA IIOP, Web, etc., while others are still being specified by the suppliers themselves.

Since a system interface needs to interoperate between communicating entities, operations interfaces for VOP networks need to be identified and specified, consistent with the information architecture. A good system interface specification methodology should be adopted for VOP network operations and management. This methodology should make use of emerging industry agreements on the use of protocol-neutral information modeling techniques where it makes sense, e.g., to capture new operations interfaces that need to be defined but protocol selections have not been made yet. A good example of this is local switching system features for voice services. A number of switched service feature memory administration interface specifications exist and the

information content of these interface specifications (i.e., their underlying information models) can be reused for VOP subscriber line service activation operations interfaces.

If industry standard operations interface specifications are not available for VOP NEs and management systems, then near-term interim specifications may need to be considered and mutually agreed to. The TMN physical architecture and implementation considerations recommendations do identify a few components, namely mediation devices, protocol adapters, and gateways, that can be employed to map (mediate or adapt) between different interface types and versions of interfaces. In many cases though, the interface mapping specification needs to be performed with good engineering judgement, since the translations between communication paradigms and data/information models are not necessarily defined by automated algorithms.

7. Evolution to NGN

7.1. Migration of PSTN/ISDN Circuit-Switched Networks to VOP

There are many technical and economic benefits associated with migration of current PSTN/ISDN circuit-switched networks to VOP networks, and numerous evolution paths are possible. This section describes an initial opportunity of using VOP as the backbone transport network (VOP/ATM Trunking) for PSTN/ISDN circuit-switched networks. The concept of VOP/ATM Trunking for PSTN/ISDN circuit-switched networks is currently being studied in the ITU-T, ATM Forum, and T1S1.

Circuit-switched network service providers can use VOP in their backbone network as a unified transport mechanism for their different networks (e.g., PSTN/ISDN, Internet, Wireless, Frame Relay, etc.) and services, since VOP technology is designed for and is capable of supporting voice, data, and video in a single switching environment. Figure 7-1 illustrates an initial circuit-switched/VOP network architecture consisting of PSTN/ISDN circuit-switched exchanges connected via a VOP-based backbone. In this architecture, the InterWorking Unit (IWU) is responsible for interworking voice channels between the TDM and VOP domains. In addition, the IWU has capabilities similar to existing circuit-switched tandem exchanges.

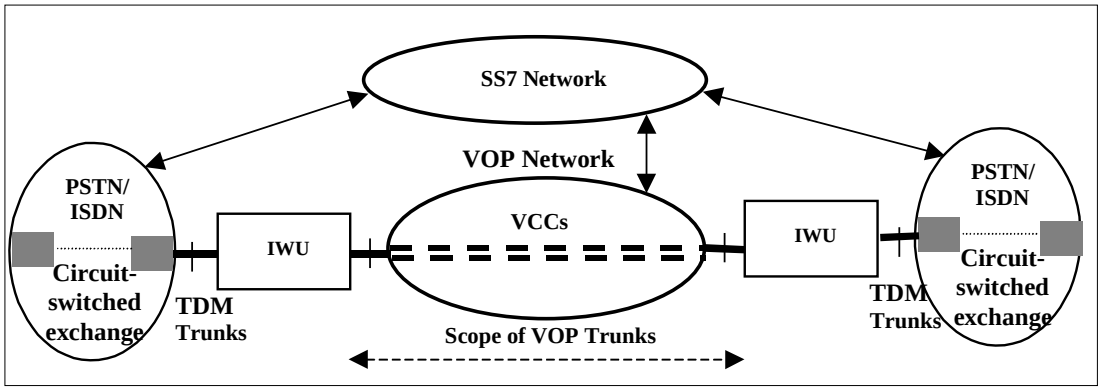

Figure 7-1 VOP Trunks

Unlike IP, ATM has a Quality of Service (QoS) capability to support latency and timing sensitive voice traffic. Therefore, the initial network evolution path (i.e., for the PSTN/ISDN service migration) and network interconnection configuration would most likely support VOP/ATM trunking in the backbone network for public voice services. In addition, the same VOP backbone network providing PSTN/ISDN services can potentially carry IP traffic, as well as, internet traffic off-loaded from the existing PSTN/ISDN. This unified transport mechanism may allow service providers to derive additional benefits from their investment in VOP.

The services provided by a PSTN/ISDN must be supported under any VOP transport infrastructure. This may not be completely possible with some of the existing VOP infrastructures. Beyond simple call set-up and release, VOP networks do not provide any

intelligent services, e.g., 800 service, number translation, number portability, nor the suite of supplementary services provided by the PSTN/ISDN. However, it is expected that the same set of voice services will be offered independent of the underlying switching and transport infrastructure. The VOP-based network architecture illustrated in Figure 7-1 may be viewed as an initial step in supporting basic PSTN/ISDN services.

The next evolutionary step is VOP support for supplementary services. As illustrated in Figure 7-2, the service applications for supplementary services may be supported as part of the VOP infrastructure or may reside outside the VOP infrastructure. In this architecture, the SA may be based on existing Intelligent Network Service Control Points (SCPs), or it may be based on client-server technology in a services node adjunct to an IWU. An SCP approach may facilitate seamless operation of supplementary services within the PSTN/ISDN/VOP-based network. Whereas, a services node adjunct approach may facilitate interoperation with IP-based applications. Both alternatives support the separation of connection control intelligence from switching and transport resources of the network and provide a foundation for the migration scenarios described in the following sections.

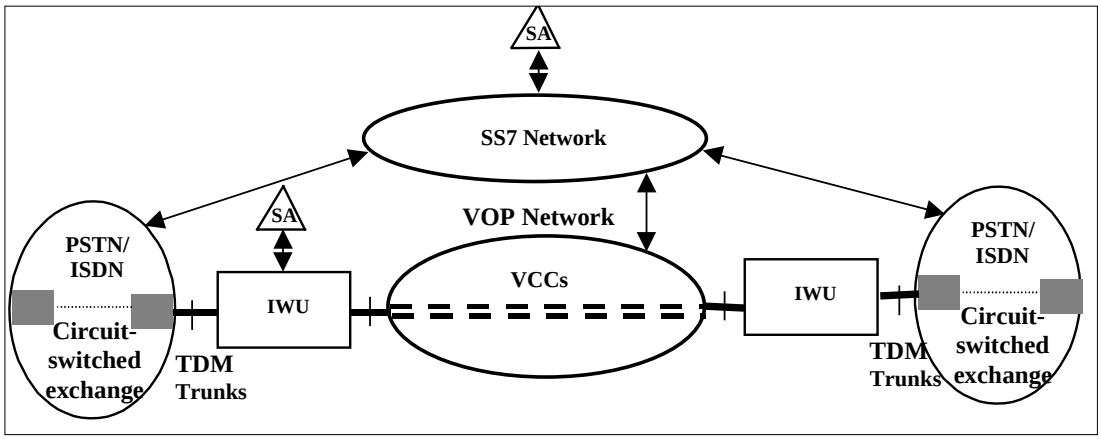

Figure 7-2 VOP Support for Supplementary Services

The above architecture could be extended to support interconnection to other VOP based networks and could be extended to the access network to support residential and customer gateway as described in previous sections.

7.2. Migration from First Generation IP Voice Solutions to VOP

This section discusses the migration from H323-based solutions (and other initial implementations) to the VOP network discussed in the SR. First, the evolution of early VOP networks is discussed. Then, the evolution of network elements is discussed.

7.2.1. Network Migration

Initial public voice over IP networks use either proprietary technology or H.323. Some private networks deployed ATM or frame relay based voice networks. Public networks are using mostly single vendor solutions to ensure interoperability between H.323

gateways, gatekeepers and clients. SIP products and deployment are expected in the near future.

When the VOP products become available, the initial VOIP networks will migrate to an architecture with a core of MGCP-based VOP network elements and edge network elements consisting of gateways to the PSTN; MGCP-based customer/access gateways and H.323/SIP interfaces (see Figure 7-3). Interworking with H.323 customer equipment will be required due the deployment and widespread availability of H.323 software and devices. Because of their relative simplicity, the use of MGCP-enabled devices is anticipated to increase quickly once they are available.

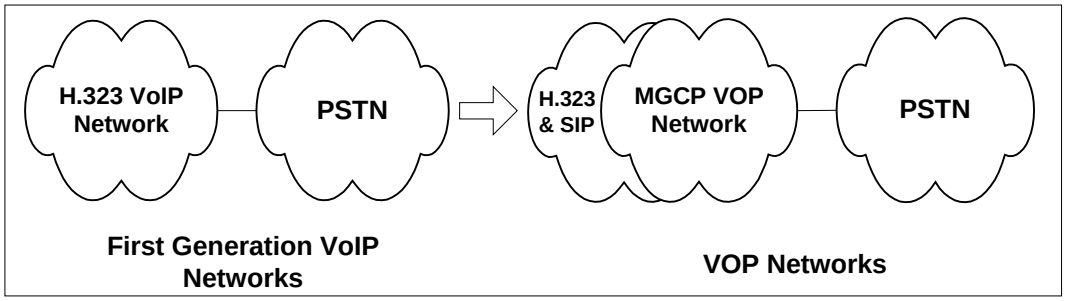

Figure 7-3 Migration of VOIP Networks

National and international network development is hampered by the lack of interoperability of proprietary solutions. Even H.323 implementations are inconsistent and hamper the interconnection of networks of different operators. This has led to the present situation where the interconnection of VOIP networks is often based on a single vendor's equipment implementation. The result of this is that carriers are closely tied to the other carriers' plans and business viability. VOP networks will be based on a relatively simpler technology; they will be more scaleable and VOP networks will be based on a set of carrier-grade definitions. Because of these advantages, interoperability will be improved and network operators will accelerate the interconnection of VOP networks. Thus, internetworks based on bilateral implementation agreements will migrate to networks more typical of the telecommunications industry and internets.

7.2.2. Network Element Migration

This section discusses the likely roles that today's VOIP network elements will assume in a VOP network in order to realize the networks discussed in the previous section. The migration of these network elements in no way precludes the offering of new VOP network elements based on the criteria discussed in this document. The growth in new carrier-class networks will likely be based on VOP network elements, as they become available. Figure 7-4 shows the situation today and for the near future.

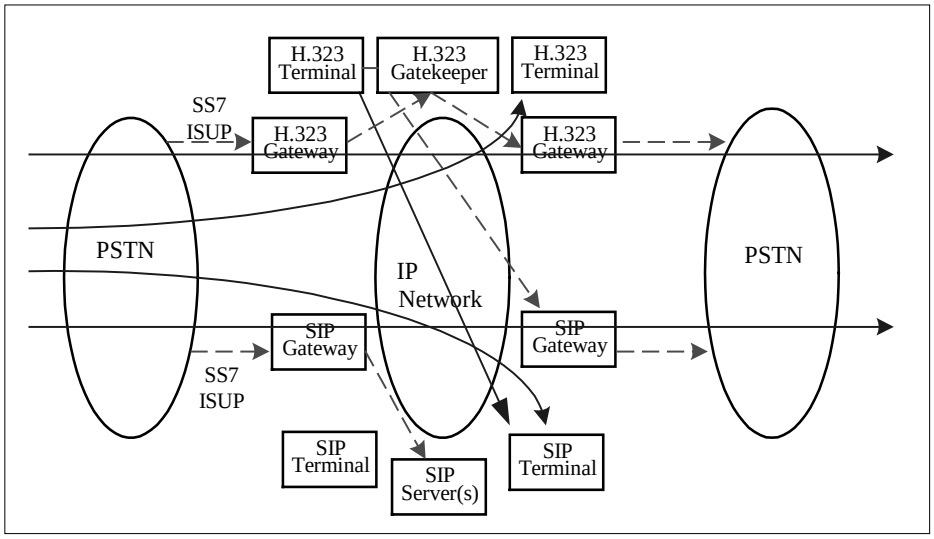

Figure 7-4 Initial VOIP Networks

- *Client Devices*

  An H.323 or SIP client can be controlled directly by a VOP network offering interworking services. So there is no inherent need for these devices to change. However, as a product class, they can be expected to migrate to a MGCP-based client because of the relative simplicity of the requirements on the client device. Such devices should be lower cost and have lower power requirements, which is especially important in the case of mobile devices.

- *Proprietary Gateways*

  This class of products provides VOIP solutions based on proprietary approaches to voice call control and voice transport. The use of IP mechanisms is nearly always standard. These products have already been migrating to H.323 standards and the remaining proprietary systems can be expected to move directly to VOP standards.

- *Standards-Based Gateways*

  Gateways based on standards, such as H.323 and SIP, will migrate to products offering VOP and H.323/SIP interworking. Interworking allows the VOP network to appear as a H.323 gateway to an H.323 device. For H.323 gateways already deployed, this would offer a graceful upgrade path. Alternatively, existing H.323 gateways could home directly on a VOP gateway that would provide the interworking function.

- *Voice Call Servers*

  Voice servers, such as H.323 gatekeepers, will assume the function of Call Connection Agents (or other control agent functions) in a VOP network. Because voice servers are usually general purpose computing servers, they can more easily change to a new control logic.

Figure 7-5 presents one instance of an VOP network based on the evolved elements.

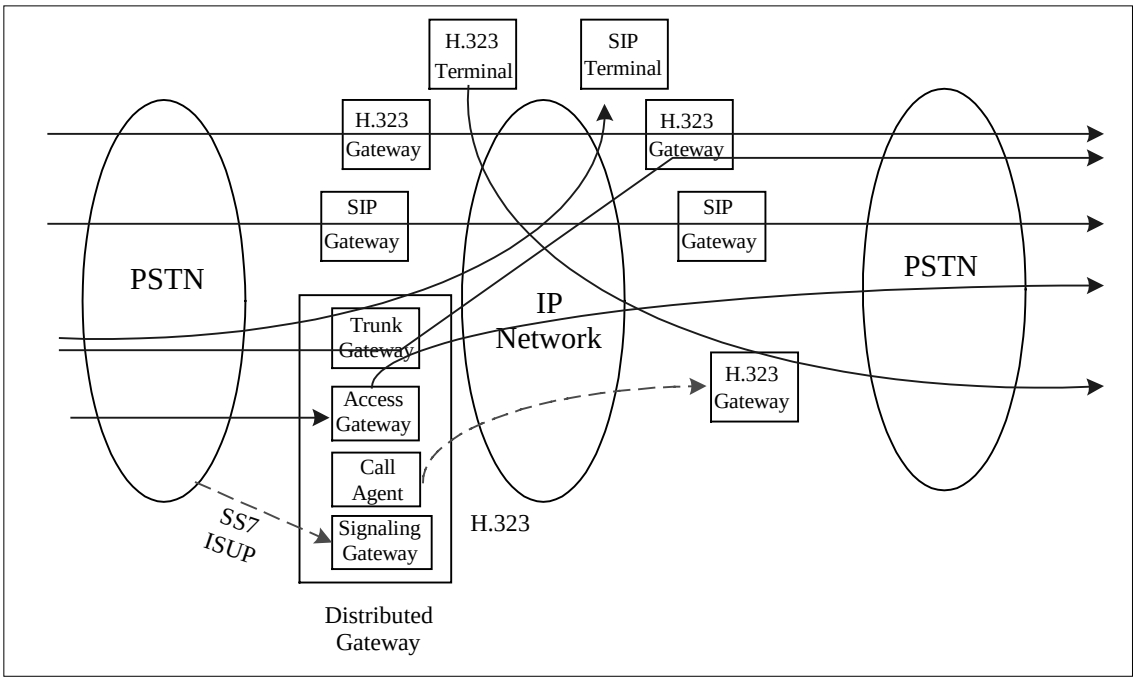

Figure 7-5 An Example VOP Network

7.3. Migration from Wireless Networks to VOP

This section describes potential migration scenarios for mobile networks (e.g., cellular, PCS, and satellite networks) to incorporate VOP technologies. Two major threads are presented, one for migration in the backbone network and one for migration in the distribution network. These representative scenarios could in real networks be pursued simultaneously, resulting in a wide variety of implementation configurations which are hybrids and offshoots of the ones presented here. These scenarios are equally applicable to networks based on GSM architecture and to networks based on ANSI 41 architecture (both CDMA and TDMA). We believe that emerging 3rd Generation (3G) networks, and IMT-2000 networks will incorporate some of the same concepts presented here.

In the present day mobile networks, operators may find themselves interconnecting with voice networks which are either circuit switched or packet based, as depicted in Figure 7-6.

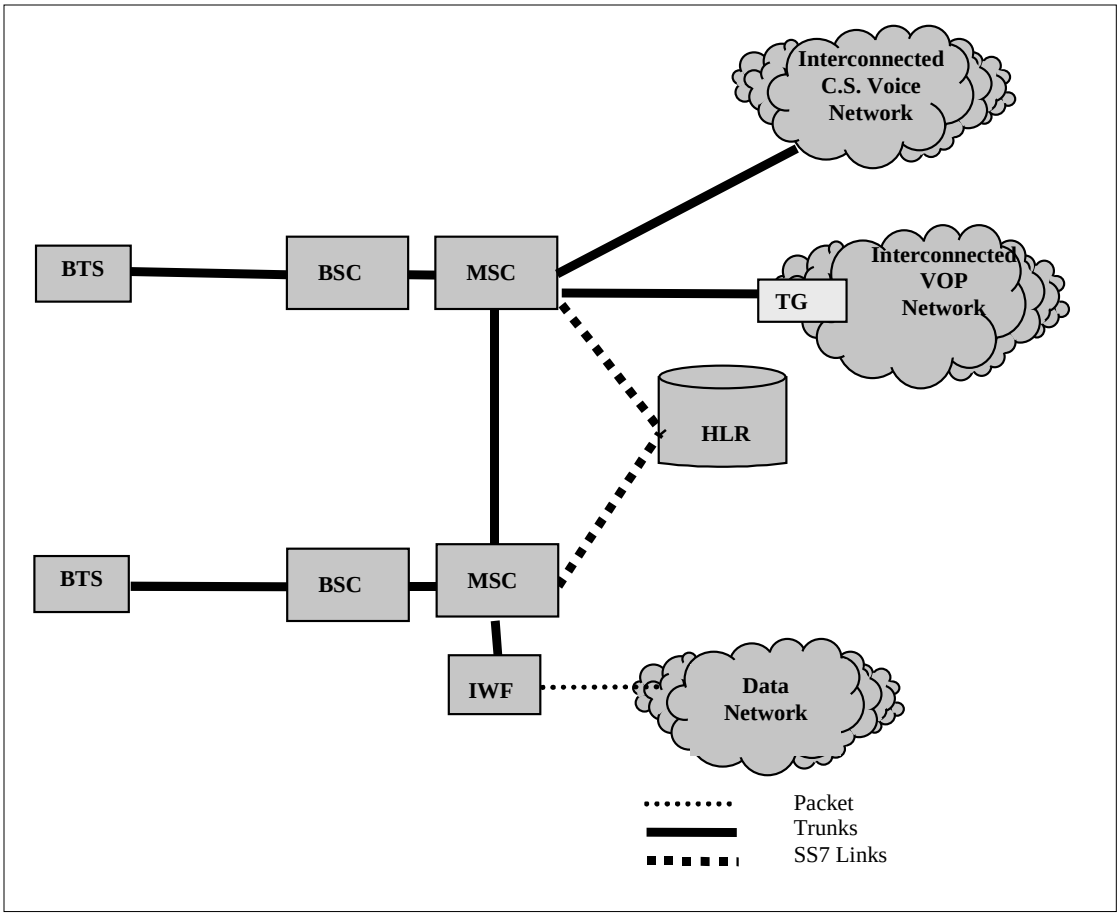

Figure 7-6 Current Mobile Network Architecture

This difference would not be visible to the mobile network. However, as VOP networks become a force in the marketplace, a mobile network could consider as its first move toward packet based architecture the incorporation of Trunk Gateways within the mobile network, as depicted in Figure 7-7.

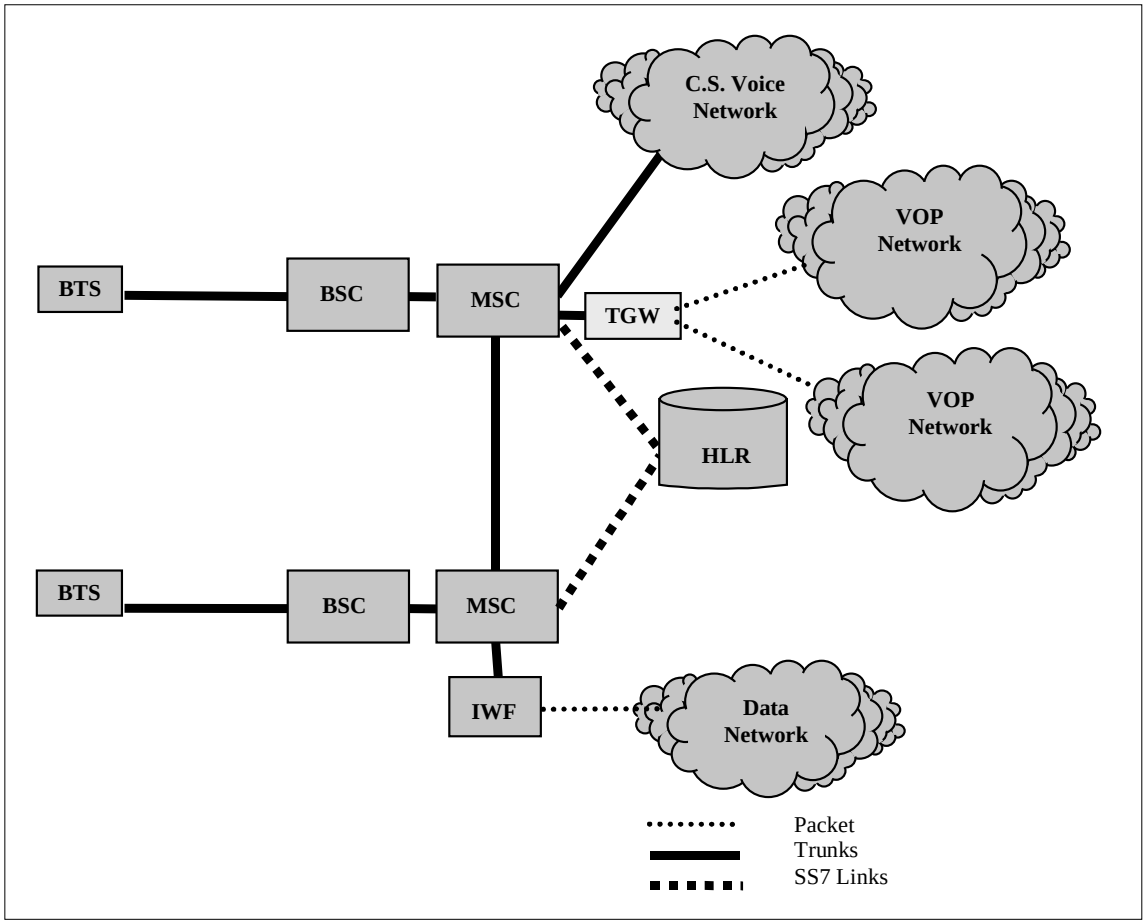

Figure 7-7 Shared Trunk Gateway

This move could have the following benefits to the mobile operator:

1. It could reduce the cost to the VOP operator to interconnect with the mobile network by allowing the VOP network to interconnect in packet mode. The cost of the TGW could be spread across multiple interconnected VOP networks. Marketing could position the mobile network as “Internet Telephony friendly” and attempt to stimulate traffic from the VOP network by offering reduced rates within communities of interest.
2. It would allow the mobile operator to develop operating knowledge of VOP technology, thus positioning the operator to evaluate the technology and prepare for further introduction of the new technologies in the future.

An additional step which is synergistic with the above, and may happen at the same time, would be to use VOP technology for voice calls trunked between MSCs, as depicted in Figure 7-8.

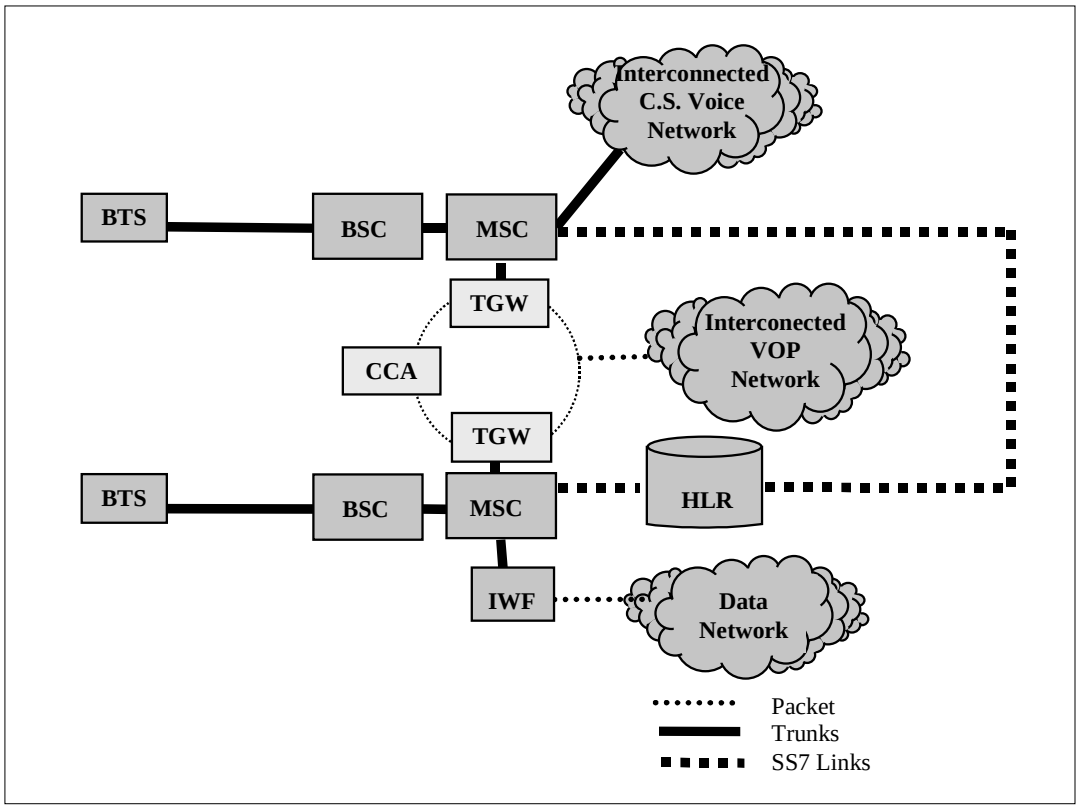

Figure 7-8 VOP Backbone

In this scenario, the mobile network incorporates and internal VOP network using multiple TGWs, controlled by one or more Call Connection Agents. The Call Connection Agent in this scenario is not particularly wireless-aware. An SS7 Gateway capable of ISUP signaling may also be required if the MSCs rely on SS7, as many do today. Economic benefits could be realized on high-usage routes by increasing transport efficiency from packet multiplexing gains. Further efficiency could be realized by consolidating operations with broadband packet-mode inter-MSC transport required in CDMA networks for inter-MSC soft handoff.

The next step in the backbone network could be the addition of mobility-aware functions in the Call Connection Agent to take on the duties of the Gateway MSC (GMSC), as depicted in Figure 7-9.

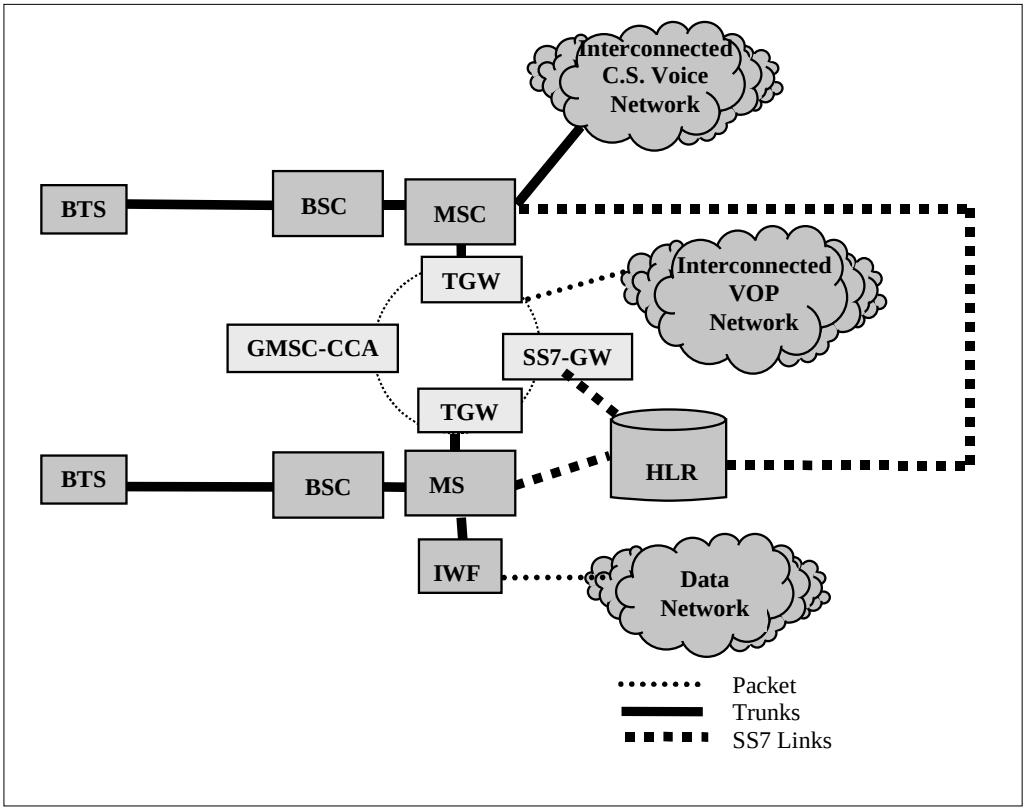

Figure 7-9 VOP Backbone with Efficient Routing

The GMSC serves as a point of concentration of inbound traffic destined for mobile subscribers. It can query the HLR for current location, and route more efficiently to the current serving MSC of the mobile subscriber, rather than having the call first go to that subscriber's Home MSC and then be forwarded. This function could easily be incorporated into a GMSC-capable Call Connection Agent. The SS7 Gateway in this scenario would also be handling TCAP signaling to carry MAP messages (either ANSI 41 or GSM).

The second series of scenarios focuses on the transport of traffic between the BTS, BSC, and MSC. Increasing voice and data traffic will drive upgrades of BTS, creating an opportunity to add new packet-based technologies economically. Data traffic from mobile users typically traverses the MSC to reach an IWF. A first step (already implemented in some systems) in migrating the distribution network to packet would be to interpose an Access Server function between the BTS and MSC to detect data traffic and route it directly to the IWF in packet mode, as depicted in Figure 7-10.

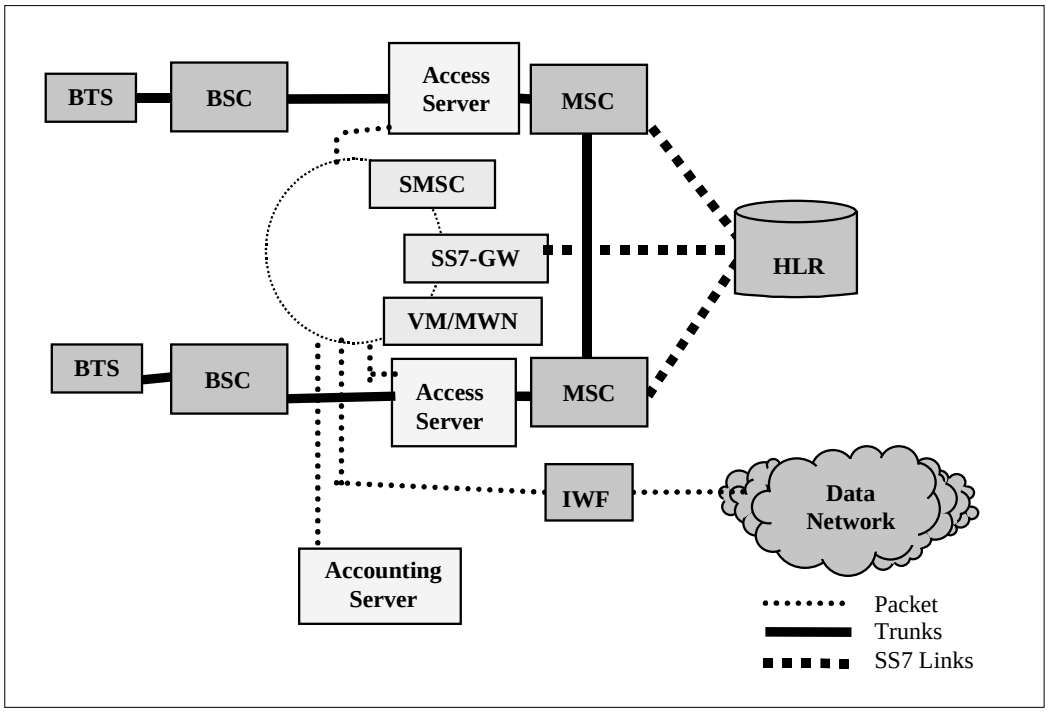

Figure 7-10 MSC Data Offload

This function would initially be transparent to voice traffic. To minimize impact on the MSC, it could also include deployment of an Accounting Server; alternatively, the MSC could receive signaling information regarding the data traffic and generate accounting data itself.

A further step in this direction would be to offload not only user data traffic, but some signaling traffic which need not be handled by the MSC in support of voice calls. Examples include signaling from the Short Message Service Center (SMSC) and Voice Mail System for Message Waiting Notification (VM/MWN). This incremental step provides the driver for further upgrading the packet environment to interface to SS7 and the MAP protocol.

The next scenario is to upgrade the packet side of the distribution architecture to carry voice channels toward the MSC, as depicted in Figure 7-11.

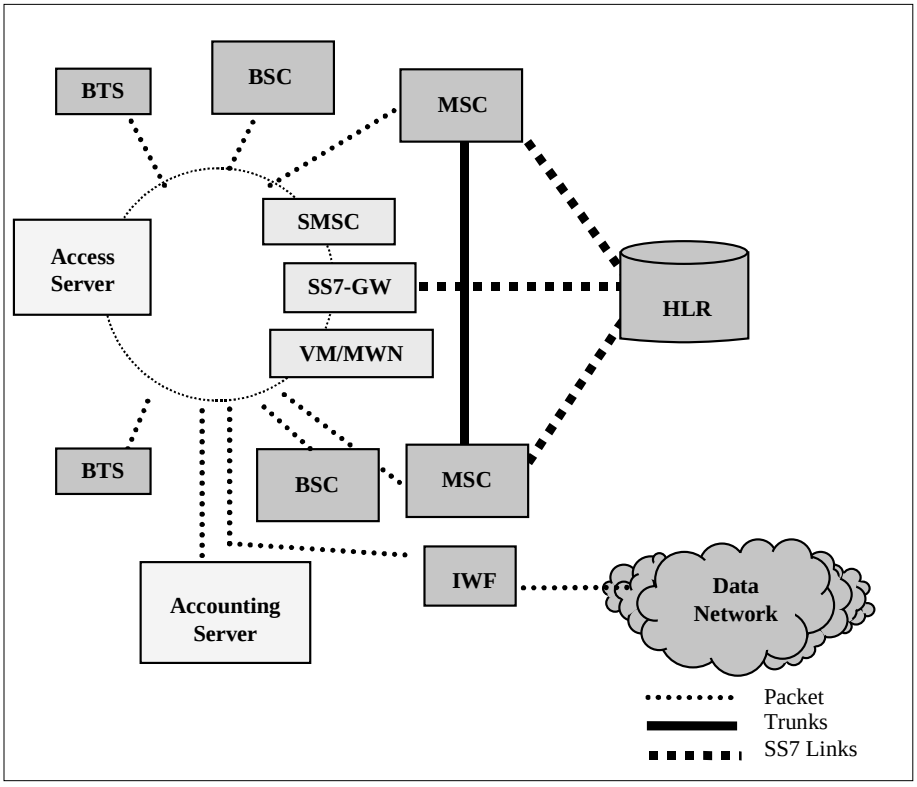

Figure 7-11 Broadband Distribution Network

The access server would gain the ability to selectively route voice channels to the packet environment. The MSC is shown here with a packet mode interface to permit the entire backhaul network to be converted to packet. This interface could be dedicated to the MSC, or shared among several MSCs on the internal packet network. The economic drivers for this could include capacity expansion which may be cheaper on the packet architecture. In particular, backhaul facilities expenses are significant, and can be reduced by moving to broadband transport technology.

Finally, the migration to a VOP MSC can begin by the introduction of the MSC Call Connection Agent as depicted in Figure 7-12.

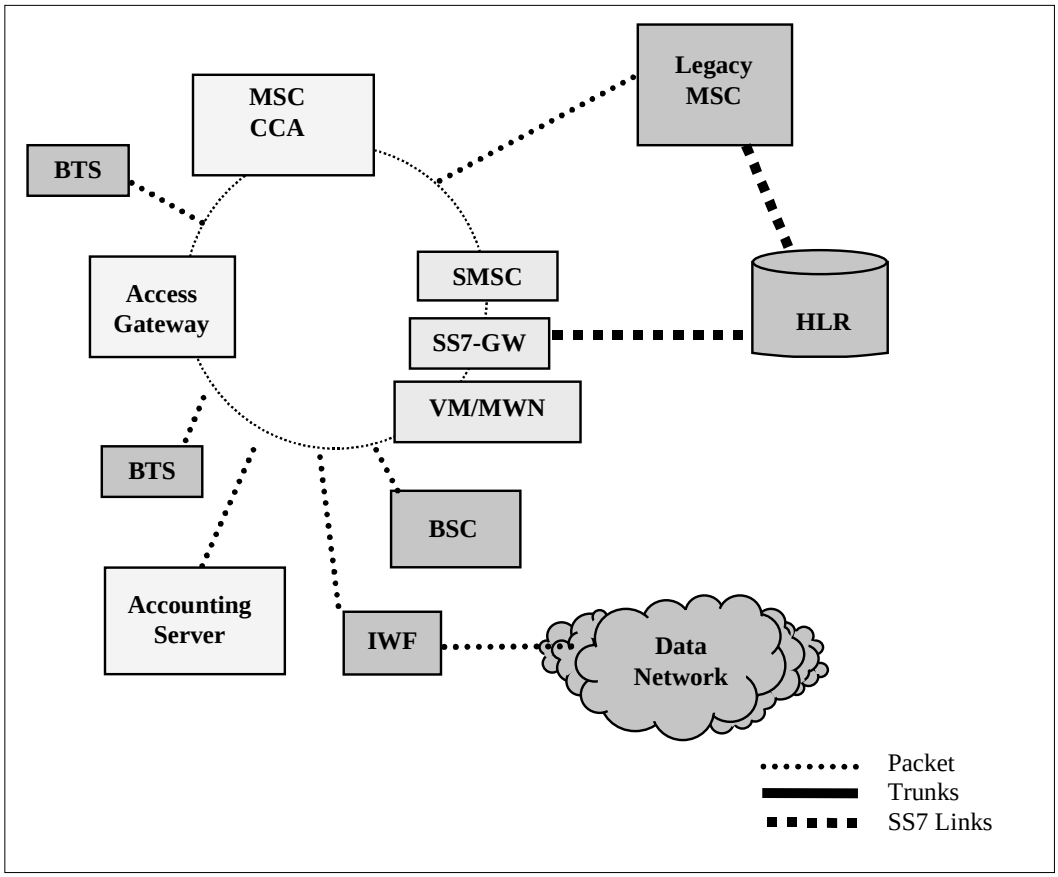

Figure 7-12 MSC Call Agent

In this figure, the Access Server has now become an Access Gateway, indicating its added functionality under the control of the MSC Call Connection Agent. The introduction of the MSC Call Connection Agent does not immediately obsolete the circuit-switched MSC. Rather, the Access Gateway retains the ability to selectively route voice calls to either the packet or the circuit call control environment. The Access Gateway could implement a variety of algorithms for choosing which calls to handle, such as service-based, source or destination-based, or load-balancing. The stage is now set for introduction of new service functionality in the VOP environment, and a continued migration toward data and multi-media services.

7.4. Evolution of VOP Networks to Next Generation Networks

As discussed earlier in Section 3.5, a Next Generation Network (NGN) is defined to be a packet-based network that employs new control, management, and signaling techniques to provide *all* types of services, from basic, narrowband voice telephony services to advanced broadband, multi-media services. All traffic is handled as data by a packet-switching backbone, such as an IP network, or an ATM network, or both. Within a NGN, service control and network resource control functionalities are based on an open, modular architecture that uses distributed object computing techniques. Connection

control intelligence, for example, is separate from the switching and transport resources of the network. And service feature intelligence is logically separate from resource control. This control architecture will promote innovation, enable new services and revenue streams, enable third-party participation in service execution, and reduce management costs and time to market.

A VOP network, in contrast, is assumed in this report to be limited to the support of traditional, narrowband [8] voice and data services. However, because both types of networks are packet-based, it follows that a VOP network could evolve to a NGN and thereby support a broader range of services and service features.

From an access, transport, and switching perspective, evolving a VOP network to a NGN will involve the following:

- Enhancing the access portion of the network to efficiently support all services (both narrowband and broadband) over integrated interfaces to customers' premises
- Augmenting the core transport and switching infrastructure and the access technologies to support broadband bandwidths.

These enhancements will not be as dramatic as the changes that will need to occur in the service control aspects of the network.

From a service control perspective, evolving a VOP network to a NGN will involve the following:

- Enhancing the service control infrastructure to support increasingly complicated services and service sessions (e.g., multi-party sessions and multiple service sessions per access session)
- Increasing the modularity of the service control infrastructure to, for example, enable third-party involvement in the execution of services.

These service control changes are discussed in greater detail in the following paragraphs.

7.4.1. Support of Complex Sessions

In a NGN, the service control architecture is assumed to be able to support complex, processing-intensive services. These services will require the network to support service session models that are much more complicated than a call model that has an originating leg and a terminating leg. The service architecture defined by the Telecommunications Information Networking Architecture Consortium (TINA-C) is an example of the kind of advanced service control paradigm that a NGN will need to employ.

According to the TINA-C architecture, users of the network engage in *Access Sessions* which support functions such as authentication of the user and negotiation of terminal parameters. Within the context of an Access Session, a user may engage in one or more *Service Sessions* with other users or other service providers. These Service Sessions may be initiated, suspended, resumed, or terminated, all without affecting the Access Session. As part of a Service Session, there may be a need for telecommunications services which will be invoked as a *Communications Session*.

[8] Users may access a VOP network via a broadband technology such as cable modems over HFC systems.

A VOP network's Call Connection Agent function would need to evolve to support these different session types in order to provide the more advanced services that a NGN can.

7.4.2. Modular Architecture

In a NGN, service control, including connection control, will be logically separate from the underlying transport, routing, and switching functions of the network. Furthermore, service and resource control functionality will be modularized to promote reuse, enable smooth scaling, increase reliability through redundancy and physical distribution, and enable third-party service creation and execution. The service control architecture for VOP networks as described in this Special Report is also distributed and modular, but not as modular as might be required to support the reusability and scalability required of a NGN. Service functions and features need to be decomposed such that service components may be reused by many different services.

To achieve the desired modularity and openness, Next Generation service control functions will be more specialized, resulting in a greater number of different, re-usable application objects than in VOP network service control. For example, a Next Generation control architecture may consist of the following distinct functional groupings:

1. *Service Factory* – responsible for dynamically instantiating components (objects) to support service sessions.
2. *Session Management* – responsible for managing access, service, and communications sessions.
3. *Connectivity Management* – responsible for managing on-net to on-net and on-net to off-net connectivity across the underlying packet network (which may consist of multiple layer networks) and interworking gateways.
4. *Interworking Management* – responsible for managing interworking with the existing PSTN service architecture (e.g., via ISUP and TCAP). This includes control of lower layer gateway devices.
5. *Service Control/Support* – responsible for providing value-added capabilities to service sessions (e.g., supplementary features).
6. *Management Agent* – responsible for communicating fault, configuration, accounting, performance, and security information to management systems.

These functional groupings may be further decomposed into application components (objects) which can be reused by different services and session types. This NGN service control architecture is graphically depicted in Figure 7-13.

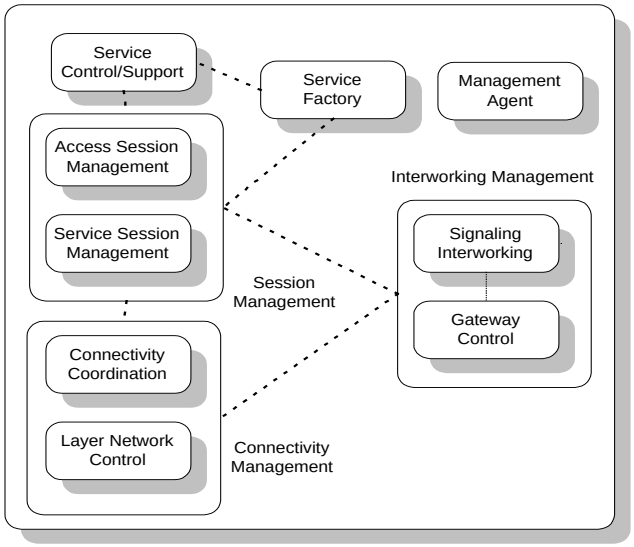

Figure 7-13 Next Generation Service Control Architecture

To achieve this level of modularity, the Call Connection Agent function of a VOP network would need to evolve so that Session Management functions could be separated from Connectivity Management functions. It would also need to support both Access Sessions and Service Sessions. Finally, it would need to separate these functions from Interworking Management functions, such as Signaling Interworking and Gateway Control.

At the same time, the Service Agent function of a VOP network would need to be enhanced to support Service Factory and Service Control functionality. As it is defined in this report, the Service Agent function simply mediates between the Call Connection Agent and traditional SCPs by sending and receiving TCAP messages to/from SCPs in support of vertical services. In the future, services are likely to involve processing, not just data base queries, hence the need for Service Control functionality.

Appendix A: Features and Abilities

This section lists and describes the various features and abilities being addressed in this report. Some feature definitions were taken from SR-504.

A.1. General Features

- *Access to Toll-Free Numbers*

  Ability to dial Toll-Free numbers.

- *Access to 900 and Other Information Services*

  Ability to dial "900" and other information services. Ability to arrange for the network to block subsequent attempts to access these services.

- *Automated Alternate Billing and Pre-Pay Services*

  The ability to offer, on a mechanized basis, alternate billing options to the caller. Options include calling card, pre-pay cards, collect, and third-number billing.

- *Call Completion*

  Ability to dial any number in the World Zone Numbering Plan and be connected to the called party or receive other appropriate terminating treatment (e.g., busy, forward to voice mail, etc.)

- *Dial Tone*

  A signal to the end user that the network is ready to process their service request.

- *Directory Assistance (411 or Equivalent)*

  Ability to dial "411" or similar code to receive assistance to obtain a telephone number not included in the local directory, or to obtain a telephone number for those customers unable or unwilling to look it up in that directory.

- *Feature Group D*

  Presubscription to carrier for intraLATA toll, long distance, and international calls.

- *Local Number Portability*

  If an end user changes their local exchange service provider, they can keep their telephone number. *Note: LNP may cause feature interactions on some of the preceding CLASS services.*

- *Operator Assistance (0, 00, or Equivalent)*

  Ability to dial "0" or "00" or similar code to obtain human assistance. Assistance may take the form of completion assistance, emergency interrupt, manual alternate billing, etc.

- *Repair (611 or Equivalent)*

  Ability to dial "611" or similar code to report trouble with a telephone line to a Telephone Company Repair Service Bureau.

- *Access to 911 Service*

  Ability to dial “911” or similar code to report an emergency and to obtain help from police, fire, or medical services in an emergency.

A.2. Custom Calling Features

- *Call Forwarding on Busy Line (CFBL)*

  The CFBL feature provides the capability for the subscriber to redirect calls intended for the subscriber's line (the base station) to another line (the remote station) whenever the subscriber’s line is busy and can not accept the call.

- *Call Forwarding on No Answer (CFDA)*

  The CFDA feature provides the capability for the subscriber to redirect calls intended for the subscriber's line (the base station) to another line (the remote station) whenever the base station does not answer the call after a predetermined number of power rings.

- *Call Forwarding Variable (CFV)*

  The CFV feature provides the capability for the subscriber to redirect calls intended for the subscriber's line (the base station) to another line (the remote station) selected by placing a courtesy call after activating the feature.

- *Call Waiting (CW)*

  CW informs a busy station user, by a burst of tone, that another call is waiting.

- *Cancel Call Waiting (CCW)*

  CCW is an addition to the CW feature and provides the CW subscriber with the ability to disable the CW feature for the duration of the telephone call.

- *Ring Control (RC)*

  RC is a Stored Program Control System (SPCS) service that allows a customer to change the length of time from when a call is offered and the physical forwarding line (base station) is first rung to when CFDA causes the call to be forwarded. To the customer RC allows the customer to change the number of rings before CFDA forwards a call. This service will be available to customers with either rotary of DTMF equipped Customer Premises Equipment (CPE).

- *Abbreviated Dialing*

  Abbreviated Dialing lets the subscriber reach frequently called local or long distance numbers by dialing only one or two digits. Typically up to either 8 or 30 directory numbers can be entered into the speed dialing memory of this service.

- *Three-Way Calling*

  TWC non-Centrex is a custom-calling feature that allows a customer to add a third party to an existing conversation without operator assistance.

A.3. CLASS Features

- *Anonymous Call Rejection (ACR)*

  ACR is a feature that allows customers to reject calls from parties who have a privacy feature that prevents the delivery of their calling number to the called party. When ACR is active, the called customer receives no alerting for a call that is rejected. The rejected call is routed to a denial announcement and subsequently terminated.

- *Automatic Callback (AC)*

  AC is a feature for analog telephone lines that allows a customer to automatically recall that last outgoing call.

- *Automatic Recall (AR)*

  AR is a feature for analog telephone lines that allows a customer to automatically return a call to the last incoming call.

- *Bulk Calling Line ID (BCLID)*

  The BCLID feature allows the Centrex, multi-line hunt group (MLHG), or private branch exchange (PBX) customer to receive call-related information on calls received from outside the Centrex, MLHG, or PBX.

- *Call Screening*

  Call Screening is a SPCS service that is intended to allow a customer, upon having a call forwarded from his or her line, typically to a network-based voice-mail service, to monitor and intercept the forwarded call. This service should be available to customers with either rotary or dual tone multifrequency (DTMF) equipped CPE.

- *Call Waiting Deluxe (CWD)*

  The CWD feature allows a customer to control the treatment applied to incoming calls while the customer is off-hook on a stable call. Analog Display Services Interface (ADSI)-compatible CPE provide a visual menu of treatment options to the called party, as well as selection keys for each option, providing superior support for this feature. Thus, CWD is a service best supported by ADSI CPE.

- *Caller Identity Delivery on Call Waiting (CEDCW)*

  CIDCW is a feature that allows a customer, while off-hook on an existing call, to receive information about a calling party on a waited call. The transmission takes place almost immediately after the customer is alerted to the new call so he or she can use this information to decide whether to take the new call.

- *Calling Number Delivery (CND)*

  CND is a feature intended for residential and small business telephone customers. It allows called CPE to receive a calling party's DN and the date and time of the call during the long silent interval between the first and second power ringing cycles. An off-hook delivery of CND can also be used as part of CIDCW and CWD features.

- *Calling Name Delivery (CNAM)*

  CNAM is a feature that allows the called party's CPE to receive a calling party's name as well as the date and time of the call during the long silent interval between

the first and second power ringing cycles. An off-hook delivery of CNAM can also be used as part of CIDCW and CWD features.

- *Calling Number/Name Presentation Restriction*

  Refers to features that allow callers to control the presentation of their calling number and/or name on a permanent basis (on every outgoing call) or on a per call basis. When the restriction is invoked, only an anonymous indication is delivered to the called party who has CND, CNAM, CIDCW, or CWD service.

- *Customer Originated Trace (COT)*

  COT is a feature that enables the recipient of an obscene, harassing, or threatening call to request an automatic trace of the last call received. The results of the trace are not provided directly to the customer, but are output to an authorized agency, such as the Telephone Company or a law enforcement agency.

- *Distinctive Ringing/Call Waiting (DRCW)*

  DRCW is an incoming call management feature that allows customers to define a special list of telephone numbers. Incoming calls that are on the list are identified to the called party using distinctive alerting treatment.

- *NPA Split Management*

  The CLASS Numbering Plan Area NPA Split Management (NPASM) feature interacts with the CLASS features AC, AR, SLE, and the screening list services to allow customers to use these features with dialing arrangements that are used for completing calls during the permissive dialing period of an NPA split. LECs assign NPA split pairs to the feature. There are four options associated with each NPA split pair and BCCs controls the status of each option. Each option is associated with function(s) of one or more CLASS features. When an option is active for an NPA split pair, the NPAs of that NPA split pair are considered interchangeable for the function(s) associated with the option.

- *Outside Area Calling Alerting (OACA)*

  OACA is a feature in which any calls outside of the local calling area are presented to the called line with a distinctive power ringing cadence or call waiting tone cadence. This distinctive alerting tells the called party that the incoming call is non-local.

- *Remote Call Forwarding (RCF)*

  The RCF feature provides for all calls to a DN to be permanently forwarded, through the Direct Distance Dialing network, to a remote DN.

- *Selective Call Forwarding (SCF)*

  SCF is an incoming call management feature that allows customers to define a special list of telephone numbers and a destination number. Incoming calls that are on the list will be forwarded to the predetermined remote station (i.e., destination number).

- *Selective Call Acceptance (SCA)*

  SCA is a feature that enables telephone customers to instruct an SPCS to accept call attempts from a limited number of calling parties. To use the service, a customer can specify DNs of calls to be accepted. Only call attempts to the customer from these

customer-specified DNs are allowed to terminate to the customer. Unaccepted callers may be connected to a denial announcement, or forwarded to a specified DN, depending on whichever terminating treatment is applicable for a customer's service. If the call is routed to a denial announcement, the caller may enter a PIN, which if correct (i.e., it matches the PIN specified for that called party), allows the call to be connected to the called party.

- *Selective Call Rejection (SCR)*

  SCR is an incoming call management feature that allows customers to define a special list of telephone numbers. Incoming calls that are on the list are prevented from terminating to the customer. Instead, all such calls are connected to an announcement informing the caller that the called party is not presently accepting his/her call.

- *Screening List Editing (SLE)*

  SLE provides customers a way, using audio announcements and dialed entries, to create and update a list of numbers to be used with features such as SCA, SCF, SCR, and DRCW. The maximum list size can be specified by the LEC, with the largest allowable value being 31. The activation code for SLE is the same as that of the feature for which the customer is building the list (for example, the SCF activation code would typically be *63, or 1163 for dial-pulse rotary sets).

A.4. Centrex Features

- *Call Pickup*

  Call Pickup Features describes four Call Pickup (CP) features: CP, Directed Call Pickup (DCP) without Barge-in, DCP with Barge-In, and Trunk Answer Any Station. These allow a station to answer a call ringing at another, unattended station.

- *Call Transfer*

  Multiway Calling (MWC) features provide the user with the capabilities to handle more than one call at a time on a given line. Features included in MWC allow the user to do the following:

  – Hold a call and originate an additional call (e.g., Call Hold)

  – Form a three-way conference (e.g., Three-Way Calling [TWC])

  – Redirect a call to another line (Call Transfer [CT])

  – Create a larger conference (Conference Calling - Six-Way Station Controlled).

- *Extension Dialing*

  Allows the subscriber to dial the other extensions on his or her residential telephone line from any extension, thus to use the extensions as an intercom system.

- *Series Completion*

  The SC feature is a capability that allows calls to a busy DN to be routed to another specified DN in the same switching office.

- *Multi-Line Hunt Group*

  The MLHG feature is a capability that allows calls to a busy DN to be routed in turn to other specified lines in the same hunt group, as predefined to the serving switching office, until one line is not busy and is offered the incoming call.

- *Attendant Features*

  Various features are provided to permit attendants to control usage and to assist in incoming or outgoing call placement to the various Centrex stations of the associated business group. The attendant can: page a called party to answer on any station, control call camp-on (a kind of call waiting service in which the attendant can periodically be connected to the held incoming caller to update call status), select private facilities, test for busy and that a private trunk is in working order, etc.

A.5. Other Features

- *Visual Screening List Editing*

  The VSLE feature allows a customer to build maintain, and review a list of DNs via a Server Display Control session using the Analog Display Services Interface (ADSI). This list may then be used by other CLASS features, such as SCF, SCR, SCA, or DRCW in order to provide special terminating treatment to calls received from any of the directory numbers on the list. In addition, VSLE allows a customer to perform certain administrative functions associated with a supported feature such as feature activation/ deactivation, terminating treatment selection, or specification of a remote directory number (i.e., a number to which calls should be forwarded). VSLE provides the same functionality as the SLE feature, but is enhanced in its use of the ADSI to provide a display-based interface with the customer.

- *Network-Based Voice Mail*

  This service provides 24-hour automated telephone answering and message storage for calls that are forwarded to the subscriber's mailbox on a network-based voice-mail system from her or his called telephone line. Calls to busy lines or to unanswered lines can be forwarded to the voice-mail. Subscribers can subsequently dial their mailboxes on the mail system and listen to, delete, forward, or, in some cases, reply to, the retrieved messages.

- *Outgoing Call Restriction/Customized Code Restriction*

  This feature allows subscribers, typically to business group services, to place certain restrictions on certain telephone lines regarding the outgoing calls that can be placed. For example, calls to non-local telephone numbers may be denied from completing, or no outgoing calls may be allowed, or calls to certain private network dialing codes may be denied.

- *"Teen Line"*

  This service, also known as Resident Distinctive Alerting Service (RDAS), allows a subscriber to have two (in some cases more than two) different telephone numbers on the same telephone line, for example, to provide a separate telephone number where a teenage member of the family can be reached. Each number rings differently and has a special call waiting signal, if that service is subscribed to. Each number can be listed separately in the local Directory.

- *Multi-Party Lines*

  Multi-party feature provides telephone service to multiple customers sharing the same line. For example, two-party feature provides telephone service to two customers sharing the same line.

- *Visual Message Waiting Indicator*

  VMWI is an SPCS feature that activates and deactivates a visual indicator on a CPE (e.g., a flashing LED) to notify the customer that new messages are waiting for him/her. The messages are administered by a third party or Independent Service Provider (ISP).

- *Toll-Free Service*

  A network service provider may offer toll-free service to a business, such that calls to a published DN of that business are toll-free to the caller. The business pays for the toll-free service and charges for these calls. This service may be offered to the business on a wholesale or retail basis. The toll-free service may be known as 800 or 888 service, or may be known to the business as Inward Wide Area Telecommunications Service (INWATS).

  INWATS is defined in SR-504, *SPCS Capabilities and Features*, as a terminating-only service that allows a subscriber to receive message calls originating within specified service areas, with the call charges billed to the called party instead of the calling party. The service is provided to one or more dedicated access lines.

- *Outward Wide Area Telecommunications Service*

  OUTWATS is provided over one or more dedicated access lines to the serving SPCS. The service should allow customers to make calls to certain zone(s) or band(s) on a direct-dialing basis for a flat monthly charge or for a charge based on accumulated usage. OUTWATS lines can dial station-to-station calls directly to points within the selected band(s) or zone(s) or can reach a WATS operator for assistance.

- *Voice-Activated Dialing*

  This is the ability to receive address digits spoken by the caller and to convert the received voice into network address signaling to enable the call to be setup to the desired destination.

- *Basic Business Group*

  The BBG feature provides the basic capabilities for handling a group of lines associated with a single customer. Basic business group includes provision for special dialing arrangements, special restriction arrangements, and special announcement capability, in addition to the capability for the switch to recognize the association of the customer's lines as a group.

- *Conference Calling — Six-Way Station Controlled*

  A business group station subscribing to this service may, after dialing the access code, sequentially call up to five other parties and add them together to make up to a six-way call. The procedure followed by the subscribing party after dialing the access code consists of calling each party, consulting with them privately, and then flashing to add them to the group already collected. A further flash by the subscriber provides

new dial tone and the ability to dial the next party and, upon flash, join the multiparty connection.

- *Centrex Custom Calling and CLASS features*

  Many of the custom calling and CLASS features identified in this appendix have variations that can be activated on Basic Business Groups within the switching system, such as on Centrex lines, for example, the Call Forwarding subfeatures, Bulk Calling Line ID, and Calling Number Delivery or Calling Name Delivery. SR-504, *SPCS Capabilities and Features*, provides a thorough review.

- *Private Virtual Networking Features*

  PVN features will provide business customers with a network service similar to CCSA, EPSCS, and other large-scale dedicated switching networks. PVN will provide many of the features contained in these networks at a lower cost by reducing customers' dependence on dedicated circuits.

  Following are some of the features that a PVN may provide:

  – Direct customer control of the network
  – Flexible dialing plans, including extension dialing
  – Call blocking
  – Selective routing
  – Priority calling/queuing
  – Call detail data
  – Call screening (originating and terminating)
  – Remote Access
  – PVN hop-off
  – Access to any interLATA Carrier (IC)
  – Interworking with dedicated private facilities.

  PVN will provide business customers with increased control over their internal communications, important network features, flexibility to alter their network in an almost real-time manner, and attractive pricing. More importantly, PVN will enable a customer to design and implement a network using the lowest cost IC between corporate locations, rather than buying a private network from a single IC. This feature will rely on the capabilities of Common Channel Signaling (CCS).

- *PBX Network Services*

  A PBX line is an SPCS line connected to a customer premises switching system and used as an originating, terminating, or two-way facility for calls to/from stations served by the PBX.

  PBX lines are eligible for the following services when provided:

  – Free terminating line service

    With this feature, calls from a class of lines (e.g., intraoffice), or from specified trunks to a line designated as a free terminating line, are not billed. The system screens intraoffice calls to prevent charging of calls to lines with this feature. Interoffice calls completed to free terminating lines may require (depending on the incoming trunk class) that answer supervision is not returned to the originating office. Calls to the official lines of a telephone company are an example of lines that may require free terminating line service.

- Denied originating or terminating service

  Denied terminating service is a system feature that denies normal call completions to a line. Calls from test panels, etc., can still terminate to the line. Denied originating service is a system feature that denies originations from a line.

- Code restriction and diversion service

  Code restriction is a feature that blocks call completion to customer-specified codes, e.g., to a particular Numbering Plan Area (NPA).

- Multi-line hunt service was previously defined.

- Make busy key

  This feature provides a method for making a group of lines appear busy to incoming calls. The feature is activated by operation of dedicated keys at the customer's premises. The dedicated keys cause the search for an idle line to skip over the lines controlled by the keys.

- Stop hunt key

  The stop hunt feature is available to customers who have the multi-line hunt service. The switching system associates a key at the customer's premises connected to the switch via a wire pair with a given line of the MLHG. Customer activation of the key stops the hunt at the line associated with the key.

- Direct Inward Dialing

  DID is a feature that allows an incoming toll or DDD call (not FX or WATS) to reach a specific PBX station line without attendant assistance. With DID, the SPCS seizes a DID trunk and outpulses the station line number to the PBX. If the called station's line is idle and not restricted from receiving terminating calls, the PBX alerts the called station and returns audible ringing on the incoming connection. If the called station's line is busy, the PBX returns busy tone. If the called station is restricted from receiving terminating calls, the PBX routes the incoming call to an announcement, reorder tone, or to the attendant. The switching system can be optioned to use DTMF (instead of dial pulse) address signaling to the PBX on DID calls.

- Automatic Identified Outward Dialing

  With this feature the PBX provides the local switch with the identification of the PBX originating line (or attendant) for charge recording purposes. The AIOD information is forwarded to the switch over a dedicated data link.

- Code Diversion

  This feature permits a PBX to deny to some of its lines the completion of station-dialed calls beyond a limited area. The exclusion may encompass all interLATA calls or calls to customer-specified 3-digit codes. When the local exchange receives (on a line with code diversion) a called number to a restricted area, it returns a code diversion signal (battery reversal) to the PBX. On detection of the reverse battery signal, the PBX blocks or allows the call, depending on the originating line.

– Routing of Hotel/Motel Calls

  This feature provides the capability to route outgoing hotel/motel guest-line noncoin toll calls to an operator system for the computing of call charges. Hotel/motel guest-line calls can be routed from the serving SPCS to an operator system over a combined trunk group.

– Outward Calling Features for PBX

  This customer feature of a local switching system allows a PBX (a customer premises switch) to take advantage of business group features relating to outgoing private facilities. Instead of terminating outgoing private facilities directly onto the PBX, the customer may instead terminate the outgoing facilities at the local switching system. The PBX is connected to the local switch with special lines from which these outgoing private facilities may be accessed. Access to the private facilities is through features like Automatic Route Selection (ARS), and may also include authorization codes, outgoing trunk queuing, etc. ARS provides limited alternate routing capability for off-network calls. PBX customers may therefore have their stations dial the outgoing private facility access code, have the PBX seize the special lines to the local switch, and have the local switch do the following: 1) recognize the PBX seizure on these special lines as a request to use the private facilities, 2) return dial tone directly to the PBX station, 3) collect the digits associated with the called number, and 4) route the call over the appropriate private facility based on the particular outward calling features selected (ARS, queuing, authorization codes). The capability of the outward calling features extends sophisticated switching system routing and control functions to a PBX that may not be able to provide such features by itself.

A.6. ISDN Features

- *Call Independent Services (ISDN Only)*

  Call Independent Services are services that can be requested without the establishment of a call. Because of the nature of the signaling capabilities available to ISDN lines, ISDN terminals as defined by National ISDN, generally, are required to identify themselves with the network through a process called terminal initialization. It is expected that the VOP network will support terminal initialization. In addition, the VOP network is expected to support the Auto-SPID capability which helps decrease the human user involvement in the terminal initialization procedure.

  Certain services can be controlled independent of call establishment. These services include the following:

  – Activation/Deactivation of certain ISDN services (e.g., Call Forwarding)

  – Message Waiting Indicator (e.g., to activate/deactivate an lamp at the terminal indicating voice messages are waiting)

  – ISDN Inspect (allows the user to determine the meaning of certain keys on the terminal)

  – Parameter Downloading (helps automate the terminal setup process).

- *ISDN Flexible Call Management*

  FC is a set of capabilities that allows an Integrated Services Digital Network (ISDN) user to establish and control two or more concurrent calls. This set of capabilities includes the ISDN Hold Capability, conference calling, transfer, and multiway calling on ISDN Basic Rate Interfaces (BRIs). When a conference call size reaches two parties (e.g., because of a conferee that drops off) or the controller is unsuccessful in adding a 3rd party to a two-party conference call, the network deactivates conference calling, releases the conference resources, and notifies the controller. In this case, the controller may re-request conference calling and start the process again, if he/she wishes.

- *ISDN Additional Call Offering Service*

  ACO allows the ISDN user to have multiple call appearances of a single directory number, to put one or more calls on hold while making another call, and to receive notification of an incoming call while being active on another call. ACO and ISDN hold provides a Call Waiting capability to ISDN.

- *Services Provided to Business Trunks - ISDN PRI*

  In general, it is assumed that the CPE served by the ISDN PRI Trunk is a PBX, although it does not have to be limited to a PBX. Since PBXs provide a number of capabilities and services already to the end users that they serve, not all services provided to analog lines and ISDN BRIs are offered to ISDN PRI Trunk.

  It is assumed that a National ISDN PRI is used for this trunking interface. On this interface, at a minimum, the following services are to be provided:

  – Calling Number/Redirecting Number Reception

  – Calling Number/Redirecting Number Delivery

  – Calling Name/Redirecting Name Delivery

  – Call-by-Call Service Selection

  – PRI Two B-Channel Transfer

  – Private Networking Features.

  The above listed features require support by the VOP network.

  In addition, it is assumed that the VOP network will provide tones and announcements for originated calls under certain conditions. The PBX is expected to provide certain tones and announcements to its end-users. These include dial tone, recall dial tone, audible ringing, and busy tone.

Following is a brief description of the services mentioned above. These descriptions do not cover all aspects of the service, rather, they provide a high level summary of the major capabilities of the service.

- *Calling Number/Redirecting Number Reception*

  Calling Number/Redirecting Number Reception is where the VOP network may receive a calling number (including privacy indications) as well as redirecting number (including privacy and reason for redirection [e.g., call forwarding busy])

sent by an ISDN user during call origination. In general, it is expected that the VOP network would ensure that the number provided is allowed to be used by the user.

- *Calling Number/Redirecting Number Delivery*

  This feature is where the VOP network may deliver a calling number (including honoring privacy) sent to a user during call termination. Calling Number/Redirecting Number Delivery is also where the VOP network may deliver a redirecting number (including honoring privacy and providing the reason for redirection) sent to an ISDN user.

- *Calling Name/Redirecting Name Delivery*

  Calling Name/Redirecting Name Delivery is where the VOP network may deliver a calling name (including honoring privacy) sent to a user during call termination. Calling Name/Redirecting Number Delivery is also where the VOP network may deliver a redirecting name (including honoring privacy and providing the reason for redirection) sent to an ISDN user.

- *Call-by-Call Service Selection*

  Call-by-Call Service Selection is where the PRI CPE requests certain services from the VOP network on a per-call basis. The services requested may be of the provider of the attached VOP network, or from another provider that may or may not have a VOP network. In this latter case, the PRI CPE includes identification of the provider of the requested service. Some of these services include access to: OUTWATS, Tie Trunk, INWATS, Foreign Exchange, Hotel/Motel, Selective Class of Call Screening, and Access to IXC Services.

- *PRI Two B-Channel Transfer*

  PRI Two B-Channel Transfer is a capability that allows the PRI CPE to efficiently utilize the B-channels on the PRI. This feature allows the PRI CPE to request two calls on the PRI to be connected together and released from the CPE and the interface. The bridging of the resulting transfer is expected occur within the VOP network. Optionally, the network may inform the PRI CPE when the transferred call is cleared from within the network.

- *Private Networking*

  Private Networking features allow the PRI CPE to initiate calls that reside in a "private network" between private network entities (e.g., PBXs and possibly Basic Business Groups) or even hop-off into the domain of the public network. As part of this capability, the VOP network is expected to allow the PRI CPE to utilize a private numbering plan, and to send and receive out-of-band information that may normally be sent during a "normal" call. Examples of such information include the passing of travel class marks, private network calling number and name information and user-entered codes.

A.7. AIN Features

Completing an AIN service typically requires the telephone network to perform a sequence of events organized by sophisticated software. This process involves a series of rapid interactions between elements of the AIN network, especially between the SSP and

SCP. An additional AIN network element may be involved with some services. The following AIN services may need to be supported by VOP*:*

- *Area-Wide Networking*

  Provides multi-location customer with abbreviated dialing plans, centralized routing, access to private facilities, and work-at-home applications.

- *Call Center Management*

  Provides alternate routing of calls to a call center based on pre-determined plans.

- *Calling Name Delivery*

  Delivers name of calling party to the called party.

- *Calling Party/Paging Party Pays*

  Enables cellular/paging subscribers to have the party calling or paging to be charged for the call.

- *Centrex Extend*

  Provides Centrex-like features to multiple locations through abbreviated dialing.

- *Customer Location Alternate Routing*

  Enables rerouting in case of customer location disablement or at customer's discretion.

- *Do Not Disturb*

  Blocks unwanted incoming calls.

- *Follow Me Service*

  Allows customers to establish time of day and day of week schedule for routing calls. Allows customers to be reached on both wireline and wireless networks.

- *Government Emergency Telephone Service (GETS)*

  GETS Provides high probability of completion and alternate carrier routing features to government subscribers.

- *Intelligent Redirect*

  Provides the ability for customers to manage their call load based on time of day, day of week percent allocation, or predetermined list priority customers.

- *Network Switch Alternate Routing*

  Enables calls to be routed to predetermined alternate locations in the event of serving switch failure.

- *Outgoing Call Restriction*

  Ability to screen calls based on a list of included or excluded NPAs, NPA-NXXs, or 10-digit telephone numbers.

- *Prime Number*

  Single number service based on Caller ID and customer-provided routing location.

- *Remote Access Forwarding*

  Call forwarding with remote access to change redirecting information.

- *Selective Call Acceptance*

  Screens incoming calls based on a list of telephone numbers or caller input and only completes those calls that satisfy the screening.

- *Virtual Private Network*

  Enables large business customers to create virtual private networks over the Public Switched Telephone Network (PSTN). Features included intra-company calling, abbreviated dialing, alternate routing, on-line service management, single number market coverage, and uniform pricing and billing among locations.

- *Work at Home*

  Allows a business customer to dial an access code to use the office network, access work features from home, and bill calls to the business.

- *500 Access Service*

  Provides single number for incoming calls in multiple locations.

Appendix B: Capabilities to be Supported by the VOP Network

This appendix identifies some of the key capabilities that will have to be supported by the VOP network in order to enable the services discussed earlier. These capabilities will impact the functional requirements of the elements of the VOP network to be discussed in Section 5.

The discussion in this appendix regarding generic network call processing capabilities is based in part on a higher-level synopsis of the discussion regarding the Advanced Intelligent Network (AIN) Basic Call Models (BCMs) for the PSTN. The AIN BCMs were studied because they provide a readily available, highly generic, Bellcore view of switching system call processing capabilities, and opportunities for their modification by vertical services, that can be modified to account for packet switching and re-allocated among the proposed VOP functional elements. The proposed allocation is accomplished elsewhere in this document. See GR-1298-CORE, Section 3, "Call Model" for more detail.

B.1. Originating Services/Capabilities

This appendix provides a list and high-level definition of originating end network call processing capabilities, and services capabilities upon which services depend.

B.1.1. Call Originating Capabilities

On an originating call basis, the following VOP capabilities are to be provided:

- *Ability to Access Intelligent Network Services*

  This is the ability during the originating end call processing for the network to activate Intelligent Network (IN) service processing when one or more defined IN trigger conditions are encountered at each particular call processing decision point defined for the IN. For example, a specific feature code trigger could activate an IN service when the indicated code is entered by the caller and collected by the network.

- *Ability to Access Originating End Vertical Network Services*

  This is the ability to modify any of the call processing capabilities defined below with installed and activated originating end vertical service capabilities. Activation of these capabilities may result in different network responses and indications to the calling entity than would the basic call processing functionality that would otherwise be performed. These vertical service features are distinct from the IN Services discussed above, but may interact with the IN services to perform a service for an end user. The services to be supported by the VOP network are discussed elsewhere in this document. Originating end network capabilities that support the service specific processing are mentioned below the basic call processing capabilities.

- *Ability to Scan For and Detect an Origination Attempt Signal or Message*

  This is the ability for the network, when an access interface is idle, to scan for and detect the occurrence of a signal or message from an entity requesting originating end call processing by the network. Following are examples:

  – The network receives an off-hook indication from an idle non-ISDN line.

  – The network receives a SETUP message from an ISDN interface.

  – The network detects a seizure signal on a trunk supported by conventional signaling.

  – The network receives an Initial Address Message (IAM) for a trunk supported by SS7.

  – The network detects a seizure signal on a private-facility trunk.

  – The VOP call agent requests via the Media Gateway Control Protocol (MGCP) NotificationRequest command for each associated access or customer gateway to report when an off-hook has been detected. The gateway informs the call agent by the MGCP Notify command when an off-hook has been detected.

- *Ability to Verify the Authority of a User to Place a Call*

  This is the ability to verify the authority of a calling entity (e.g., user CPE or incoming trunk) to continue to place the call with the given properties (e.g., line restrictions). The type of authorization may vary for different types of originating resources (e.g., for lines or trunks) and consists of current originating authorization screening procedures such as provided by a Denied Origination feature.

- *Ability to Provide Call Denial Indication*

  If call placement is denied, the network must provide an ability to send a denial indication to the calling entity. For example, the network would send reorder tone, or an in-band intercept announcement, to a non-ISDN caller, or a Release message to an ISDN or xDSL caller. A VOP call agent could request a gateway to do this by sending an MGCP NotificationRequest command to the gateway. The gateway could respond to the call agent when the caller abandons with a Notify command. The call agent then uses the NotificationRequest command to request the gateway to scan for other call origination attempts, as previously mentioned.

- *Ability to Detect Call Abandonment*

  This is the ability at any time during the originating call setup processing to detect that the calling entity has abandoned the call before it has been answered and to respond by returning that network interface to its idle condition. The network also releases the originating end resources for that call. Following are examples:

  – The network receives an on-hook signal from a caller served by a non-ISDN line.

  – The network receives a call-clearing message from a caller served by an ISDN interface, or detects that the ISDN interface has gone down.

  – The network receives a disconnect indication for a conventional trunk or a private-facility trunk.

  – The network receives a Release message (REL) from an SS7-supported trunk.

- A VOP call agent requests via the MGCP NotificationRequest command or ModifyConnection command (once a connection has been created) for an originating end access or customer gateway to report when an on-hook has been detected. The gateway informs the call agent by the MGCP Notify command, or alternatively by a DeleteConnection command (once a connection has been created), when an on-hook has been detected. The call agent then uses the DeleteConnection command to request the gateway to delete any existing connection, then uses the NotificationRequest command to request the gateway to scan for other call origination attempts, as previously mentioned.

- *Ability to Request and Receive Call Control or Call Processing Information*

  Once authority to continue call placement is verified, this ability enables the network to send an indication to the end user or other calling entity that the network is ready to receive their service request, along with the ability to collect further information about the request from the calling entity. Following are examples:

  - For a call from a non-ISDN line, the network sends an in-band prompt, e.g., dial tone, to prompt the user, attaches a digit receiver, and collects digits within applied timing (e.g., a dialed number, or vertical service code such as *69), translating any speed dialing codes into the full called party number.

  - For a call from an ISDN BRI or PRI following en bloc sending procedures, all the information necessary to process the call, which can include a vertical service code, feature activator, called party number, etc., is included in the SETUP message. For a call from an ISDN BRI not following en bloc sending procedures, the network prompts the caller with a SETUP Acknowledge message to send more information. The network then follows ISDN overlap sending procedures.

  - For conventional trunks, if required by the type of trunk, an appropriate start signal is returned. A digit receiver is attached, digits are collected within applied timing.

  - For SS7-supported trunks, all the information available is contained in the IAM. A check is made to ensure that the IAM contains all the information necessary to process the call.

  - For private-facility trunks, if required by the private-facility trunk group, an appropriate start signal is returned. Depending on the private-facility trunk group, digits may be collected.

  - A VOP call agent can use an MGCP CreateConnection command to cause a gateway to provide dial tone, collect digits using an MGCP DigitMap, and report these to the call agent using an MGCP Notify command.

- *Ability to Analyze and Act On Collected Call Control or Call Processing Information*

  This is the ability of the network (e.g., VOP network call agent) to analyze call control or processing information collected from the calling entity, and to decide the following:

  1. To route the call over the network to a destination customer, access or trunk gateway, e.g., to a destination node, a PSTN called party, a PSTN trunk, or a private-facility trunk. The following activities may be part of this functionality:

     - Receipt of Calling Number

This activity enables the VOP network to receive a calling number (including privacy indications) sent by an ISDN user during call origination. In general, it is expected that the VOP network would ensure that the number provided is allowed to be used by the user.

– Receipt of End-User to End-User information (e.g., Subaddress)

This activity enables the VOP network to receive information provided by the ISDN user that needs to be conveyed unchanged to the called user.

– Translation of Collected Information

This activity enables the VOP network to interpret and translate the collected information according to the specified PSTN numbering plan.

2. To activate a particular vertical service feature. The following activity may be part of this functionality:

– Vertical Service Code/Feature Activator Interpretation

This activity enables the VOP network to recognize and process particular end user actions pertaining to specific service requests. End user actions include using the switch hook flash, dialing a vertical service code such as Automatic Recall *69, Cancel Call Waiting *70, or Voice/Data Protection features.

3. To treat the call as an emergency call, e.g., a “911” call in the North American PSTN.

4. That the information collected is not valid, e.g., the digits collected are not valid per the North American PSTN Number Plan, or not enough of the expected information has been received before a collection timer expires, e.g., the inter-digit timer expires before the next dialed digit is received on an analog PSTN call, or a Code Restriction and Diversion feature might limit the range of destinations to which the calling entity may direct a call.

In either of event 3 or 4, the “call placement denial indication capability” as previously discussed would be used to end the call attempt.

- *Ability to Route the Call*

This is the ability of the network to route a call to a destination network interface or node designated by the calling entity, e.g., to a destination CPE, a home intercom station, an ISDN EKTS intercom station, a PSTN called party, a PSTN trunk, or a private-facility trunk, or simulated facility group. This capability also includes any final call authorization checks over the ability to route the call over adjacent circuit-switched network facilities. For calls traversing the VOP network, then continuing over the PSTN or private network, the network should select the initial adjacent PSTN or private-facility trunk over which to route the call. (It is assumed that the switching systems of the adjacent PSTN or circuit switched private network will handle the routing and trunk busy processing once the call has been connected to that network. However, the VOP network may have to determine an alternate trunk interface into the adjacent network if the initial trunk selection is unavailable to carry the call, e.g., as a result of receiving a trunk busy indication from that network or receipt of an SS7 Continuity check failure via a COT message.) The network must also be able to reroute calls to or from wireless entities as they roam.

- *Provision of Network Busy Indication*

  This is the ability of the network to send to the calling entity an indication that it is unable to route the call either through itself within the specified performance or through an adjacent network (as a result of receiving a network busy indication from that network). For example, the VOP network may send a "fast busy" (reorder) signal to a non-ISDN line; e.g., the call agent may do this via a request using an MGCP ModifyConnection command for the gateway to apply the busy signal. The network should then provide Call Abandon or Call Placement Denial processing, as previously discussed.

- *Ability to Derive Information Needed for Call Setup*

  This is the ability of the network, once it verifies that it has the ability to route the call, to derive additional information needed by the terminating end to complete call setup beyond what was received from the calling entity, e.g., the network determines the Calling Party ID and/or the ANI for a non-ISDN line.

- *Ability to Send Call to Terminating End Call Processing*

  This is the ability of the network to send an indication of the desire to setup a call to the terminating end call processing and to pass collected or derived call information from the network originating end capabilities to the appropriate terminating end capabilities so that the latter can perform its call processing. For example the VOP call agent may send to the selected terminating end gateway an MGCP CreateConnection command containing a RemoteConnectionDescriptor. For the PSTN, the information that may be passed to the terminating call portion includes: Charge Number; Calling Party ID; Calling Party BGID; Calling Party Station Type (determined by the Class of Service information, ISDNUP originating line information parameter, or ANI II information from EAMF signaling); Bearer Capability; Called Party ID; Calling Party Subaddress; Called Party Subaddress; Carrier; Route Index; Carrier Identification Code, Circuit Code, and Carrier Selection, etc. The network should also send to calling entities call progress information expected by these calling entities, e.g., a Call Proceeding message to an ISDN line.

- *Ability to Receive and Respond to Call Progress from Terminating End Call Processing*

  This is the ability of the network to receive and act on the following call progress indications from the terminating end call processing.

  – If an indication of call progress is returned (e.g., terminal seized, or called party being alerted), the network may (depending on the standard call processing for a given calling entity) pass or send a call progress signal to the calling entity, e.g., pass the in-band audible alerting signal to a calling non-ISDN line, or send an ISDN Progress or Alerting message to a calling ISDN line, and provide for detection of indications of activation of mid-call vertical services. The VOP call agent might use an MGCP ModifyConnection command to pass this information to the originating gateway and to request it to send call progress signals to the calling entity, i.e., end point.

  – If an indication of call rejection is returned (e.g., called line/party busy, or call not answered after being alerted for a specified time), the network may (depending on the standard call processing for a given calling entity) provide call

denial indications to the calling entity (e.g., busy signal to an analog line) and wait for caller abandonment as previously discussed, or provide terminating end release processing, as discussed below.

– If an indication of call acceptance is returned (e.g., called party answer signal or message), the network may (depending on the standard call processing for a given calling entity) send an answer indication to the calling entity then provide an active call condition. For example, the VOP call agent might use an MGCP ModifyConnection command to request the originating end gateway to send any answer indication then change mode to e.g., SendReceive to support voice transmission.

- *Provision of Active Call Capabilities*

  This is the ability of the network to provide for voice transmission within the required performance levels and for detection of indications of: activation of mid-call vertical services, e.g., a "Flash" signal from the caller to activate analog Three way Calling, or of caller or called entity disconnection. The network may (depending on the standard call processing for a given calling entity) send an answer signal (e.g., to conventional or private-facility trunks) or message (e.g., ISDN Connect message or SS7 ANM message) when this capability is first used on a call. For example, the VOP call agent might use an MGCP ModifyConnection command to request the originating end gateway to send any answer indication then change mode to e.g., SendReceive to support voice transmission, to detect a mid-call event, and to notify the call agent via a Notify command when it occurs.

- *Provision of Call Release Capabilities*

  This is the ability of the network originating end to respond to an indication of calling entity disconnection (e.g., detection of on-hook) or called entity disconnection (e.g., on-hook) or reconnection (e.g., off-hook) to clear or restore the active call. The network also can initiate originating end call clearing under basic or service-specific call processing control. Following are examples, assuming originating end call control, as in the PSTN:

  – If the calling party disconnects, the network should return its originating end capabilities for this call to their idle condition, i.e., the call is cleared without further delay, e.g., the call agent would send an MGCP DeleteConnection command to the originating end gateway, then send the NotificationRequest command to request the gateway to scan for other call origination attempts, as previously mentioned.

  – If the called party disconnects, the network may start appropriate timing before clearing the originating end call resources, depending on the indication received, the access type and the position of the network in any connection. For a calling SS7 trunk, if timing is to be done, a Suspend message (SUS) is sent. Timed release disconnect is not done for a call terminating to an ISDN interface or to an EKTS group. Timing is also not done if an SS7 Release message was sent to the network terminating end. In these cases, the network immediately returns its originating end capabilities for this call to their idle condition. For the other cases, when the release timing expires, the network should return its originating end capabilities for this call to their idle condition. For example, initially the VOP call agent might send MCGP ModifyConnection commands if timing the

release. After time-out, the call agent could send the DeleteConnection commands to the gateways to return to idle conditions.

– If the terminating call portion sends an indication that the terminating party has gone off-hook or an SS7 Resume message (RES) is received before the timer expires, active call capabilities resume. If the originating access is an SS7 trunk, a RES is sent. For example, the VOP call agent might use another MGCP ModifyConnection command to request the originating end gateway to change mode to e.g., SendReceive to support voice transmission, to detect a mid-call event, and to notify the call agent via a Notify command when it occurs.

B.1.2. Originating End Service-Support Capabilities

This section presents a list and high-level description of generic originating end capabilities intended to support known PSTN/AIN vertical services that are also desirable to be supported by a VOP network.

- *Provide Vertical Service Feature Activation/Deactivation Indication*

  This is the ability for the network to provide the calling entity with a service-specific indication that an originating end vertical service feature has been activated or deactivated.

  As an example, for an analog line, when exercising certain service-specific capabilities, the network could, instead of normal dial tone, provide the following alternative dial tone signals:

  1. Stutter (i.e., Message Waiting Indicator) Dial Tone
  2. Recall/Confirmation Dial Tones.

  The former is an indication to the end user that messages are waiting to be retrieved. The latter can be an acknowledgement of a successful user action (e.g., acknowledge using the switch-hook flash to initiate a three way call, or acknowledge user entry of service profile information such as speed dialing numbers, etc.).

  The network service might instead request that the network send an audible announcement to provide a service-specific indication of activation or deactivation, such as “Your return call service is now deactivated”.

- *Record, Store, and Play Audible Announcements*

  This is the ability to record audible announcements, including voice messages and standard network signals and tones. This also comprises the ability to store these announcements such that they may be accessed and played to end users under control of a particular basic originating end call processing capability, originating end vertical service feature, or IN service feature. For example, the Provide Call Denial Indication Capability might send an intercept announcement declaring that the digits dialed were invalid. See also the above example of a Return Call service activation announcement. Although network element manufacturers or vertical service manufacturers may provide default announcements, network service providers should be able to record their own selection for the network to play instead, for each such announcement.

  Network Call Progress Announcements such as Intercept announcements need to be supported.

- *Voice Response*

  The originating end must support voice response capabilities for the Network Facility Access (NFA) feature that supports Voice Activated Dialing (VAD) and Voice Activated Network Control (VANC) services.

- *PSTN Supervisory and Address Signals*

  The originating end must support all PSTN line and trunk supervisory and address signals, such as various Direct Current (DC), Single Frequency (SF) and Multi-Frequency (MF) trunk signals and on-hook versus off-hook (DC), and other line DC signals, dial pulse, caller-generated signals such as Dual Tone Multi-Frequency (DTMF) signals, and operator services tones and signals.

- *Call Progress Tones*

  Generation of PSTN Call Progress Tones, such as busy, re-order, and audible ringing, needs to be supported, and receipt of a network equivalent indication from the terminating end that these tones need to be generated needs to be supported.

- *Communicate via SS7 Protocols*

  This is the ability to communicate via Signaling System 7 (SS7) data communications protocols over Common Channel Signaling (CCS) links with CCS entities such as PSTN SSP switching systems, and SCPs including Line Information Databases (LIDBs), or other AIN databases. This includes all lower layer SS7 protocols needed to communicate with and between STPs to route communications between the above higher-layer entities, as well as error messages and reports.

  - To support interconnection with CCS-supported PSTN trunks, the originating end network must specifically be able to communicate using the ISDN User Part (ISDNUP).

  - To support access to IN nodes, SCPs, LIDBs or other AIN databases, e.g., to support an originating end retrieval of calling party name data, given the calling party number, such as for the business group version of Calling Name Delivery service, the originating end network must specifically be able to communicate using the Transaction Capabilities Access Part (TCAP).

- *Call Hold*

  This capability allows an originating end network vertical service or IN feature to separate a call from a controlling entity in order for this entity (such as an end user via a CPE) to perform some other task while the call is held, initiate a new call, retrieve another already held call, or possibly join two calls to form a three way call. The separated call is not cleared, but remains active, terminated to a low noise entity (quiet termination) or to an announcement or music source. For an ISDN user, a channel must be reserved for the terminal initiating hold so that the held call can be retrieved by the initiating terminal without being concerned about the availability of a free channel. Optionally allowed for an ISDN user is the ability to notify the remote user that the call is held or retrieved.

- *Call Retrieve*

  This ability allows an originating end network vertical service or IN feature to retrieve a held call, i.e., to allow the call to be rerouted to its original controlling entity for communication with it, for example, in a Three Way Calling feature. The

held call may also be joined with another received call and the terminating entity, for example in the Three Way Calling feature. Optionally allowed for an ISDN user is the ability to notify the remote user that the call is held or retrieved.

- *Outgoing Memory Slot Administration*

  This is the ability to enter and store the last number "dialed". Needed for PSTN Automatic Callback service (*66).

- *Determination of Calling Party Identity*

  These are the specific abilities to determine calling party identity and privacy choice from the calling entity to support Caller ID services, to allow the calling entity to modify their default privacy choice on a per-call basis, and to be able to convey these to the terminating end. For example for analog lines, the calling party number must be determined, along with its presentation/privacy status, and transmitted to the terminating end handling the called party. In Calling Name Delivery service for Basic Business Groups (BBGs), the originating end determines the calling party name and conveys it to the terminating end, along with its presentation/privacy status.

- *Provide Automatic Identified Outward Dialing*

  With this feature the Private Branch Exchange (PBX) provides the local switch with the identification of the PBX originating line (or attendant) for charge recording purposes. The AIOD information is forwarded to the switch over a dedicated data link.

- *Provide Billing Data*

  This is the ability of the originating end to track and store (i.e., collect and record) appropriate active call data, typically called Automatic Message Accounting (AMA) data, for use in billing the call. Usual billing parameters include service type, length of connection, etc. VOP calls may also need to address different levels of service quality and the number of packets sent and received rather than length while the call is active.

- *Provide Operator Services Signals*

  This is the ability of the network to generate and send to the calling entity various signals or messages pertinent to operator services or Alternate Billing Services (ABS) during call origination. Examples from the analog PSTN include signals sent from a payphone to an operator over an operator trunk to indicate that appropriate amount of coins have been entered into the payphone. Another example is the coin release or collect signals sent from the operator to a payphone to release coins back to the calling payphone user, or to collect the coins entered by the user into the payphone upon successful call completion. Another example is generation of an ABS "Bong" tone as an indication to the caller to provide her or his calling card information to the network for alternate billing of the call.

B.2. Terminating Services/Capabilities

On a terminating basis, the capabilities that are to be provided include call terminating capabilities and terminating end service-support capabilities.

B.2.1. Call Terminating Capabilities

On a call-terminating basis, the following capabilities are to be provided:

- *Ability to Access Intelligent Network Services*

  This is the ability during the call processing for the network to activate Intelligent Network (IN) service processing when one or more defined IN trigger conditions are encountered at each particular call processing decision point defined for the IN. For example, an IN trigger could activate an IN service whenever the network terminating end is notified about an incoming call.

- *Ability to Access Terminating End Vertical Network Services*

  This is the ability to modify any of the call processing capabilities defined below with installed and activated terminating end vertical service capabilities. Activation of these capabilities may result in different network responses and indications to the called entity (and perhaps also to the calling entity) than would the basic call processing functionality typically being performed by that capability, in the absence of vertical service feature activation. These vertical service features are distinct from the IN Services discussed above, but may interact with the IN services to perform a service for an end user. The services to be supported by the VOP network are discussed elsewhere in this document. Terminating end network capabilities that support the service specific processing are mentioned below the basic call processing capabilities.

- *Ability to Scan for and Detect a Termination Attempt Signal or Message*

  This is the ability for the network terminating end to scan for and detect the occurrence of a message from the originating end, requesting terminating end call processing by the network, and to receive collected or derived call information from the network originating end capabilities so that the terminating end can perform its call processing. For example, the VOP call agent may send an MGCP CreateConnection command to a selected terminating end gateway. For the PSTN, the information that may be passed to the terminating call portion includes: Charge Number; Calling Party ID; Calling Party BGID; Calling Party Station Type (determined by the Class of Service information, ISDNUP originating line information parameter, or ANI II information from EAMF signaling); Bearer Capability; Called Party ID; Calling Party Subaddress; Called Party Subaddress; Carrier; Route Index; Carrier Identification Code, Circuit Code, and Carrier Selection, etc.

- *Ability to Authorize Call Termination*

  This is the ability of the network terminating end (e.g., a VOP call agent) to verify its authority to route this call to the terminating entity, e.g., by checking business group restrictions, line access restrictions to certain incoming calls, or ISDN bearer capabilities. Among the access restrictions that may be checked for analog lines are those imposed by invoking Denied Termination, Do Not Disturb, CLASS Selected Call Acceptance, Selected Call Rejection, Anonymous Call Rejection, Selected Call Forwarding or unconditional Call Forwarding Variable feature processing that the called user has subscribed to.

  – If access is verified, the network invokes its Select Facility capability.

– If access is denied, the network provides an indication of call denial to the originating end. The network terminating end may instead perform service-specific processing such as playing an announcement to the caller. After any vertical service functionality has been exercised, the network releases its terminating end resources for this call.

- *Ability to Detect Call Abandonment*

  This is the ability at any time during the terminating call setup processing to detect an indication from the network originating end that the calling entity has abandoned the call before it has been answered by the called entity. The network responds by releasing the terminating end resources for that call. For example, the VOP call agent may send an MGCP DeleteConnection command to a selected terminating end gateway. See the corresponding originating end capability for examples of calling entity abandonment.

- *Ability to Select Facility for Call Presentation*

  This is the ability of the network terminating end to check the busy/idle status of the called entity. Following are examples of the conditions checked:

  1. For a non-ISDN line, if the line is already involved with an existing call, the line is treated as network-determined user busy. User busy, also called line busy, may also be detected as a result of an analog line being out of order, marked as busy by a customer make-busy key, or as a result of certain maintenance actions.
  2. For conventional trunks, SS7-supported trunks, and private-facility trunks, busy is when all trunks within the selected trunk group are busy.
  3. Certain Basic Business Group (BBG) features may use Simulated Facility Groups that cause the network to restrict the amount of traffic between the BBG and the public network and the amount of intra-BBG traffic generated by group members.
  4. A VOP call agent may use an MGCP AuditEndpoint command and after gateway notification perhaps also an MGCP AuditConnection command to request that a gateway check for this busy/idle status. The Gateway would report the status to the call agent using an MGCP Notify command for the following conditions:

– If the terminating access is not busy, the terminating end sends an indication to the originating call portion that an idle facility is available. For example, if the call originated from an ISDN interface, an ISDN CALL PROCEEDING message is sent to the caller by the originating end that received it from the terminating end of the network. In VOP the call agent would send a ModifyConnection command to the originating end gateway for the gateway to send the appropriate indication to the calling entity.

– If the terminating access is busy, if AIN service logic is not needed on the call and no switch-based features, such as Multi Line Hunt Group (MLHG) or Series Completion features, apply, the terminating end sends an indication to the originating end that an idle facility is busy. In VOP the call agent would send a ModifyConnection command to the originating end gateway for the gateway to send the appropriate indication to the calling entity. The network then waits for caller disconnection. When it perceives caller disconnection, it releases its terminating end resources for this call. For VOP, the originating end transactions were previously discussed. To

disconnect the terminating end the call agent would send an MGCP DeleteConnection command to the terminating end gateway.

  - If a terminating feature acts on the call such that the call is completed (e.g., as in the Call Waiting feature, if the user toggles to the incoming call, placing the existing call on hold), the busy indication is not passed to the network originating end.

- *Ability to Present the Call to and Alert the Called Entity*

  This is the ability for the network terminating end to alert, i.e., to notify, the called entity about the presence of the incoming call and to wait for detection of when the terminating entity has accepted, answered or rejected the call or of when the calling entity has abandoned the call. For an idle analog line, an audible notification is provided by generation of power ringing. For ISDN lines, alerting is via an explicit SETUP message. A seizure signal would be sent to a conventional trunk, while an IAM or CRM might be sent regarding an SS7-supported trunk. For VOP, the call agent might use an MGCP ModifyConnection command to cause the terminating end gateway to apply ringing and to report via a Notify command when the called entity answers.

  1. If the network detects that the terminating entity has accepted the call, then it passes an appropriate call progress indication to the originating end (e.g., audible ringing signal) and waits for other indications. A VOP call agent might send an MGCP ModifyConnection command to the originating end gateway for this purpose. Examples of this call acceptance indication include: seizure of a conventional or private-facility trunk, or sending power ringing to an analog (non-ISDN) line.
  2. If the network detects that the terminating entity has answered the call, then it passes this indication to the originating end and invokes its terminating end Active Call Capabilities. Following are examples of call answer:
     - The network has received an indication that the analog terminating party has gone off-hook.
     - The network has received a CONNECT message from an ISDN user (or an off-hook indication from an analog user within a terminating EKTS group).
     - The SSP has received an answer indication on a conventional trunk or private-facility trunk.
     - The SSP has received an ANM for an SS7-supported trunk in response to an IAM.
  3. If the network detects that the caller has abandoned the call, then it invokes its terminating end Call Release Capabilities.
  4. If the network detects that the called entity has rejected the call, then it passes this rejection to the originating end, then it invokes its terminating end Call Release Capabilities. Examples of call rejection include: one or more ISDN users sending a call clearing message in response to the terminating call, or the network does not receive the proper wink acknowledgement signal from a conventional trunk. A call can not be rejected from a non-ISDN line.

- *Provision of Active Call Capabilities*

  This is the ability of the network to provide for voice transmission within the expected performance levels and for detection of indications of activation of mid-call vertical services, e.g., a "Flash" signal from the called party to activate a joining of the caller, called party and called party's voice mail box in a call screening feature. The network may send a Connect Acknowledge message to a called ISDN line when this capability is first used on a call. This capability also provides for caller or called entity disconnection. For example, the VOP call agent might use an MGCP ModifyConnection command to request the terminating end gateway to change mode to e.g., SendReceive to support voice transmission, to send the above acknowledgement if needed, to detect a mid-call event, and to notify the call agent via a Notify command when it occurs.

- *Provision of Call Release Capabilities*

  This is the ability of the network terminating end to respond appropriately to an indication of calling entity disconnection or called entity disconnection or reconnection to clear or restore the active call. The network also can initiate terminating end call clearing under basic or service-specific call processing control. For example, assume the following originating end call control, as in the PSTN:

  1. If the calling party disconnects or abandons the call, the network should return its terminating end capabilities for this call to their idle condition, i.e., the call is cleared without further delay, e.g., the VOP call agent would send an MGCP DeleteConnection command to the terminating end gateway.

  2. If the called party disconnects, the network may start appropriate timing before clearing the terminating end call resources, depending on the indication received, the access type and the position of the network in any connection. Timed release disconnect is not done for a call terminating to an ISDN interface or to an EKTS group. Timing is also not done if an SS7 Release message was received by the network terminating end. In these cases, the network immediately returns its terminating end capabilities for this call to their idle condition. For the other cases, when the release timing expires, the network should return its terminating end capabilities for this call to their idle condition. For example, initially the VOP call agent might send MCGP ModifyConnection commands if timing the release. After time-out, the call agent could send the DeleteConnection commands to the gateways to return to idle conditions.

  3. If the terminating call portion sends an indication that the terminating party has gone off-hook or an SS7 Resume message (RES) is sent before the timer expires, active call capabilities resume. For example, the VOP call agent might use another MGCP ModifyConnection command to request the terminating end gateway to change mode to e.g., SendReceive to support voice transmission, to detect a mid-call event, and to notify the call agent via a Notify command when it occurs.

B.2.2. Terminating End Service-Support Capabilities

This section presents a list and high-level description of generic terminating end capabilities intended to support known PSTN/AIN vertical services that are also desirable to be supported by a VOP network.

- *Conference Bridge*

  This capability allows a terminating end network vertical voice conference call service, or multiway calling service, in which several calls are completed each to a port of the network conference bridge. Once each call is active on the bridge, all callers can communicate with each other through the bridge. Their callers may terminate individual calls and the bridge port would be released for reuse on another call. The network service can also maintain a timer for the reserved length of the conference, then disconnect all calls from the bridge that are participating in that conference. The bridge control feature or conference vertical service can receive information from each caller during or after call setup to the conference bridge to determine if the caller can be connected to, or denied access to, the bridge for a particular conference. For example, an access code might be dialed, once connected to the bridge, to allow the bridge controller to validate the caller's right to participate in a given conference at that time.

- *Record, Store, and Play Audible Announcements*

  This is the ability for the terminating end to record audible announcements, including voice messages and standard network signals and tones. This also comprises the ability to store these announcements such that they may be accessed and played to end users under control of a particular basic terminating end call processing capability, terminating end vertical service feature, or IN service feature. For example, the Active Call Capability might invoke a Wake Up Call service consisting of an audible announcement once the user answers a call from the network at a certain time of day. Although network element manufacturers or vertical service manufacturers may provide default announcements, network service providers should be able to record their own selection for the network to play instead, for each such announcement.

- *Voice Response*

  The terminating end must support voice response capabilities for the Network Facility Access (NFA) feature that supports Voice Activated Network Control (VANC) services.

- *Call Progress Tones*

  Generation of PSTN Call Progress Tones, such as audible ringing, by the terminating end (or reception from another network), transmission from the terminating end to the originating end of the network, and their regeneration by the originating end to a calling entity, needs to be supported.

- *Communicate via SS7 Protocols*

  This is the ability to communicate via Signaling System 7 (SS7) data communications protocols over Common Channel Signaling (CCS) links with CCS entities such as PSTN SSP switching systems, and SCPs including Line Information Databases (LIDBs), or other AIN databases. This includes all lower layer SS7 protocols needed to communicate with and between STPs to route communications between the above higher-layer entities, as well as error messages and reports.

  1. To support interconnection with CCS-supported PSTN trunks, the terminating end network must specifically be able to communicate using the ISDN User Part (ISDNUP).

2. To support access to IN nodes, SCPs, LIDBs or other AIN databases, e.g., to support a terminating end retrieval of calling party name data, given the calling party number, such as for the residential version of Calling Name Delivery service, the terminating end network must specifically be able to communicate using the Transaction Capabilities Access Part (TCAP).

- *Distinctive Alerting*

  This is the ability for the terminating end to generate distinctive alerting indications to the called entity to serve as notification to called parties of special events (e.g., the call is from a special number as determined in advance by the called party). These alerts are requested by various terminating end vertical services typically invoked during Call Presentation and Alerting processing. For idle called analog lines, this may occur via changes to the normal applied power-ringing cadence, known as Distinctive Ringing, as directed, for example, by a Resident Distinctive Alerting Service (RDAS). For active, off-hook called analog lines, this may occur via changes to the normal applied call waiting signal, under control of a Distinctive Ringing/Call Waiting (DR/CW) service feature. For ISDN lines, this is via an explicit message.

- *Transmit Calling Party Identification to Terminating Entity Being Alerted*

  This is the ability to send Calling Party Number and Name information to the terminating entity being alerted.

  For example, it is the ability to transmit this caller ID information to current-generation Caller ID Customer Premises Equipment (CPE) using Frequency Shift Key (FSK) signaling on analog lines. When alerting an idle analog line, the FSK is transmitted between power rings. When alerting an analog line engaged in an active call via a Caller Identification Delivery under Call Waiting (CIDCW) or Call Waiting Deluxe (CWD) feature, the FSK is preceded by a CPE Alerting Signal (CPE) designed to briefly interrupt conversation and prepare the line to receive FSK.

  For ISDN lines, it is the ability to deliver calling number and/or name (including honoring privacy). This delivery includes the delivery of display information in an explicit message.

  For Centrex, Multi-Line Hunt Group (MLHG) or PBX customers, it is the ability to receive call-related information, including caller number and name, over a dedicated data link from the terminating end network, via the Bulk Calling Line Identification (BCLID) service.

- *Call Waiting Alerting*

  This is the ability to provide a unique notification (audible for analog lines) to a terminating entity such as an end user already engaged on a call that another call is waiting, under control of a Call Waiting vertical service typically invoked during Select Facility processing. An audible notification is provided for analog lines whereas an explicit message is used for ISDN lines, for example in the ISDN Additional Call Offering feature. The call waiting service typically allows the called party to use call hold and retrieve capabilities to alternate between the held and active call.

- *Caller Identity Delivery on Call Waiting Alerting*

  This is the ability to transmit the CPE Alerting Signal (CAS) of the CLASS CIDCW feature, as well as non-ISDN Calling Party Identification to the Terminating Entity being alerted.

- *Direct Inward Dialing*

  This is the terminating end network capability to support the special signaling protocol for DID trunks to a PBX. It is often deployed in a 2-way arrangement which includes both DID and originating end Direct Outward Dialing (DOD). See the recommendations in Section 5.1.1.3.2.1.2 for the Access Gateway regarding DID and DOD.

- *Call Hold*

  This ability allows a terminating end network vertical service or IN feature to separate a call from a terminating entity such as a called CPE, in order to transfer the call to another party as in a Call Transfer feature, or to receive another call, retrieve another held call, or join the two received calls together with the terminating entity, for example in a Call Waiting or Call Waiting Deluxe feature. The separated call is not cleared, but remains active while terminated to a low noise entity (quiet termination) or to an announcement or music source. Optionally allowed for an ISDN user is the ability to notify the remote user that the call is held or retrieved.

- *Call Retrieve*

  This ability allows a terminating end network vertical service or IN feature to retrieve a held call, i.e., to allow the call to be rerouted to its original terminating entity for communication with it, for example, in a Call Waiting feature. The retrieved call may also be joined with another received call and the terminating entity, for example in a Call Waiting Deluxe feature. The retrieved call may instead be rerouted to another terminating entity, for example under a Call Transfer feature. Optionally allowed for an ISDN user is the ability to notify the remote user that the call is held or retrieved.

- *Incoming Memory Slot Administration*

  This is the ability to enter and store the number of the last incoming call. This is needed for PSTN Automatic Recall service (*69) or Customer Originated Trace service.

- *Call Forwarding*

  This is the ability to redirect or reroute the incoming call when requested by a vertical service, such as call forwarding features discussed below, to the destination indicated by the service. The terminating end will invoke originating end call processing capabilities as needed to redirect or reroute the call and will pass to the originating end call information needed to setup, bill, and provide vertical services for, the redirected call. For example, the controlling vertical service might be invoked to check the following conditions and perform call forwarding activities when the conditions are true: when the terminating end capabilities detect line busy (Call Forwarding on Busy Line service), or when the called party does not answer after a specified number of alerts (such as Call Forwarding Don’t Answer service, say, after a specified number of power rings), or when the calling party number is found on a list of callers that are to be forwarded to another specified destination (Selective Call Forwarding). Unconditional Call Forwarding (Call Forwarding Variable) service or

Remote Call Forwarding might also be invoked whenever the network checks for authorization to terminate the call. Processing of an active Night Service or Centralized Attendant Service or Call Pick Up feature or Call Transfer feature would also cause unconditional rerouting of a call to another designated destination.

- *Provide Billing Data*

  This is the ability of the terminating end to track and pass to the originating end Billing feature on request appropriate active call data, typically called Automatic Message Accounting (AMA) data, for use in billing the call. Usual billing parameters include service type, length of connection, etc. VOP calls may also need to address different levels of service quality and the number of packets sent and received rather than length while the call is active.

- *Operator/Attendant Barge-in, Busy Verification, or Emergency Override Support*

  This is the ability of the terminating end to provide the special means for operator or attendant features to determine the busy versus idle condition of a called line and to connect this originating entity to the selected line regardless of its idle or busy status.

B.3. Network Services/Capabilities

This section lists and briefly defines network capabilities that are independent of call processing that need to be supported by a VOP network. Communications and other Capabilities in support of Operations are not explicitly considered in this section.

- *Communicate via SS7 Protocols*

  This is the ability to communicate via Signaling System 7 (SS7) data communications protocols over Common Channel Signaling (CCS) links with CCS entities such as PSTN SSP switching systems, and SCPs. This includes all lower layer SS7 protocols needed to communicate with and between STPs to route communications between the above higher-layer entities, as well as error messages and reports.

  1. **Support for TCAP:** To support services such as Automatic Callback (Repeat Call) and Automatic Recall (Return Call) between originating and terminating end PSTN switching systems in which part of the communications is carried over the network, the network must specifically be able to communicate with each PSTN switch using the Transaction Capabilities Access Part (TCAP).

     To support requests for information from an IN SCP to the network, or through the network in part to an IN SSP switching system, the network must specifically be able to communicate with such SCPs and switching systems using the Transaction Capabilities Access Part (TCAP).

     The VOP network will have to support TCAP to query SCPs in other networks for a variety of services discussed earlier. For example, a SCP may need to periodically access data stored for a network based vertical service.

  2. **Support for Billing:** TCAP must also be supported to allow the network to periodically transmit AMA data about call billing over specified time intervals for all calls handled by or for a given service provider, originated at various network gateways, to certain Billing administration systems of that service provider.

3. **Support for optional ISUP parameters:** The VOP network will have to support numerous optional parameters (such as the Transit Network Selection [TNS]) to enable the VOP network provide equal access to various long distance providers.

- *Communication with Billing Systems*

  This is the ability of the network to communicate collected billing records to billing administration systems for processing, using other than TCAP.

- *Screening List Editing*

  This is the ability to edit various service-specific databases stored on the network. Such databases include speed dialing lists, or lists of calling entities whose requests for call completion are to be accepted (as for CLASS Selective Call Acceptance service) or denied (as for CLASS Selective Call Rejection service).

- *ISDN Customer Station Rearrangement*

  This is the ability to support movement of an ISDN station from one network port to another. This capability assures that all pertinent data, subscribed features, AIN triggers, etc., associated with that station are translated and stored by the network with the new port for use in originating and terminating calls involving that station.

- *Message Service Notification*

  This is the ability for the network to communicate with a message service such that the message service host directs the network to route a standard notification of new messages waiting to the subscriber. The message notification request would be made to the network as needed by the message service host. An example is the Simplified Message Desk Interface (SMDI) between a voice mail or other messaging service and PSTN local analog switching systems. The messaging server uses SMDI to notify the switch that serves its subscriber that she or he has messages waiting. The switch uses FSK to request that a compatible CPE turn-on an indicator, or uses stutter dial tone, to notify the subscriber.

Appendix C: Message Flows

C.1. Sample Call Flows

This appendix describes sample, high-level, end-to-end message flows. Refer to Section 4.2 for discussion of the underlying architecture of the network and to Section 5 for discussions of the functional requirements describing the key elements of the architecture.

C.1.1. Assumptions

The call flows in this section depend on the following assumptions (note that these assumption were also listed in Section 4.2):

1. A CCA contains all information (e.g., trunk status tables) that a normal PSTN switch needs for call processing.
2. Each network node contains procedures that ensure the delivery of error-free messages between network nodes. Furthermore, these procedures maintain message sequencing.
3. Each trunk between a PSTN switch and a TG is uniquely identified by the switch's PC and a CIC. The trunk is also uniquely identified by the TG's address and a channel_number.
4. All calls have identical Quality of Service and bandwidth requirements.
5. The voice to packet converters (VPCs) in a TG are interchangeable in the sense that any one may be used during call setup. In other words, neither the caller nor the CCA prefers one VPC to another.
6. The virtual circuits out of a TG are interchangeable in the sense that any one may be used during call setup. In other words, neither the caller nor the CCA prefers one virtual circuit to another.
7. Given a Called Party Number and the address of a TG, an RTS is able to determine the address of the next CCA that should handle a call.
8. The virtual circuits in the packet network are switched.
9. Each CCA manages the trunks terminating at its subordinate TGs.
10. Each TG manages its internal VPCs and the virtual circuits that it terminates.
11. Each trunk between a PSTN switch and a TG is associated with a single SG, but each SG may serve multiple PSTN switches.
12. One and only one CCA serves each TG, but each CCA may serve multiple TGs.
13. One and only one CCA serves each SG, but each CCA may serve multiple SGs.
14. A TG marks a trunk "busy" only after a CCA instructs it to do so. In other words, a TG never initiates the seizure of a trunk.

C.1.2. A Successful Call Setup

The message flow in this section describes a successful call setup across the network shown in **Error! Reference source not found.**. Such a call setup could occur when an IXC with VOP capabilities provides connectivity between SSP1 and SSP2. In other words, when the IXC's network contains all network nodes in the figure except SSP1 and SSP2.

Note that the message flow in this section is only an example and is based on the prior assumptions. Actual message flows may vary depending on the network protocols used and the types of interconnectivity offered (e.g., PVCs versus SVCs in the packet network).

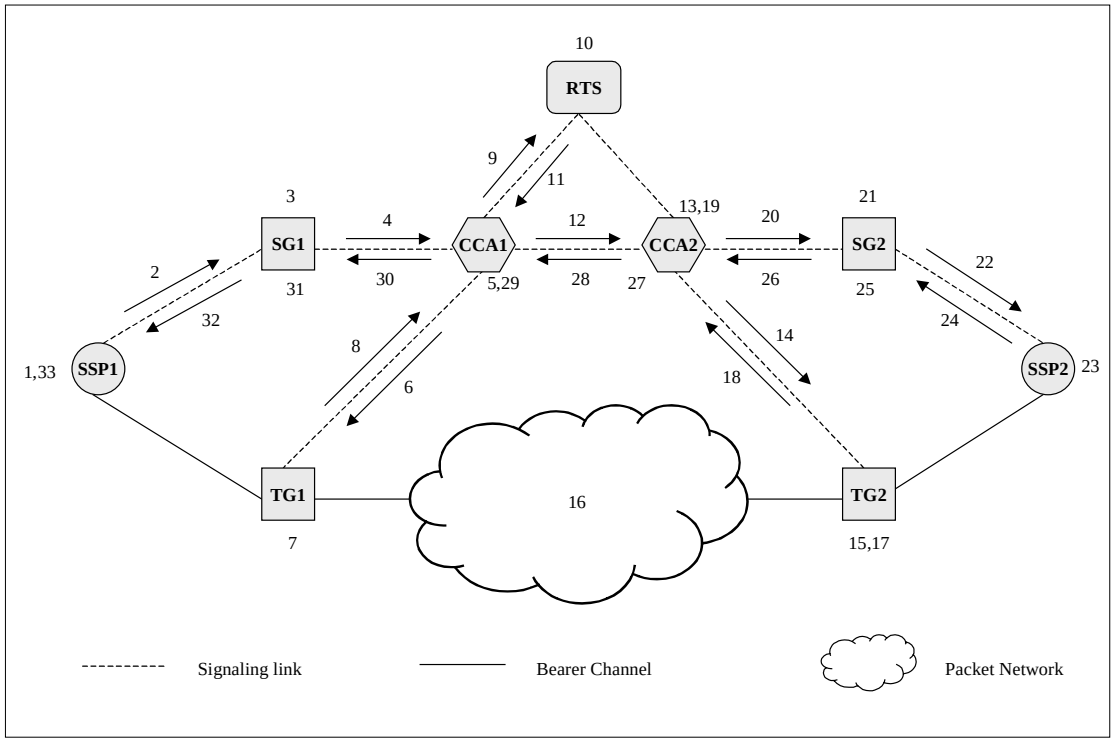

Figure C–1 A Message Flow for a Successful Call Setup

Overview

The message flow in Figure C–1 can be broken down into nine major components:

1. SSP1 sends a "connect request" to CCA1. (Steps 1 through 4)
2. CCA1 instructs TG1 to switch the incoming trunk through to an outgoing virtual circuit. (Steps 5 through 8)
3. CCA1 queries the RTS to determine the address of a CCA serving the terminating PSTN switch (i.e., SSP2). (Steps 9 through 11)
4. CCA1 sends a "connect request" to CCA2. (Step 12)

5. CCA2 instructs TG2 to switch a virtual circuit through to a trunk going to SSP2, and TG2 establishes a virtual circuit to TG1. (Steps 13 through 18)
6. CCA2 sends a “connect request” to SSP2, and SSP2 completes the call setup (e.g., provides power and audible ringing). (Steps 19 through 23)
7. After SSP2 provides power ringing, it returns a “connect acknowledgement.” This acknowledgement passes through SG2, CCA2, CCA1, and SG1 before arriving at SSP1. (Steps 24 through 33)
8. When the Called Party answers, SSP2 removes audible and power ringing, switches the trunk through to the access line, and returns an “answer message.” This “answer message” propagates back to SSP1 in the same way that the “connect acknowledgement” did.
9. SSP1 switches through the call in the forward direction, and the call setup is complete.

The remainder of this section describes the message flow in Figure 4-10 in further detail. The first phase of a call setup is the delivery of a “connect request” to CCA1. The next four steps accomplish this task.

1. Call processing at SSP1

- Receives the dialed digits from the Calling Party.
- Selects and reserves (i.e., marks "busy") an outgoing trunk based on the dialed digits.
- Switches the access line through to the trunk in the backward direction.
- Determines the PC of the switch at the far end of the reserved trunk. In this case, it's the PC of SG1 because SG1, TG1, and CCA1 form a virtual switch.
- Sends an IAM.

2. SS7 IAM containing the following parameters:

- DPC = PC of SG1.
- OPC = PC of SSP1.
- SLS code.
- CIC = identity of the trunk between SSP1 and TG1.
- Calling Party Number (CpPN) parameter.
- Called Party Number (CdPN) parameter.
- Other ISUP parameters.

3. Protocol interworking at SG1

- Performs MTP level 1 and 2 functions (e.g., signaling link flow control and error detection).
- Extracts the Signaling Information Field (SIF) (i.e., the OPC, DPC, SLS, and ISUP data) from the IAM.
- Encapsulates the SIF in a Protocol_A Transport_Message.

4. **Protocol_A Transport_Message containing the following parameters:**

   - Destination_address = address of CCA1.
   - Origination_address = address of SG1.

C.1.3. SIF from IAM

After receiving a “connect request,” CCA1 should instruct TG1 to switch the incoming trunk through to an outgoing virtual circuit. CCA1 and TG1 must also reserve any resources needed. The following four steps achieve these objectives.

5. **Call processing at CCA1**

   - Determines the following information based on the OPC and CIC in the SIF.
     - The TG involved in the call. In this case, it's TG1.
     - The channel_number of the trunk between SSP1 and TG1.
   - Marks the trunk "busy" if dual seizure has not occurred.
   - Instructs TG1 to switch through the connection.

6. **Protocol_B Connect_Message containing the following parameters:**

   - Destination_address = address of TG1.
   - Origination_address = address of CCA1.
   - Channel_number = identity of the trunk between SSP1 and TG1.

7. **Call processing at TG1**

   - Reserves (i.e., marks "busy") the trunk identified by the channel_number in the Connection_Message.
   - Reserves a Voice to Packet Converter (VPC).
   - Reserves an outgoing virtual circuit and determines a port_identifier for the virtual circuit.
   - Switches the incoming trunk through to the VPC and the VPC through to the virtual circuit (in both directions).

8. **Protocol_B Connect_Acknowledgement_Message containing the following parameters:**

   - Destination_address = address of CCA1.
   - Origination_address = address of TG1.
   - Channel_number = identity of the trunk between SSP1 and TG1.
   - Port_identifier = identity of the outgoing virtual circuit at TG1.
   - Status = successful connection setup.

   After successfully switching through the call in TG1, CCA1 should query the RTS to determine the address of the CCA serving the terminating PSTN switch (i.e., SSP2). The next three steps provide that address.

9. Protocol_C Routing_Query containing the following parameters:

- Destination_address = address of RTS.
- Origination_address = address of CCA1.
- Transaction_identifier = a number used by CCA1 to correlate a response to a query.
- TG_address = address of TG1.
- CdPN from the IAM.

10. Routing and Translation Server

- Determines the address of the CCA that serves the terminating PSTN switch given that the call has already been routed to TG1.

11. Protocol_C Routing_Response containing the following parameters:

- Destination_address = address of CCA1.
- Origination_address = address of RTS.
- Transaction_identifier = the same number as in the Routing_Query.
- Routing_address = address of the CCA that serves the terminating PSTN switch. In this case, it is CCA2.

After receiving the address of the CCA serving SSP2, CCA1 should send the following “connect request.”

12. Protocol_D Setup_Message containing the following parameters:

- Destination_address = address of CCA2.
- Origination_address = address of CCA1.
- TG_address = address of TG1.
- Port_identifier = identity of the virtual circuit at TG1.
- CdPN and CgPN from the IAM.

Other ISUP parameters from the IAM (e.g., Charge Number and Originating Line Information for billing purposes, Redirecting Number and Redirecting Information for Call Forwarding).

When CCA2 receives the “connect request,” it should instruct TG2 to switch a virtual circuit through to a trunk going to SSP2. CCA2 and TG2 must also reserve any resources needed. Furthermore, the virtual circuit between TG1 and TG2 should be established at this time. The next six steps accomplish these tasks.

13. Call processing at CCA2

- Determines an appropriate TG based on the Origination_address and/or the TG_address in the received Setup_Message. In this case, it is TG2.
- Determines the appropriate terminating PSTN switch based on the CdPN in the Setup_Message. In this case, it’s SSP2.
- Reserves (i.e., marks "busy") a trunk from TG2 to SSP2.

- Determines the channel_number of the trunk.

14. Protocol_B Connect_Message containing the following parameters:

- Destination_address = address of TG2.
- Origination_address = address of CCA2.
- Channel_number = identity of the trunk from TG2 to SSP2.
- Remote_TG_address = TG_address that CCA2 received in the Setup_Message = address of TG1.
- Remote_port_identifier = port_identifier that CCA2 received in the Setup_Message = identity of the virtual circuit at TG1.

15. Call processing at TG1

- Reserves (i.e., marks "busy") the trunk specified by the channel_number.
- Reserves a VPC.
- Reserves an outgoing virtual circuit and determines a port_identifier for the virtual circuit.

16. Packet network

- Creates a virtual circuit in the backward direction using the TG_address, port_identifier, remote_TG_address, and remote_port_identifier.

17. Call processing at TG1

- Switches the trunk through to the VPC and the VPC through to the virtual circuit (in both directions).
- Returns a Connect_Acknowledgement_Message to CCA2.

18. Protocol_B Connect_Acknowledgement_Message

- Destination_address = address of CCA2.
- Origination_address = address of TG2.
- Channel_number = identity of the trunk from TG2 to SSP2.
- Status = successful connection setup.

After successfully switching through the call in TG2, CCA2 should send a “connect request” to SSP2, and SSP2 should complete the call setup (e.g., provide power and audible ringing). The next five steps achieve these objectives.

19. Call processing at CCA2

- Determines the following information based on the trunk reserved for the call.
- The PC of the PSTN switch at the far end of the trunk.
- The CIC of the trunk.
- Determines the address of the SG serving the terminating PSTN switch.
- Generates the SIF for an IAM. The SIF includes the CdPN, CgPN, and other ISUP parameters from the received Setup_Message.

20. Protocol_A Transport_Message containing the following parameters:

- Destination_address = address of SG2.
- Origination_address = address of CCA2.
- SIF for an IAM.

21. Protocol interworking at SG2

- Extracts the SIF from the Transport_Message and creates and IAM by adding MTP level 1 and 2 information.
- Performs MTP level 1 and 2 functions (e.g., signaling link flow control).

22. SS7 IAM containing the following parameters:

- DPC = PC of SSP2.
- OPC = PC of SG2.
- SLS code.
- CIC = identity of the trunk from TG2 to SSP2.
- Other ISUP data from the Transport_Message.

23. Call processing at SSP2

- Marks the incoming trunk "busy" if dual seizure has not occurred.
- Performs any vertical services required.
- Applies audible ringing to the trunk.
- Applies power ringing to the access line serving the Called Party.

After power ringing has been applied, SSP2 should return a "connect acknowledgement." This acknowledgement passes through SG2, CCA2, CCA1, and SG1 before arriving at SSP1. At that time, timer T_{IAM} is cancelled. The remaining steps in this subsection describe how this acknowledgement travels through the network.

24. SS7 ACM containing the following parameters:

- DPC = PC of SG2.
- OPC = PC of SSP2.
- SLS code.
- CIC = identity of the trunk from TG2 to SSP2.

25. Protocol interworking at SG2

- Performs MTP level 1 and 2 functions (i.e., signaling link flow control and error detection).
- Extracts the SIF from the ACM.
- Encapsulates the SIF in a Protocol_A Transport_Message.

26. Protocol_A Transport_Message containing the following parameters:

- Destination_address = address of CCA2.

- Origination_address = address of SG2.
- SIF from ACM.

27. Call processing at CCA2

- Determines the following information based on the OPC and CIC in the SIF.
  - The addresses of the preceding CCA and TG (i.e., the addresses of CCA1 and TG1).
  - The port_identifier of the virtual circuit at the preceding TG.

28. Protocol_D Setup_Acknowledgement_Message containing the following parameters:

- Destination_address = address of CCA1.
- Origination_address = address of CCA2.
- TG_address = address of TG1.
- Port_identifier = identity of the virtual circuit at TG1.

29. Call processing at CCA1

- Determines the following information based on the TG_address and port_identifier in the received Setup_Acknowledgement_Message.
  - The PC of the originating PSTN switch. In this case, it's the PC of SSP1.
  - The CIC of the trunk from the TG to the originating PSTN switch.
- Generates the SIF for an ACM.
- Determines the address of the SG serving the originating PSTN switch. In this case, it is SG1.

30. Protocol A: Transport_Message containing the following parameters:

- Destination_address = address of SG1.
- Origination_address = address of CCA1.
- SIF for the ACM.

31. Protocol interworking at SG1

- Extracts the SIF from the Transport_Message and creates and ACM by adding MTP level 1 and 2 information.
- Performs MTP level 1 and 2 functions (e.g., signaling link flow control).

32. SS7 ACM containing the following parameters:

- DPC = PC of SSP1.
- OPC = PC of SG1.
- SLS code.
- CIC = identity of the trunk from TG1 to SSP1.

33. Call processing at SSP1

- Cancels timer T_{IAM}.

When the Called Party answers the call (i.e., goes off-hook), SSP2 should remove audible ringing from the incoming trunk and power ringing from the access line. At that time, SSP2 should switch through the call in both directions and send an "answer message" (i.e., an ANM) to SG2. The "answer message" propagates back to SSP1 in the same way that the "connect acknowledgement" did (i.e., steps (24) through (32) above). When SSP1 receives the "answer message," it will switch through the call in both directions, and the call setup will be complete.

C.1.4 A Successful Call Release Initiated by the Calling Party

The message flow in this section describes a successful call release across the network shown in Figure C–2. Note again that the message flow in this section is only an example.

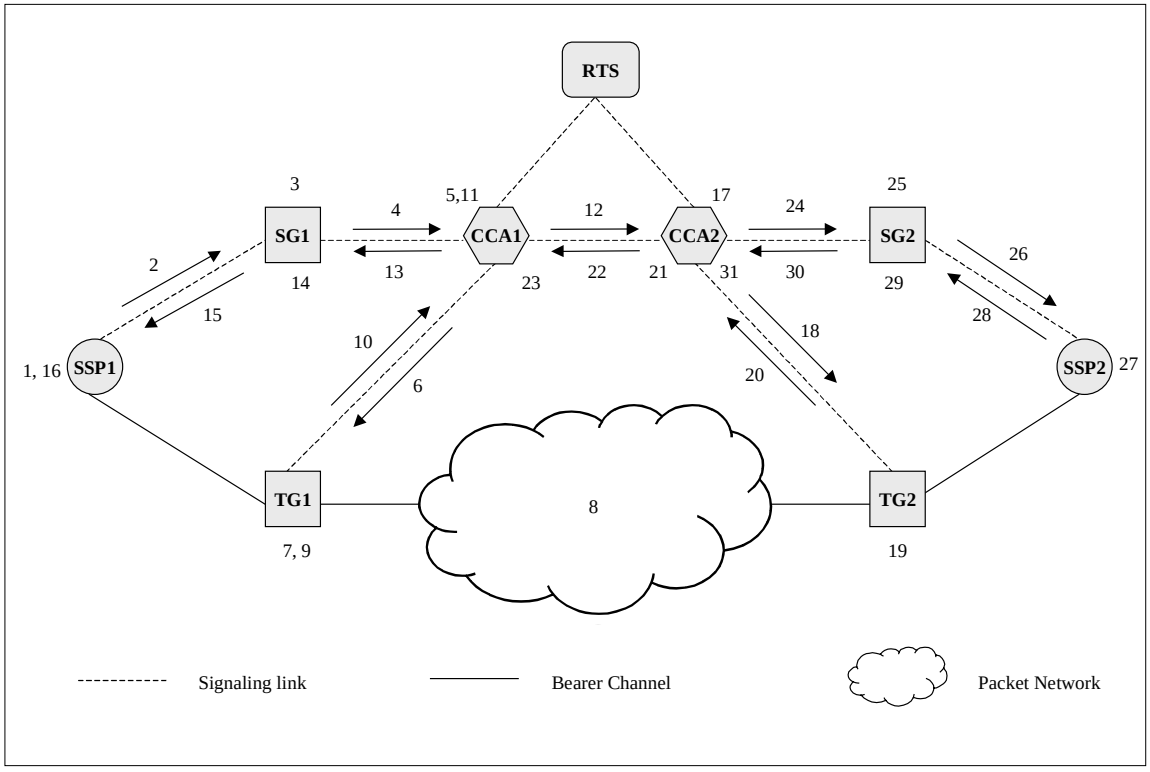

Figure C–2 A Message Flow for a Successful Call Release Initiated by the Calling Party

Overview

The message flow in Figure C–2 can be broken down into six major components:

1. SSP1 sends a "disconnect request" to the CCA1. (Steps 1 through 4)
2. CCA1 instructs TG1 to release the incoming trunk, the VPC, and the outgoing virtual circuit. (Steps 5 through 10)

3. CCA1 sends a “disconnect request” to CCA2 and a “disconnect acknowledgement” to the originating PSTN switch. (Steps 11 through 16)
4. CCA2 instructs TG2 to release the incoming virtual circuit, the VPC, and the outgoing trunk. (Steps 17 through 20)
5. CCA2 sends a “disconnect request” to SSP2 and a “disconnect acknowledgement” to CCA1. (Steps 21 through 26)
6. SSP2 releases the trunk and access line and returns a “disconnect acknowledgement” to CCA2. (Steps 27 through 31).

The remainder of this subsection describes the message flow in Figure C–2 in further detail. The first phase of a call release is the delivery of a “disconnect request” to the CCA1. The next four steps accomplish this task.

1. Call processing at SSP1

- Receives an on-hook indication from the Calling Party.
- Determines the PC of the switch at the far end of the trunk reserved for the call. In this case, it’s the PC of SG1 because SG1, TG1, and CCA1 form a virtual switch.
- Releases the outgoing trunk and access line.
- Sends an REL.

2. SS7 REL containing the following parameters:

- DPC = PC of SG1.
- OPC = PC of SSP1.
- SLS code.
- CIC = identity of the trunk between SSP1 and TG1.

3. Protocol interworking at SG1

- Performs MTP level 1 and 2 functions (e.g., signaling link flow control and error detection).
- Extracts the SIF.
- Encapsulates the SIF in a Protocol_A Transport_Message.

4. Protocol_A Transport_Message containing the following parameters:

- Destination_address = address of CCA1.
- Origination_address = address of SG1.
- SIF from the REL.

After receiving a “disconnect request,” CCA1 should instruct TG1 to release the incoming trunk, the VPC, and the outgoing virtual circuit. The following six steps achieve these objectives.

5. Call processing at CCA1

- Determines the following information based on the OPC and CIC in the SIF.

- The TG involved in the call. In this case, it's TG1.
- The channel_number of the trunk.

6. Protocol_B Disconnect_Message containing the following parameters:

- Destination_address = address of TG1.
- Origination_address = address of CCA1.
- Channel_number = identity of the trunk between SSP1 and TG1.

7. Call processing at TG1

- Identifies the incoming trunk, VPC, and outgoing virtual circuit associated with the call using the channel_number in the Disconnect_Message.
- Disconnects the incoming trunk from the VPC and the VPC from the virtual circuit.
- Idles the VPC and trunk.

8. Packet network

- Releases the virtual circuit associated with the call.

9. Call processing at TG1

- Idles the virtual circuit.
- Returns a Disconnect_Acknowledgement_Message to CCA1.

10. Protocol_B Disconnect_Acknowledgement_Message containing the following parameters:

- Destination_address = address of CCA1.
- Origination_address = address of TG1.
- Channel_number = identity of the trunk between SSP1 and TG1.
- Status = successful release.

After successfully releasing the call in TG1, CCA1 should send a "disconnect request" to CCA2 and a "disconnect acknowledgement" to the originating PSTN switch.

11. Call processing at CCA1

- Determines the following information based on the TG_address and channel_number in the received Disconnect_Acknowledgement_Message:
  - The PC of the originating PSTN switch. In this case, it is the PC of SSP1.
  - The CIC of the trunk from TG1 to the SSP1.
  - The port_identifier of the (just released) virtual circuit at TG1.
  - The address of the next CCA associated with the call. In this case, it's CCA2.
- Idles the trunk.
- Sends a Teardown_Message to CCA2.

- Determines the address of the SG serving the originating PSTN switch. In this case, it's the address of SG1.
- Generates the SIF for an RLC and sends it to SG1.

12. Protocol_D Teardown_Message containing the following parameters:

- Destination_address = address of CCA2.
- Origination_address = address of CCA1.
- TG_address = address of TG1.
- Port_identifier = identity of the (just released) virtual circuit at TG1.

13. Protocol_A Transport_Message containing the following parameters:

- Destination_address = address of SG1.
- Origination_address = address of CCA1.
- SIF for the RLC.

14. Protocol interworking at SG1

- Extracts the SIF from the Transport_Message and creates an RLC by adding MTP level 1 and 2 information.
- Performs MTP level 1 and 2 functions (e.g., signaling link flow control).

15. SS7 RLC containing the following parameters:

- DPC = PC of SSP1.
- OPC = PC of SG1.
- SLS code.
- CIC = identity of the trunk from TG1 to SSP1.

16. Call processing at SSP1

- Idles the trunk specified by the CIC in the RLC.

After receiving a "disconnect request," CCA2 should instruct TG2 to release the incoming trunk, the VPC, and the outgoing virtual circuit. The next four steps accomplish these tasks.

17. Call processing at CCA2

- Determines the following information based on the TG_address and port_identifier in the received Teardown_Message:
  - The address of the TG associated with the call. In this case, it's TG2.
  - The channel_number of the trunk reserved for the call.

18. Protocol_B Disconnect_Message containing the following parameters:

- Destination_address = address of TG2.
- Origination_address = address of CCA2.
- Channel_number = identity of the trunk between TG2 and SSP2.

19. Call processing at TG2

- Identifies the incoming virtual circuit, VPC, and outgoing trunk associated with the call using the channel_number in the Disconnect_Message.
- Disconnects the trunk from the VPC and the VPC from the virtual circuit.
- Idles the trunk, VPC, and virtual circuit
- Returns a Disconnect_Acknowledgement_Message to CCA2.

20. Protocol_B Disconnect_Acknowledgement_Message containing the following parameters:

- Destination_address = address of CCA2.
- Origination_address = address of TG2.
- Channel_number = identity of the trunk between TG2 and SSP2.
- Status = successful release.

After successfully releasing the call in TG2, CCA2 should send a "disconnect request" to SSP2 and a "disconnect acknowledgement" to CCA1.

21. Call processing at CCA2

- Determines the following information based on the TG_address and channel_number in the received Disconnect_Acknowledgement_Message:
  - The PC of the terminating PSTN switch. In this case, it's the PC of SSP2.
  - The CIC of the trunk from the TG to the terminating PSTN switch.
  - The address of the previous CCA and TG associated with the call. In this case, it's CCA1 and TG1.
  - The port_identifier of the (just released) virtual circuit at TG1.
- Sends a Teardown_Acknowledgement_Message.
- Determines the address of the SG serving the terminating PSTN switch.
- Generates the SIF for an REL and sends it to SG2.

22. Protocol_D Teardown_Acknowledgement_Message containing the following parameters:

- Destination_address = address of CCA1.
- Origination_address = address of CCA2.
- TG_address = address of TG1.
- Port_identifier = identity of the (just released) virtual circuit at TG1.

23. Call processing in CCA1

- Idles the trunk associated with the TG_address and port_identifier in the received Teardown_Acknowledgement_Message.

24. Protocol_A Transport_Message containing the following parameters:

- Destination_address = address of SG2.

- Origination_address = address of CCA2.
- SIF for the REL.

25. Protocol interworking at SG2

- Extracts the SIF from the Transport_Message and creates an REL by adding MTP level 1 and 2 information.
- Performs MTP level 1 and 2 functions (e.g., signaling link flow control).

26. SS7 REL containing the following parameters:

- DPC = PC of SSP2.
- OPC = PC of SG2.
- SLS code.
- CIC = identity of the trunk from TG2 to SSP2.

After receiving a "disconnect request," SSP2 should release the trunk and the access line and return a "disconnect acknowledgement" to CCA2. When CCA2 receives the "connection acknowledgement," it should idle the trunk between TG2 and SSP2. The remaining steps describe these actions.

27. Call processing at SSP2

- Idles the incoming trunk and access line.
- Returns an RLC.

28. SS7 RLC containing the following parameters:

- DPC = PC of SG2.
- OPC = PC of SSP2.
- SLS code.
- CIC = identity of the trunk from TG2 to SSP2.

29. Protocol interworking at SG2

- Performs MTP level 1 and 2 functions (i.e., signaling link flow control and error detection).
- Extracts the SIF from the RLC.
- Encapsulates the SIF in a Protocol_A Transport_Message.

30. Protocol_A Transport_Message containing the following parameters:

- Destination_address = address of CCA2.
- Origination_address = address of SG2.
- SIF from RLC.

31. Call processing at CCA2

- Idles the trunk identified by the OPC and CIC in the SIF in the received Transport_Message.

C.1.5. Difficulty in Managing Remote Resources

This section highlights a potential difficulty that a CCA may experience when managing a TG's resources. This difficulty exists even when all of the assumptions in Section 4.3.1.1 are met.

Specifically, assumption 9 states that each CCA will contain a status map that tracks the busy/idle state of each trunk terminating at its subordinate TGs. Call processing in each CCA will use this status map to signal and route calls appropriately.

The separation of the busy/idle state of a trunk in a CCA from its actual state in a TG may cause a difficulty. Should the two states go out of sync, call processing in the CCA could make incorrect decisions and cause a reduction in call throughput at the TG.

To keep these states in sync, the protocol between a CCA and a TG should be designed to minimize such synchronization errors. Including an "audit" message, which could be sent by a CCA to collect and return the status of a TG's resources, is one possible solution [9]. When the CCA receives an "audit response," it would update its status map according to the contents of the message.

Such auditing of a TG's resources, however, can corrupt an otherwise accurate status map in a CCA unless sufficient safeguards are devised. In particular, corruption can occur when a TG processes messages in the order that is different than their creation order in a CCA. This reordering may be caused by the TG's architecture (e.g., distributed) or by the network between a CCA and a TG altering the sequencing of messages.

To prevent such corruption, the network link between a CCA and a TG should ensure that messages are delivered in the order that they are sent. One drawback of MGCP is that messages are transmitted over UDP, which does not ensure message sequencing. Additionally, the CCAs and/or the TGs may need more sophisticated state machines or the CCAs may need to time-stamp messages as they are created so that a TG can execute them in the same sequence. At this time, MGCP messages have transaction identifiers but no time-stamps or sequence numbers. Further work is needed to ensure that MGCP manages remote resources well. Alternately, a different auditing mechanism may be useful.

The remainder of this subsection provides an example message flow between CCA1 and TG1 in Figure C–2 that would cause an error in CCA1's status map. This error would occur without CCA1, TG1, or SSP1 knowing that it happened and would cause SSP1 to repeatedly drop new calls.

To begin, suppose a call has been setup on a trunk between SSP1 and TG1 using the message flow in Subsection 4.3.1.2. Then the state of that trunk in both CCA1 and TG1 will be "busy." Next, suppose that the calling party initiates the release described in Subsection 4.3.1.3 only this time CCA1 generates an "Audit" message just prior to the Disconnect_Message at step (5). Then the following steps may occur:

[9] In fact, MGCP has two such "audit" messages: Audit Connection and Audit Endpoint.

5a) Call Processing at CCA1

- Sends an Audit_Message to TG1.

5b) Call processing at CCA1

- Determines the following information based on the OPC and CIC in the SIF.
  - The TG involved in the call. In this case, it's TG1.
  - The channel_number of the trunk.
- Sends a Disconnect_Message to TG1.

6a) Protocol_B Audit_Message containing the following parameters:

- Destination_address = address of TG1.
- Origination_address = address of CCA1.

6b) Protocol_B Disconnect_Message containing the following parameters:

- Destination_address = address of TG1.
- Origination_address = address of CCA1.
- Channel_number = identity of the trunk between SSP1 and TG1.

7a) Call_Processing at TG1

- Starts the audit of TG1's resources.
- Determines that the trunk that is about to be released is busy.

7b) Call processing at TG1

- Identifies the incoming trunk, VPC, and outgoing virtual circuit associated with the call using the channel_number in the Disconnect_Message.
- Disconnects the incoming trunk from the VPC and the VPC from the virtual circuit.
- Idles the VPC and trunk.

The trunk is now marked "idle" in TG1 and "busy" in CCA1.

8) Packet network

- Releases the virtual circuit associated with the call.

9a) Call processing at TG1

- Idles the virtual circuit.
- Returns a Disconnect_Acknowledgement_Message to CCA1.

9b) Call processing at TG1

- Completes the audit of TG1's resources.
- Returns an Audit_Acknowledgement_Message to CCA1.

10a) Protocol_B Disconnect_Acknowledgement_Message containing the following parameters:

- Destination_address = address of CCA1.
- Origination_address = address of TG1.
- Channel_number = identity of the trunk between SSP1 and TG1.
- Status = successful release.

10b) Protocol_B Audit_Acknowledgement_Message containing the following parameters:

- Destination_address = address of CCA1.
- Origination_address = address of TG1.
- Audit_information = information about the status of TG1's trunks including the fact that the trunk that was just idled in step (7b) is "busy."
- Status = successful audit.

11a) Call processing at CCA1

- Determines the following information based on the TG_address and channel_number in the received Disconnect_Acknowledgement_Message:
  - The PC of the originating PSTN switch. In this case, it's the PC of SSP1.
  - The CIC of the trunk from TG1 to the SSP1
  - The port_identifier of the (just released) virtual circuit at TG1
  - The address of the next CCA associated with the call. In this case, it's CCA2.
- Idles the trunk.
- Sends a Teardown_Message to CCA2.
- Determines the address of the SG serving the originating PSTN switch. In this case, it's the address of SG1.
- Generates the SIF for an RLC and sends it to SG1.

The trunk is now marked "idle" in both TG1 and CCA1 (as it should be).

11b) Call processing at CCA1

- Marks the trunk that was just idled in step (11a) "busy" based on the content of the Audit_Acknowledgement_Message.

At this point, the trunk is marked "idle" in TG1 and "busy" in CCA1. Also, neither CCA1 nor TG1 knows that an error exists.

While uncorrected, CCA1 should discard any "connect request" involving the trunk (provided call processing follows the procedures in GR-317-CORE). Whenever that happens, timer T_{IAM} in SSP1 should eventually expire, and SSP1 should terminate the call. Thus, SSP1 should drop all calls attempted on the trunk until the error in CCA1 is corrected. Furthermore, SSP1 will not detect the error in CCA1 because SS7 networks legitimately drop IAMs in some cases (e.g., congestion).

References

1. **GB910,** *SMART TMN™ Telecom Operations Map (TOM),* Version 1.0, (TeleManagement Forum, October 1998).

2. **GR-317-CORE,** *Switching System Generic Requirements for Call Control Using Integrated Services Digital Network User Part (ISDNUP)* Issue 2 (Bellcore, December 1997) plus Revision 1, November 1998.

3. **GR-394-CORE,** *Switching System Generic Requirements for Interexchange Carrier Interconnection Using the Integrated Services Digital Network User Part (ISDNUP) (A module of LSSGR, FR-64)* Issue 2 (Bellcore, December 1997) plus Revision 1, November 1998.

4. **GR-508-CORE,** *Automatic Message Accounting (AMA) Section 8 (A Module of LSSGR, FR-6),* Issue 2 (Bellcore, December 1997).

5. **GR-1100-CORE,** *Bellcore Automatic Message Accounting (AMA) Format (BAF) Requirements*, Issue 2 (Bellcore, December 1997) plus Revisions.

6. **GR-1298-CORE,** *AINGR: Switching System (A module of AINGR, FR-15)* Issue 4 (Bellcore, September 1997) plus Revision 1, October 1998.

7. **GR-2869-CORE,** *Generic Requirements Based on the Telecommunications Management Network (TMN) Architecture,* Issue 2, (Bellcore, October 1996).

8. **IETF internet draft,** "draft-ietf-ippm-ipdv-02.txt" , G. Almes, S. Kalidindi.

9. **IETF internet draft,** "draft-ietf-ippm-delay-05.txt", G. Almes, S. Kalidindi.

10. **IETF internet draft,** "draft-ietf-ippm-loss-05.txt", G. Almes, S. Kalidindi.

11. **IETF RFC 2330**, *Framework for IP performance Metrics.*

12. **ITU-T Recommendation I.35IP**.

13. **ITU-T Recommendation I.380**.

14. **ITU-T Recommendation I.356.**

15. **ITU-T Recommendation M.3010,** *Principles for a Telecommunications Management Network (TMN),* 1996.

16. **ITU-T Recommendation M.3400,** *TMN Management Functions,* 1996.

17. *Legacy Network and Voice Over the Internet* (Yankee Group, March 1998).

18. **MDP-326-140**, *Digital Channel Bank—Requirements and Objectives* (formerly known as AT&T PUB 43801), November 1982.

19. *Packetized Voice Services: 1997 Market Assessment and Forecast* (International Data Corporation [IDC], January 1998).

20. **SR-504,** *SPCS Capabilities and Features (A Module of LSSGR, FR-64),* Issue 1 (Bellcore, March 1996).

21. **SR-4619,** *1999 Version of National ISDN PRI CPE Generic Guidelines,* Issue 1 (Bellcore, December 1998).

22. **SR-4620**, *1999 Version of National ISDN Basic Rate Interface (BRI) Customer Premise Equipment Generic Guidelines,* Issue 1 (Bellcore, December 1998).

23. *Telecommunications—The Battle for the Last Mile* (Jupiter Communications/Wall Street Journal Reports, September 21, 1998).

24. **TR-NWT-000444,** *Switching System Requirements Supporting ISDN Access Using the ISDN User Part,* Issue 3 (Bellcore, May 1993).

NOTE:

All Bellcore documents are subject to change, and their citation in this document reflects the most current information available at the time of this printing. Readers are advised to check current status and availability of all documents.

To Contact Bellcore

Bellcore Customer Service
8 Corporate Place, Room 3A-184
Piscataway, New Jersey 08854-4156
1-800-521-CORE (2673) (USA and Canada)
(732) 699-5800 (all others)
(732) 336-2559 (FAX)

To Order Documents

- Perform the following steps to order from the online catalog:

1. Enter the URL line: telecom-info.bellcore.com
2. Click on the Search button located on top
3. In the Keywords filed, enter the document number (or keywords), then click on Submit Search

or

1. Enter the above URL line
2. Click on the Browse button located on top, then click on the subject of interest.

- Bellcore employees should perform the following steps:

1. Access the Bellcore Internal Home Page
2. Click on the Marketwise button located on top
3. Click on DOCS - Bellcore Product Catalog
4. Enter data in one or more of the files (e.g., enter a document number in the Product Number field), then follow the instructions to search the online catalog.

Glossary

3G	Third Generation Wireless
A to D	Analog to Digital
AAL2	Adaptation Layer Type 2
AAL5	Adaptation Layer Type 5
ABS	Alternate Billing Services
AC	Automatic Callback
ACR	Anonymous Call Rejection
ADPCM	Adaptive Differential PCM
ADSI	Analog Display Services Interface
ADSL	Asynchronous Digital Subscriber Line
AESA	ATM End System Address
AG	Access Gateway
AIN	Advanced Intelligent Network
AINI	Advanced Intelligent Network Interface
AMA	Automatic Message Accounting
ANM	Answer Message
ANSI	American National Standards Institute, Inc.
AON	Active Optical Network
API	Application Programming Interface
AR	Automatic Recall
ASOG	Access Service Ordering Group
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
BA	Billing Agent
BAF	Bellcore AMA Format
BBG	Basic Business Group
BCLID	Bulk Calling Line Identification
BCM	Basic Call Model
BICI	Broadband Inter-Carrier Interface
B-ISDN	B-Integrated Services Digital Network
B-ISUP	B-Integrated Services Digital Network User Part
BML	Business Management Layer
BRI	Basic Rate Interface
BSC	Business Service Center
BTS	Business Tracking System
CALEA	Communications Assistance for Law Enforcement Act
CATV	Community Antenna Television (cable TV)
CBR	Constant Bit Rate
CCA	Call Connection Agent
CCA	Call Connection Agent
CCS	Common Channel Signaling
CCW	Cancel Call Waiting
CDMA	Code Division Multiple Access
CdPN	Called Party Number
CDR	Call Data Record
CELP	Code Excited Linear Prediction

CFB	Call Forwarding on Busy Line
CFBL	Call Forwarding on Busy Line
CFDA	Call Forwarding on No Answer
CFV	Call Forwarding Variable
CG	Customer Gateway
CgPN	Calling Party Number
CIC	Carrier Identification Code
CIDCW	Caller Identity Delivery on Call Waiting
CIOA	Classical IP over ATM
CLC	Carrier Liaison Committee
CLECs	Competitive Local Exchange Carriers ,
CMIP	Common Management Interface Protocol
CNAM	Calling Name Delivery
CND	Calling Number Delivery
CNU	Coaxial Network Units
CORBA	Common Object Request Broker Architecture
CORBA	Common Object-oriented Request Broker Architecture
COT	Customer Originated Trace
CP	Call Pickup
CPE	Customer Premises Equipment
CPN	Calling Party Number
CT	Call Transfer
CW	Call Waiting
CWD	Call Waiting Deluxe
D to A	Digital to Analog
DC	Direct Current
DCP	Directed Call Pickup
DID	Direct Inward Dialing
DLC	Digital Loop Carrier
DNS	Domain Name Servers
DOCSIS	Data-Over-Cable Service Interface Specifications
DOD	Direct Outward Dialing
DOE	Direct Order Entry
DPC	Destination Point Code
DR/CW	Distinctive Ringing/Call Waiting
DS	Digital Service
DSLAM	Digital Subscriber Line Access Multiplexer
DTMF	Dual Tone MultiFrequency
DWDM	Dense Wavelength Division Multiplexing
EKTS	Electronic Keyboard Telephone Service
EML	Element Management Layer
EMS	Element Management System
ETSI	European Telecommunications Standards Institute
FE	Functional Element
FIB	Forwarding Information Base
FIFO	First In First Out
FSK	Frequency Shift Key
FTP	File Transfer Protocol
FTTC	Fiber to the Curb

FTTH	Fiber to the Home
GII	Global Information Infrastructure
GMSC	Gateway Mobile Switching Center
GR	Bellcore Generic Requirement
GR	Generic Requirement
HDT	Host Digital Terminal
HFC	Hybrid Fiber-Coax
IAM	Initial Address Message
IDC	International Data Corporation
IETF	Internet Engineering Task Force
IGMP	Internet Group Multicast Protocol
ILEC	Incumbent Local Exchange Carrier
IN	Intelligent Network
IP	Internet Protocol
IPsec	IP Security
IPTEL	IP Telephony
ISDNUP	ISDN User Part
ISP	Independent Service Provider or
ISP	Internet Service Provider
ISUP	Integrated Services Digital Network User Part
IT	Information Technology
ITCM	Integrated Telephony Cable Modem
ITESF	Internet Traffic Engineering Solutions Forum
ITU	International Telecommunication Union
IXC	International Exchange Carrier
LAN	Local Area Network
LANE	LAN Emulation
LAPD	Link Access Protocol for the D-channel
LD	Long Distance
LDP	Label Distribution Protocol
LEC	Local Exchange Carrier
LEC SPCS	Local Exchange Carrier Stored Program Control System
LIDBs	Line Information Databases
LLA	Logical Layer Architecture
LMDS	Local Multipoint Distribution Service
LNP	Local Number Portability
LSOG	Local Service Ordering Group
LSP	Label Switched Path
LSR	Label Switching Router
MAF	Management Application Function
MAN	Metropolitan Area Network
MARS	Multicast Address Resolution Server
MCNS	Multimedia Cable Network System
MCS	Multicast Server
MEGACO	Media Gateway Control Working Group
MF	Multi-Frequency
MFA	Management Functional Area
MGCP	Media Gateway Control Protocol
MIB	Management Information Base

MLHG	Multi Line Hunt Group
MMUSIC	Multiparty Multimedia Session Control
MPLS	Multiprotocol Label Switching
MPOA	multiprotocol over ATM
MSC	Multiple System Coupling
MSR	Message Storage and Retrieval
MTP	Message Transfer Protocol
MTTR	Mean Time to Repair
MVDS	Multichannel Video Distribution Service
MWC	Multiway Calling
NANP	North American Numbering Plan
NE	Network Element
NEL	Network Element Layer
NFA	Network Facility Access
NGN	Next Generation Network
NHRP	Next Hop Resolution Protocol
N-ISDN	N-Integrated Services Digital Network
NM	Network Management
NML	Network Management Layer
NMS	Network Management System
NO	Network Operator
NPA	Numbering Plan Area
NPASM	NPA Split Management
NRC	Network Reliability Council
O&M	Operations and Management
O/E	Optical to Electrical
OACA	Outside Area Calling Alerting
OAM&P	Operations, Administration, Maintenance, and Provisioning
OBF	Ordering and Billing Forum
OCAA	Outside Area Calling Alerting
ONU	Optical Network Unit
OPC	Originating Point Code
OS	Operating System
OSS	Operations Support System
PBX	Private Branch Exchange
PC	Point Code
PCM	Pulse Code Modulation
PHB	Per-Hop Behavior
PINT	PSTN/Internet Interfaces
PISN	Private Integrated Services Network
PONs	Passive Optical Networks
POTS	Plain Old Telephone Service
PRI	Primary Rate Interface
PSAP	Public Safety Answering Point
PSDN	Packet Switched Data Network
PSN	Public-Switched Network
PSTN	Public Switched Telephone Network
PTN	Public Telecommunications Network
PVN	Private Virtual Networking

QOS	Quality of Service
QOS	Quality of Service
R&D	Research and Development
RADIUS	Remote Authentication Dial-In User Service
RC	Ring Control
RCF	Remote Call Forwarding
RDAS	Resident Distinctive Alerting Service
RED	Random Early Detection
REL	Release message
RES	Resume message
RF	Radio Frequency
RLC	Release Complete
RPP	Reliability Prediction Procedure
RSVP	Reservation Protocol
RT	Remote Terminal
RTA	Routing and Translation Agent
RTCP	Real-time Transfer Control Protocol
RTP	Real-time Transfer Protocol
RTS	Routing and Translation Server
RTSP	Real-Time Stream Protocol
SA	Service Agent
SAP	Session Announcement Protocol
SC	Series Completion
SCA	Selective Call Acceptance
SCCP	Simple Conference Control Protocol .
SCF	Selective Call Forwarding
SCN	Switched Circuit Networks
SCP	Service Control Point
SCR	Selective Call Rejection
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SF	Single Frequency
SG	Signaling Gateway
SGCP	Simple Gateway Control Panel
SIF	Signaling Information Field
SIGTRAN	Signaling Transport
SIO	Signaling Information Octet
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLE	Screening List Editing
SLS	Signaling Link Selection
SMDI	Simplified Message Desk Interface
SML	Service Management Layer
SMS	Service Management System
SMSC	Short Message Service Center
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SP	Service Provider
SPCS	Stored Program Control System

SR	Special Report
SS7	Signaling System 7
SSP	Service Switching Point
SSTP	Service Support Transfer Protocol
STP	Signaling Transfer Point
SUS	Suspend Message
SVC	Switched Virtual Circuit
T1A1	The Performance and Signal Processing Technical Subcommittee
TCA	Threshold Crossing Alert
TCAP	Transaction Capabilities Access Part .
TDM	Time Division Multiplexed
TDMA	Time Division Multiple Access
TEI	Terminal Endpoint Identifier
TG	Trunk Gateway
TGW	Functional Requirements section
TINA	Telecommunication Information Networking Architecture
TMN	Telecommunications Management Network
TSPs	Telecommunications Service Providers
TWC	Three-Way Calling
UDP	Update DIP Parameters
UNI	User Network Interface
UPS	Uninterrupted Power Supply
UPT	Universal Personal Telecommunications
VAD	Voice Activated Dialing
VANC	Voice Activated Network Control
VBR	Variable Bit Rate
VC	Vacant Code
VM/MWN	Voice Mail System for Message Waiting Notification
VMWI	Visual Message Waiting Indicator
VOIP	Voice over IP
VOP	Voice Over Packet
VPC	voice to packet converter
VPI/VCI	Virtual Path Identifier/V-Channel Indicator
VPN	Virtual Private Network
VSI	Virtual Switch Interface
VSLE	Visual Screening List Editing
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WG	Work Group
WS	Work Station
xDSL	Digital Subscriber Line

Telcordia Enterprise License Agreement and Limited Warranty

For Technical Documents: Generic Requirements (GRs), Special Reports (SRs), Technical References (TRs), Technical Advisories (TAs), Family of Requirements (FRs), Family of Documents (FDs), (collectively "Licensed Product(s)")

IMPORTANT! PLEASE READ CAREFULLY.

USE OF THIS LICENSED PRODUCT INDICATES THAT YOU (LICENSEE) HAVE READ AND ACCEPT THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH THE TERMS OF THIS AGREEMENT, YOU WILL NOT BE ALLOWED TO PURCHASE THIS LICENSED PRODUCT.

1. LICENSE GRANT

Telcordia Technologies Generic Requirements License Management, a division of Ericsson Inc. ("Telcordia"), grants to Licensee under this Enterprise License Agreement ("Agreement") a personal, non-exclusive, non-transferable, limited license to use this Licensed Product by employees of Licensee for internal business purposes only. All intellectual property rights, title and interest in all Licensed Product(s) furnished to Licensee remain in Telcordia. This License does not preclude the execution of additional license agreements with Licensee for the Licensed Product(s).

Telcordia has exclusive rights to all Licensed Product(s) which are protected by United States and international copyright laws.

2. LICENSEE'S USE:

a. Licensee may place the Licensed Product(s) on a server, internal web site, or other electronic computing platform shared or accessible to employees or affiliates of Licensee. Licensee may make paper and electronic copies of Licensed Product(s) as determined by Licensee to be necessary for Licensee's internal purposes; provided all copies, in whole or in part, of the Licensed Product(s) shall bear the same Telcordia copyright and disclaimer notices legend as appear on the Licensed Product(s) originally furnished to Licensee by Telcordia.
b. Subject to the preceding paragraph, and conditioned upon Licensee sublicensing the rights as set forth in the paragraph below, Licensee may reproduce and distribute Licensed Product(s) to "Affiliates" defined as (i) the parent entity (corporation or partnership) which directly or indirectly owns the majority of the outstanding shares or interests of Licensee, (ii) a sibling entity (corporation or partnership) the majority of whose outstanding shares or interests are owned by its parent entity, or (iii) a subsidiary entity (corporation or partnership) the majority of whose outstanding shares or interests are owned by Licensee, provided, however, that such entity shall continue to remain an Affiliate hereunder only as long as the applicable ownership interest as described above exists.

   Licensee may sublicense the rights granted in this section to an Affiliate, provided Licensee shall remain responsible for any breach by such Affiliate. Licensee shall ensure that such Affiliate agrees to be bound by the rights, obligations and limitations set forth herein, and Licensee shall ensure that Telcordia shall have the right of direct enforcement of such obligations against such Affiliate. If a direct enforcement claim is denied, for any reason, it is agreed that Telcordia may assert such claim against Licensee.

c. Licensee must treat the Licensed Product(s) like any other copyrighted material.
d. Licensee may reference Licensed Products in creating specifications and related documentation (the "Licensee Documentation").
e. Licensee may, in marketing or in conjunction with the sale of a product or related services (collectively, "Licensee Product"), make reference to the Licensed Product utilized in the development of Licensee Product; provided that Licensee shall make no statement, representation or warranty on behalf of Telcordia, including but not limited to, a certification by Telcordia of a product's or related service's compliance with the Licensed Product, unless otherwise agreed to by the parties in writing.

f. The foregoing license does not include the right to make copies of the Licensed Product(s) for sale to third parties or copy or incorporate any portions of the Licensed Product into Licensee Documentation.
g. It is understood that nothing in this agreement grants or is intended to grant any license, express or implied, to any patents, or software.
h. Licensee shall immediately notify Telcordia (i) of any unauthorized attempt by a third party to access the Licensed Product, or (ii) if Licensee becomes aware of any unauthorized use or disclosure of any Licensed Product.

LICENSEE MAY NOT:

i. Copy the Licensed Product, except as provided above;
ii. Make copies of the Licensed Product or portions thereof except as are permitted above for internal purposes that contain provisions that conflict or differ in content from comparable provisions of the Licensed Product, unless such differences are identified specifically, and it is made clear in such copies that the results are not part of the Licensed Product;
iii. Transfer the Licensed Product to another party, except as provided above;
iv. Make the Licensed Product available, in whole or in part for the purposes of external distribution to third parties other than Affiliates, or create derivative works for sale;
v. Grant sublicenses, leases, or other rights to the Licensed Product or rent the Licensed Product(s) to others, except as provided above; or
vi. Make telecommunications data transmissions of the Licensed Product to the public or any third party.
vii. Except as provided above, data, in whole or in part, may not be extracted from the Licensed Product(s) for use in any derivative Licensee Product or used to verify and subsequently modify data in any Licensee Product which is sold, licensed or otherwise provided to third parties unless Licensee has executed a separately negotiated Special License Agreement with Telcordia.

3. AUDITS

Upon reasonable written notice to Licensee, Telcordia shall have the right to review Licensee's compliance with the terms and conditions of this Agreement. If such review reveals a violation of the requirements set forth herein, in addition to any other remedies it may have, Telcordia may terminate this Agreement in accordance with the Termination section of this Agreement.

4. FEES AND PAYMENTS

All fees and charges due hereunder shall be paid in full within thirty (30) days of the date of the invoice. All payments required hereunder shall be nonrefundable. Overdue payments are subject to a late payment charge, calculated and compounded monthly, and calculated at an annual rate of either (1) one percent (1%) over the prime rate available in New York City, as published in The Wall Street Journal on the first Monday (or the next bank business day) following the payment due date; or (2) 18 percent (18%), whichever shall be higher. If the amount of the late payment charge exceeds the maximum permitted by law, the charge will be reduced to that maximum amount.

Licensee shall pay or reimburse Ericsson for all sales or use taxes, duties, or levies imposed by any authority, government or government agency (other than those levied on the net income of Ericsson) in connection with this Agreement. If Ericsson is required to collect a tax to be paid by Licensee, Licensee shall pay this tax on demand. If Licensee fails to pay these taxes, duties or levies, Licensee shall pay all reasonable expenses incurred by Ericsson, including reasonable attorney's fees, to collect such taxes, duties or levies.

Telcordia shall provide Licensee with one (1) copy of the Licensed Product. Any additional copies in electronic or paper media will be provided to Licensee at a cost of $75.00 per copy. Please contact our Customer Service Center at buss.document-info@ericsson.com or 732-699-5828.

5. LIMITED WARRANTY AND REMEDY

Telcordia warrants that the media on which the Licensed Product is provided to the original Licensee is free from defects in materials and workmanship for 90 days after delivery to the original Licensee. Licensee's sole and exclusive remedy for any reported nonconformity with this warranty is to receive from Telcordia a replacement Licensed Product at no additional charge. Licensee must return the Licensed Product with prepaid postage and

recorded delivery, bearing a postmark dated no later than the 90th day, to Customer Service Center, Ericsson Inc. (IDO), Room RRC 1B-180, One Ericsson Drive, Piscataway, New Jersey 08854-4151 U.S.A.

6. DISCLAIMER OF WARRANTIES

EXCEPT AS SET FORTH ABOVE, THE LICENSED PRODUCT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, EVEN IF TELCORDIA HAS BEEN MADE AWARE OF SUCH PURPOSE, OR ANY WARRANTY AGAINST INFRINGEMENT OF PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS. LICENSEE ASSUMES RESPONSIBILITY FOR THE SELECTION OF THE LICENSED PRODUCT TO ACHIEVE ITS INTENDED RESULTS, AND FOR THE USE AND RESULTS OBTAINED FROM THE LICENSED PRODUCT.

7. LIMITATION OF LIABILITY

IN NO EVENT WILL TELCORDIA BE LIABLE TO LICENSEE FOR ANY DAMAGES, INCLUDING DIRECT DAMAGES, LOST PROFITS, OR OTHER INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, EVEN IF TELCORDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS, AND LICENSEE MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO LICENSEE.

8. THIRD PARTY PRODUCTS AND INFORMATION WARRANTY

Telcordia does not warrant third party products or information which Telcordia may use to prepare the Licensed Product. Third party products or information may be warranted by third parties as expressly provided in the documentation accompanying the third party product or information, if any. Licensee's exclusive remedy under any third party warranty is as provided in the third party documentation accompanying the third party product or information, if any.

9. RETURN POLICY

Licensed Product(s) may be returned within 30 days of receipt for Telcordia credit only. Returned Licensed Product(s) must be in their original packaging with all seals intact. Licensed Product(s) that have been delivered electronically (downloaded from the SuperStore) are ***not*** eligible for credits, refunds or returns, even if duplicative with Licensed Product(s) that are the subject of prior or contemporaneous orders. Licensee assumes all responsibility for managing its inventory of Licensed Product(s).

10. TERMINATION

If Licensee breaches one or more of its obligations under this Agreement, Telcordia may elect at any time, in addition to any other remedy, to terminate the license and rights granted. Prior to the termination, Telcordia must give Licensee two (2) months written notice specifying the breach. Telcordia may terminate the license and rights granted if Licensee does not remedy all breaches specified in the written notice within the two (2) month notice period. Upon termination of the license and rights granted, Licensee shall destroy or return all Licensed Product(s), including all copies, and certify in writing to Telcordia the destruction or return.

11. PUBLICITY

Notwithstanding anything herein to the contrary, each party is prohibited from using in advertising, publicity, promotion, marketing, or other similar activity, any name, trade name, trademark, or other designation including any abbreviation, contraction or simulation of the other without the prior, express, written permission of the other.

12. ASSIGNMENT

Neither this Agreement nor any license, rights or obligations hereunder shall be assignable or transferable (in insolvency proceedings, by mergers, by purchase, by operation of law or otherwise) by Licensee without the written consent of Telcordia. Any such purported assignment or transfer shall be void without such written consent.

13. GENERAL

Export/Reexport. Licensee acknowledges that any commodities and/or technical data provided under this Agreement is subject to the Export Administration Regulations (http://ecfr.gpoaccess.gov, Title 15-Commerce and Foreign Trade, Volume 2, Section VII, Subchapter C-Export Administration Regulations, collectively, "the EAR") administered by the Bureau of Industry and Security of the U.S. Department of Commerce (http://www.bis.doc.gov) and that any export or re-export thereof must be in compliance with the EAR, either through license or appropriate license exception. Licensee agrees that it shall not export or reexport, directly or indirectly, either during the term of this Agreement or after its termination or expiration, any commodities and/or technical data (or direct products thereof) received from Telcordia under this Agreement in any form to destinations in Country Group E, (as specified in Supplement No. 1 to Part 740 of the EAR, as modified from time to time by the U.S. Department of Commerce, or to destinations, entities or persons that are otherwise controlled or embargoed under U.S. law.
Licensee acknowledges it is not a foreign national of Country Group E or a denied party on U.S. export regulations.

Foreign Tax Payment. For a Licensee which is not a United States corporation, Ericsson will not accept remittance of less than the full amount billed to Licensee as full payment unless:

a. Licensee withholds that amount to satisfy tax withholding requirements imposed by the country (other than the United States) in which Licensee resides or in which Licensee has accepted delivery of the Licensed Product; and

b. Licensee furnishes a receipt issued by the withholding tax jurisdiction and certifying deposit of the withheld amount into its treasury or other tax depository to Telcordia's sole credit, or a certification on Licensee's stationery that Licensee has deposited the withheld amount into its tax jurisdiction's treasury or other tax depository to Telcordia's sole credit.

Further, to ensure the orderly processing of Telcordia tax returns, Licensee shall provide to Telcordia a summary of all amounts withheld during the year no later than ten business days after December 31 of each year addressed to: Ericsson Inc., 6300 Legacy Dr., Plano, Texas 75024, Attn.: Kendra Senegal.

Governing Law. This Agreement is a contract between Telcordia and the Licensee of the Licensed Product. This contract is to be interpreted in the federal and state courts of New Jersey, in accordance with the laws of the State of New Jersey without regard to its conflict of laws principles, and the parties consent to the jurisdiction of such courts for this purpose.

Entire Agreement. Licensee further agrees that this is the complete and exclusive statement of the Agreement between Licensee and Telcordia and supersedes any proposal or prior Agreement, oral or written, or any other communication between us relating to the subject matter of this Agreement.

All questions about this Agreement should be directed to:

Ericsson Inc. (IDO)
Customer Service Center
One Ericsson Drive, RRC 1B-180
Piscataway, NJ 08854
Phone: +1.732.699.5828 (Worldwide)

END OF TERMS AND CONDITIONS

Rev. 06/2013