Paper No. 28

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC,
Patent Owner.

Case No. IPR2015-00812
U.S. Patent No. 8,850,009

Before KARL D. EASTHOM, JENNIFER S. BISK, and GREGG I. ANDERSON, *Administrative Patent Judges*.

PETITIONER'S REPLY BRIEF

Table of Contents

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. Introduction

In its Institution Decision, the Board correctly found that Beser and RFC 2401 render claims 1-8,10-20, and 22-25 of the '009 patent obvious. Paper 8 (Dec.) at 10-14. In its Response ("Resp.") (Paper 24), Patent Owner advances a number of irrelevant challenges or clarifications to the Board's claim constructions, makes several narrow challenges to the substance of the Board's findings about Beser and RFC 2401, challenges whether RFC 2401 is a printed publication, and then concludes by asserting that the Board lacks the ability to compare the prior art to the challenged claims on its own and instead must rely on expert testimony. Each of Patent Owner's arguments lacks merit and should be rejected.

The Board's initial determination that the challenged claims are unpatentable is supported by more than substantial evidence and should be maintained.

II. Claim Construction

Petitioner believes that the constructions set forth in the petition represent the broadest reasonable constructions of the claims. However, in the Institution Decision, the Board correctly found that it need not adopt specific constructions here because under any reasonable construction, Beser and RFC 2401 render the claims obvious.

Many of the terms Patent Owner construes in its Response are irrelevant to this proceeding because it never challenges that Beser and RFC 2401 teach them. These include: "encrypted communication link," (Resp. at 5-7), "provisioning information," (*id.* at 7-10), "secure communications service," (*id.* at 10-11), "[VPN] communication link," (*id.* at 12-22), "domain name," (*id.* at 22), and "modulation," (*id.* at 23). The Board need not address the remaining term "interception," (*id.* at 4-5), because as explained below, under any interpretation proposed by Petitioner or Patent Owner, or adopted by the Board, Beser and RFC 2401 discloses this limitations. Finally, Patent Owner agrees with Petitioner's construction of "[]DNS request" so the Board need not revisit this term. *Id.* at 3.

III. Beser and RFC 2401 Render Claims 1-8,10-20, and 22-25 Obvious

The Board correctly found that Beser and RFC 2401 render claims 1-8,10-20, and 22-25 obvious. In its Response, Patent Owner raises four primary challenges to those findings: (i) a person of ordinary skill would not have combined Beser and RFC 2401, (ii) Beser does not disclose a "request to lookup an IP address," (iii) Beser does not disclose "interception" of such a request, and (iv) Beser and RFC 2401 do not suggest that originating device 24 receives all three elements specified by the "receiving" step.

Initially, this panel should reject Patent Owner's arguments because most of them already were rejected by another panel in a proceeding involving a related

patent. In the Final Written Decision in IPR2014-00237, the Board found that Beser and RFC 2401 rendered claims containing elements similar to the '009 patent invalid. Paper 41 at 37-41 (May 11, 2015). The Board rejected Patent Owner's arguments that a person of ordinary skill would not have combined Beser and RFC 2401, (Paper 41 at 37-41), and that Beser does not disclose the step of "intercepting a request to lookup an IP address," (*id.* at 22-28). In the current proceeding, Patent Owner simply rehashes those same rejected arguments. This panel should reject those arguments again. Even if Patent Owner's arguments are reconsidered on the merits, they are wrong and must be rejected.

A. A Person of Ordinary Skill Would Have Combined Beser and RFC 2401

As explained in the petition and by Dr. Tamassia, a person of ordinary skill in the art would have found it obvious to combine Beser and RFC 2401 to provide end-to-end encryption in an IP tunnel between Beser's originating and terminating end devices. Pet. at 30-34; Ex. 1005 at ¶¶383-403. The petition explained that the Beser IP tunnel would hide the true addresses of two communicating end devices providing user anonymity, and that a person of ordinary skill would have been motivated to follow Beser's suggestion to use IPsec (RFC 2401) to hide the data transmitted between the end devices. Pet. at 32; Ex. 1005 at ¶¶398-99. In its Institution Decision, the Board agreed and preliminarily found a person of ordinary skill would have combined Beser and RFC 2401. Dec. at 10-12.

In its Response, Patent Owner primarily repeats the arguments it raised in IPR2014-00237 and which were rejected by the Board. *See* Paper 41 at 37-41 (May 11, 2015); Paper 30 at 56-58 (Aug. 29, 2014). It again argues that Beser's statements recognizing that encryption can present practical challenges in some circumstances "teaches away" from the use of encryption. Resp. at 36, 38-41. Patent Owner's argument still cannot be squared with Beser's disclosure.

Beser recognizes encryption ordinarily should be used when the contents of a communication need to be protected (Ex. 1007 at 1:54-56), and it discloses using encryption when user-identifiable data are sent over the network such as during establishment of the IP tunnel, (*id.* at 11:22-25). Pet. at 27. Beser also criticizes prior art IP tunneling methods that sometimes prevent use of encryption, (Ex. 1007 at 2:1-8, 2:22-24), and states its tunneling method is intended to overcome such problems, (*id.* at 2:43-45). A person of ordinary skill reading Beser would have understood that encryption should ordinarily be used to protect the contents of communications in an IP tunnel. Ex. 1005 at ¶¶384-86, 389-90, 398-99.

Neither Patent Owner nor Dr. Monrose have asserted Beser's tunneling method is technically incompatible with encryption – they simply raise practical concerns that only affect some configurations of the system. At his deposition, Dr. Monrose admitted there was no inherent incompatibility with using IPsec to encrypt multimedia data, and a person of ordinary skill would have had

computational concerns only if IPsec was configured to use certain types of encryption. Ex. 1066 at 80:20-81:8, 82:7-17. Dr. Monrose also admitted that a person of ordinary skill in the art in February 2000 generally would have been able to adjust the configuration of a system to allow multimedia data to be encrypted. *Id.* at 79:3-11. Petitioner's expert Dr. Tamassia similarly explained that a skilled person would be able to change the configuration of a system to accommodate use of encryption in Beser's IP tunnel. Ex. 1005 at ¶¶389-90 (explaining adding more computing power or using lower resolution could solve any issues). Patent Owner criticizes the Board for finding that adding more computer power to a system would alleviate the potential concerns identified in Beser, arguing that approach is not always the solution to every problem. Resp. at 35. But adding more computing power is one of several ways to address the practical considerations mentioned in Beser, as Dr. Monrose has previously recognized. Ex. 1067 at 206:20-208:6 (in a related proceeding, admitting more powerful computers or lower recording fidelity would resolve Beser's concerns), 211:16-212:2.

Patent Owner also argues Beser teaches away from encryption because its tunneling method was designed to have a low computational burden on a system, and therefore, it was designed to replace computationally expensive security techniques such as encryption. Resp. at 36, 38. But Patent Owner mischaracterizes the purpose of Beser's design. Beser was designed to provide a better method for

ensuring user privacy by allowing communications over the Internet to be anonymous. *See* Ex. 1007 at 2:36-40, 3:4-9. Beser explains users increasingly had privacy concerns, (*id.* at 1:13-25), and that it was easy for computer hackers to determine the identity of two users communicating over the Internet because the source and destination addresses of IP packets were viewable, (*id.* at 1:26-53). Beser explains that while encrypting data could protect the contents of the communication, encryption did not provide privacy because it did not hide the identities of devices that are communicating. *Id.* at 2:1-5; *see id.* at 1:56-58. Beser then discusses conventional IP tunneling techniques, which could provide privacy by hiding the true addresses of end devices, but notes those techniques sometimes were incompatible with encryption. Ex. 1007 at 2:22-24; *see also id.* at 1:54-2:35; *see* Pet. at 33. Beser also notes that both encryption and prior art IP tunnels were computationally expensive. Ex. 1007 at 1:60-63, 2:12-17, 2:33-35.

Beser states that its IP tunneling technique was designed to overcome these problems with the prior art. Ex. 1007 at 2:43-45. Beser's IP tunnel hides the identities of communicating devices, but in contrast to prior art IP tunnels which were computationally expensive, (*id.* at 2:33-35), Beser's IP tunnel has a low "computational burden," (*id.* at 3:4-9). Because of its low computational burden, Beser's method is flexible and can be integrated into existing communications systems and combined with other security techniques. *See* Ex. 1005 at ¶¶388, 393;

Ex. 1007 at 3:4-9, 4:55-5:2. Beser's tunneling method also can be combined with encryption: Beser specifically notes the its IP tunnel can improve the security of encryption by helping to "prevent a hacker from intercepting all media flow between the ends," (Ex. 1007 at 2:36-40), and from "accumulating . . . sufficient information to decrypt the message," (*id.* at 1:56-58).

Next, Patent Owner argues that using encryption in Beser's system would be "redundant" because Beser teaches hiding the identities of the end devices instead of protecting the contents of a communication. Resp. at 38; *see id.* at 36 (arguing Beser is intended to replace encryption). But Beser never states its technique is intended to replace encryption. In fact, Beser distinguishes between using encryption to protect the data inside packets and using IP tunnels to hide the true addresses of the end devices, as Patent Owner recognizes. Resp. at 34; *see id.* at 14-15 (recognizing the difference between privacy and security). And Dr. Monrose agreed that a person of ordinary skill would have recognized that using a security technique to protect the identities of the parties communicating is not a substitute for using encryption to protect the contents of the communications sent between the parties. Ex. 1066 at 74:4-15; 74:25-75:3.

Thus, the Board correctly found a person of ordinary skill would have combined the teachings of Beser and RFC 2401 and should maintain its finding.

B. Independent Claims 1 and 14

The Board correctly found Beser likely discloses the "interception" of a "[] DNS request to lookup a network address." As explained in the Petition, Beser shows an originating device 24 initiates an IP tunnel with terminating device 26 by sending out a tunneling request that contains device 26's unique identifier. Pet. at 35-37. This request is intercepted by each of first network device 14 and trusted-third-party network device 30, which can be a DNS server. *Id.* In IPR2014-00237, the Board relied on this same request in finding that "Beser's trusted-third-party device 30 is 'informed of the request' from device 14; thereby 'receiving a request pertaining to a first entity [26] at another entity [14 or 30]' and satisfying the 'intercepting a request' element of claim 1 (and a similar element in claim 16)." Paper 41 at 24.

Patent Owner argues that Beser's tunneling request is not a "DNS request to lookup a network address" because it is not a "DNS request" and no single device looks up the address of the terminating device. Resp. at 27-30. It also argues the tunneling request cannot be "intercepted" by first network device 14 or trusted-third-party network device 30 because in Beser's system those devices are designed to always process the requests. *Id.* at 30-33. Finally, it argues that Beser and RFC 2401 do not show that originating device 24 receives all three elements specified by the "receiving" step. *Id.* at 40-42. Each of Patent Owner's

contentions reflects a misunderstanding of its own claims and a mischaracterization of what Beser actually discloses.

1. Beser Teaches a DNS Request to Lookup an Address

The tunneling request sent by originating device 24 is a "DNS request to lookup a network address" because in one embodiment the Beser trusted-third-party network device 30 is a DNS server, and when trusted device 30 receives a tunneling request, it uses the domain name in the request to lookup two IP addresses. Pet. at 36-37. For the first address, it consults an internal database of registered devices to look up the IP address of the second network device 16 that is associated with the unique identifier. *Id.* at 23, 36; Ex. 1007 at 11:45-55. For the second address, it looks up a private IP address for the terminating device 26 by sending a message to network device 16 requesting the address. Pet. at 23, 36; Ex. 1007 at 9:29-30, 12:16-19, 14:19-27, Figs. 6 & 9. As a result of this process, originating device 24 ultimately receives an IP address for terminating device 26. Pet. at 25; Ex. 1007 at 21:48-52; *see* Ex. 1066 at 103:22-104:3 (Dr. Monrose admitting he does not dispute that the originating device receives an IP address for the terminating device).

Patent Owner asserts Beser does not disclose this element, and raises several challenges. **First**, Patent Owner argues that the "tunneling request" is not a "DNS request" because Beser does not disclose that tunneling requests follow the DNS

protocol. Resp. at 28. But nothing in the parties' agreed upon construction for "DNS request" requires it to follow the DNS protocol. *See* Resp. at 3. Even if the claimed "DNS request" did need to follow the DNS protocol, Beser teaches that the tunneling request follows that protocol. *See* Ex. 1007 at 1:50-53, 4:9-11. In his declaration, Dr. Tamassia noted that the trusted-third-party network device 30 could be a DNS server and explained that the "functionality of a DNS server was extremely well-known by February 2000." Ex. 1005 at ¶306; *see id.* at ¶¶303, 307. He also explained that "a unique identifier could be a domain name (*e.g.* if a web browser made a request for a website)," (*id.* at ¶319), and that in response to tunneling requests, trusted device 30 would resolve domain names into IP addresses, (*id.* at ¶¶327-28). A person of ordinary skill would have understood that when a request to resolve a domain name is sent to a DNS server, that request follows the DNS protocol. *Id.* at ¶306; *see* Ex. 1007 at 1:50-53. Dr. Tamassia explained that DNS servers were extremely well-known, and a person of ordinary skill would have known what the DNS protocol was. Ex. 1005 at ¶306; Ex. 1066 at 84:5-86:3 (Dr. Monrose admitting a person of ordinary skill would have been well aware of what "the DNS protocol" was).

Next, Patent Owner argues that the tunneling request is not a request to "lookup a network address" because the trusted device 30 does not "look up" any IP addresses in response to a tunneling request. Resp. at 28-29. But that argument

is irrelevant to the claims, which simply specify an "interception of the DNS request," and under the broadest reasonable construction, do not require a DNS lookup to be performed, let alone specify that a particular device perform a lookup. ***The claims simply do not require a lookup***, and thus Patent Owner's remaining arguments can be dismissed.

Based on its incorrect theory that a lookup is required, Patent Owner next argues that neither of Beser's lookups actually lookup an IP address. Patent Owner first argues Beser does not disclose that trusted device 30 performs a "lookup" of network device 16's public IP address in response to a tunneling request. Resp. at 29. Patent Owner admits that trusted device 30 contains a database or similar data structure that correlates each unique identifier to the public IP addresses of second network device 16 and terminating device 26, but asserts that Beser "never suggests that this data structure is looked up when the tunnel request is received by device 30." Resp. at 29. Patent Owner's position is contrary to Beser's explicit disclosure.

Beser describes the database as an example of how the trusted-third-party network device 30 performs Step 116 of Figure 5, "associat[ing] a public IP address for a second network device," which it performs after receiving the tunneling request sent to it in Step 114. Ex. 1007 at Fig. 5, 11:26-58. Figure 5 has four steps, and Beser walks through each step sequentially on 9:64 to 12:19. *See*

Ex. 1066 at 104:25-107:13. Beser discusses Step 116 in two sequential paragraphs that appear at 11:26-58, as Dr. Monrose agreed. Ex. 1066 at 107:15-108:8. The first paragraph explains trusted device 30 associates the public IP address for second network device 16 with the unique identifier in the request. Ex. 1007 at 11:24-32. The second paragraph describes an example of how the association is performed, stating "[f]or example, the trusted-third-party network device 30 may . . . retain[]a list of E.164 numbers of its subscribers [and] [a]ssociated with a E.164 number in the directory database is the IP 58 address of a particular second network device 16." *Id.* at 11:45-50; *see id.* at 11:55-58 (noting other types of unique identifiers could be used). Thus, Beser teaches that in Step 116 of Figure 5, trusted device 30 receives the tunneling request, (*id.* at 11:9-16), and in response, it associates an IP address with the unique identifier by looking it up in its internal database, (*id.* at 11:26-58). *See* Ex. 1066 at 107:15-108:8.

Patent Owner also suggests the tunneling request cannot be one to "lookup a network address" because trusted device 30 looks up the public IP address of the second network device 16 instead of the public IP address of the terminating device 26. Resp. at 29. But the claims only specify a request to lookup "a network address of a second network device based on an identifier associated with [that] device," (Ex. 1003 at 56:28-30), and the '009 specification provides that the IP address looked up "need not be the actual address of the destination computer," Ex.

1003 at 40:52-57. *See* Ex. 1066 at 63:25-64:24. In Beser's system, the IP address of the second network device is looked up "based on" the unique identifier (*e.g.*, domain name) associated with the terminating device. Thus the lookup meets the language of the claims.

Finally, Patent Owner challenges Beser's second network address "lookup" by arguing first and second network devices (14 & 16), and not trusted device 30, negotiate private IP addresses for the end devices (24 & 26). Resp. at 28-29. Patent Owner's argument is premised on a single embodiment in Beser, and it simply ignores that Beser discloses embodiments where the trusted-third-party network device 30 performs the negotiation with the first and second network devices (14 & 16). Ex. 1007 at 9:29-30, 12:16-19, 14:19-27, Figs. 6 & 9; *see* Pet. at 24, 36. Petitioner showed certain embodiments in Beser met the claim limitations, which is all that is required. *Arthrocare Corp. v. Smith & Nephew, Inc.*, 406 F.3d 1365, 1372 (Fed. Cir. 2005) (no requirement that every possible embodiment of a prior art reference satisfy the claims).

Patent Owner also asserts that no private IP addresses are "looked up" during the negotiation because second network device 16 "assigns" a private IP address to terminating device 26. Resp. at 29. That argument fails for at least two reasons. One, even if second network device 16 "assigns" the IP address to terminating device 24, the trusted device 30 "looks up" the IP address when it

sends a message to network device 16 requesting a private IP address. Ex. 1007 at Fig. 9 (packets 164 and 166), 13:33-14:18; Pet. at 23, 41 (discussing same). Two, second network device 16 does not simply "assign" an IP address – it looks one up by selecting an unused address out of a pool of IP addresses. Ex. 1007 at 13:49-64; Pet. at 24. Thus, the Board should find that Beser teaches a "DNS request to lookup a network address." *See* IPR2014-00237, Paper 41 at 22-24 (finding that Beser discloses a request to lookup an IP address).

2. Beser Teaches "Interception" of a DNS Request

Beser shows that each of the first network device 14 and the trusted-third-party network device 30 "intercept" the tunneling request sent by originating device 24. Pet. at 32-34. The tunneling request contains the unique identifier for terminating device 26, (Ex. 1007 at 8:1-3, 10:37-42), but it is received and processed by first network device 14, (*id.* at 8:21-22, 8:39-43, 10:22-23). Because the request pertains to terminating device 26 but is received by network device 14, it is intercepted by network device 14. Pet. at 33. If network device 14 determines the request needs special processing by detecting a unique sequence of bits in the packet, (Ex. 1007 at 8:34-43), network device 14 forwards the request to trusted device 30, (*id.* at 8:3-7, 8:48-49). Pet. at 33; *see also* Ex. 1007 at Figs. 4 & 6. The trusted-third-party network 30 device thus also "intercepts" the tunneling request. Pet. at 33-34; *see also* IPR2014-00237, Paper 41 at 23-24.

In its Response, Patent Owner contends that neither first network device 14 nor trusted-third-party network device 30 intercept the tunneling request because Beser's system is designed such that tunneling requests are always "intended for" and received by those two devices. Resp. at 32-33. But Patent Owner's arguments are irrelevant to what the claims require. The only disclosure in the '009 patent of a DNS device that "intercepts" lookup requests is DNS proxy 2610, which "intercepts ***all DNS lookup functions*** from client 2605." Ex. 1003 at 40:39-41 (emphasis added). The '009 patent thus provides that DNS proxy 2610 "intercepts" lookup functions, even though the DNS proxy receives every single lookup request sent by the client. *Id.* at Fig. 26, 40:39-41. Dr. Monrose agreed that the DNS proxy in the '009 patent receives every DNS request and that the system is designed, *i.e.*, "pre-established" to intercept every DNS request. Ex. 1066 at 55:8-20. Thus, the Board should reject Patent Owner's arguments that Beser cannot show an "interception" because the system is designed such that IP tunnel requests are received by network device 14 and trusted device 30.

Moreover, Patent Owner mischaracterizes Beser. Even if an "interception" were to include an "intent" element—a position that no party has taken in this proceeding—Beser discloses such as system. The originating device 24 never "intends for" its tunneling request to be received by the trusted device 30. As the petition explains, the originating device 24 sends tunneling requests to first

network device 14. Pet. at 37-38. Dr. Monrose agreed that the tunneling request is addressed to the first network device and not the trusted-third-party network device. Ex. 1066 at 94:7-95:14. Network device 14 runs a tunneling application that monitors traffic for a distinctive sequence of bits, and if it detects a packet containing those bits, it forwards that packet to trusted device 30. Pet. at 37-38; Ex. 1007 at 8:39-43. In Beser's system, it is first network device 14 that "intends" for trusted device 30 to receive the request. Ex. 1066 at 97:8-98:10, 101:9-14. The originating device 24 only "intends" for the tunneling request to go to network device 14. Thus, the tunnel request is received by trusted device 30, even though originating device 14 did not "intend" to send the tunnel request to that device, and thus trusted device 30 "intercepts" the request. *See* Pet. at 37-38.

All of Patent Owner's arguments about "interception" are anchored on it including an "intent" element, and not on any of the actual proposed constructions. Resp. at 30-33; *see* Ex. 1066 at 124:23-127:13, 132:8-13 (Dr. Monrose admitting he did not apply Petitioner's, Patent Owner's, or the Board's constructions of "intercepting," and in fact, had no opinion of what the term "intercepting" requires). The Board can reject those arguments because no one in this proceeding has advanced such a construction of "interception." Patent Owner asserts Dr. Tamassia "clarified" his construction of "interception" to mean "receiving a request ~~pertaining to~~ intended for or ordinarily received by a first entity at another

entity." *See* Resp. at 31; Ex. 1005 at ¶69. But it mischaracterizes Dr. Tamassia's testimony, who was discussing the rationale underpinning his construction, and was neither proposing nor applying a different construction. Ex. 2015 at 79:9-80:13, 85:9-12; *see* Ex. 1005 at ¶68. Even if "interception" were to require receiving a request "intended for" another entity, that is disclosed by Beser, as explained above. Further, even if Patent Owner's "alternative" construction specifying "performing an additional evaluation" on the request were adopted, (Resp. at 4), Beser discloses that as well: the trusted device 30 evaluates the request by checking an internal table of secure devices, (Ex. 1007 at 11:45-58), which is the same process shown in the '009 patent, (Ex. 1003 at 40:41-45).

3. Beser Teaches that Originating Device 24 Receives an Indication, a Network Address, and Provisioning Information

Patent Owner argues that Petitioner relies on two features in Beser and RFC 2401 to teach three different claim elements, and asserts that such reliance is improper. Resp. at 40-41. Patent Owner's argument suffers from a fatal flaw: Petitioner relies on three different features in Beser and RFC 2401 to teach the three claim elements. Pet. at 40-44. Claims 1 and 14 specify that a first device "receive" "(1) an indication that the second network device is available . . ., (2) the requested network address of the second network device, and (3) provisioning information for an encrypted communication link." Ex. 1003 at 56:31-38. Patent Owner asserts that Petitioner relied on the same two features in Beser for the

indication and the requested network address, but Patent Owner is wrong. Petitioner explained that after Beser's originating device 24 sends out a tunneling request, it receives the private IP address of the terminating device 26 as well as its own private IP address. Pet at 41-42; Ex. 1007 at 21:48-62. The originating device 24 receives the claimed "(2) the requested network address" because it receives the private IP address of terminating device 26. Pet. at 42. It also receives the claimed "(1) indication" because originating device 24 receives a second private IP address: its own.[1] Pet. at 41. Thus, Petitioner has relied on two separate elements to teach two claim limitations. Patent Owner's contrary argument can be dismissed.

C. Dependent Claims 2-8,10-13, 15-20, and 22-25

Patent Owner does not separately address these claims so they rise and fall with claims 1 and 14. Resp. at 42.

IV. RFC 2401 Is a Prior Art Printed Publication

A. The Evidence Shows RFC 2401 Is a Prior Art Printed Publication

RFC 2401 was published in November 1998, as indicated on the document's face. Pet. at 26 (*citing* Ex. 1008 at 1). RFC 2401 states its "[d]istribution . . . is

[1] Device 24 also receives an encryption key as suggested by RFC 2401 (*i.e.*, "(3) provisioning information"), (Pet. at 44), which Patent Owner has not contested. *See also* Dec. at 13.

unlimited" and requests "discussion and suggestions for improvement[]" from the "Internet community." Ex 1008 at 1. Dr. Tamassia explained that RFC documents are the official publication channel for Internet standards and the publication process is described in RFC 2026 (Ex. 1036). Ex. 1005 at ¶¶148-55. RFC 2026 explains that anyone can obtain RFCs from a number of Internet hosts, (Ex. 1036 at 5-6), and that each RFC "is made available for review via world-wide on-line directories," (*id.* at 4). *See* Ex. 1005 at ¶149. Persons of ordinary skill in the art would have known how to obtain RFC publications such as RFC 2401 because of their wide distribution and importance to the Internet community. Ex. 1005 at ¶¶153-55. Dr. Monrose has not disputed any of this testimony, or offered a contrary opinion. Ex. 1066 at 112:25-114:6, 118:10-121:11.

After institution, Petitioner submitted supplemental information to further corroborate its assertion that RFC 2401 was prior art published in November 1998. That information included a declaration from Sandy Ginoza, acting as a designated representative of the Internet Engineering Task Force (IETF), discussing the IETF's RFC publishing practices. Ex. 1060 at ¶¶1-5; Ex. 1063 at 6:23-7:4; *id.* at 10:5-11:22 (confirming her knowledge of IETF RFC publishing practices). Ms. Ginoza testified that the "RFC Editor maintained a copy of RFC 2401 in the ordinary course of its regularly conducted activities" and that RFC 2401 was published and "has been publicly available through the RFC Editor's web site or

through other means since its publication in November 1998." Ex. 1060 at ¶ 107; *id.* at ¶¶105-107. In a deposition about her declaration, Ms. Ginoza testified:

> Q Is th[is] document . . . [titled "Request for Comments: 2401"] a true and correct copy of the record of RFC 2401 as it's kept in the files of the RFC Editor?
>
> A Yes.
>
> * * *
>
> Q Was RFC 2401 publicly available as of the date listed on its face?
>
> A Yes.
>
> Q What date was RFC 2401 made publicly available?
>
> A November 1998.

Ex. 1063 at 39:14-40:24; *see* Ex. 1062 (redline comparison showing no substantive differences between Ex. 1008 and Ex. 1061, produced by the IETF).

The supplemental information also included industry publications from prior to February 2000, which explicitly reference RFC 2401 and state that RFC 2401 could be downloaded from the IETF. Ex. 1064 at 9 (discussing RFC 2401 and stating "All of these documents are available on the IETF website"); Ex. 1065 at 3 (March 15, 1999 article, stating RFC 2401 was available on the IETF website).

B. Patent Owner's Arguments Lack Any Merit

Patent Owner mounts two challenges to RFC 2401, first asserting the evidence submitted with the petition was insufficient to establish it was published. Resp. at 42-48. But the Board already addressed this issue, finding the petition and

the supporting evidence submitted with the petition were sufficient for institution, and inviting the parties to adduce further evidence during trial about its publication *vel non*. Dec. at 6-7; Paper 13 at 4 (denying rehr'g). While Petitioner submitted supplemental information further supporting its position, Patent Owner made no attempt to do so. Dr. Monrose admitted he was familiar with RFCs, (Ex. 1066 at 112:25-113:15), but expressly declined to form any opinion on whether RFC 2401 was prior art, (*id.* at 118:4-119:15, 120:5-121:11). Though Patent Owner criticizes Dr. Tamassia's testimony on this issue because he lacks personal knowledge of RFC 2401's publication, (Resp. at 44-45), his testimony was based on his personal knowledge of RFC publication generally in February 2000. Ex. 2015 at 103:1-12. Moreover, his testimony is corroborated by RFC 2026, the Ginoza materials, and industry publications. *See* § IV.A, above. In sum, all of the evidence in the record shows that RFC 2401 was published and available by November 1998.

Second, Patent Owner argues the supplemental information does not establish publication, raising a number of frivolous arguments. It asserts Ms. Ginoza's testimony is entitled to no weight because she does not have personal knowledge RFC 2401's publication. Resp. at 48-50. But Ms. Ginoza was testifying "on behalf of the Internet Engineering Task Force" as a designated corporate representative, (Ex. 1063 at 10:5-22; Ex. 1060 at 1 (entitled "Declaration of the RFC Publisher for the [IETF]")), and as such, she was testifying to "the

knowledge of the corporation." *Poole v. Textron, Inc.*, 192 F.R.D. 494, 504 (D. Md. 2000). It is well-established that corporate representatives "need not have first-hand knowledge of the events in question" so long as they are "adequately prepared" to answer on behalf of the corporation. *Id.*; *see U.S. v. Taylor*, 166 F.R.D. 356, 361 (M.D.N.C.) *aff'd,* 166 F.R.D. 367 (M.D.N.C. 1996) ("a corporation [must] prepar[e] its Rule 30(b)(6) designee to the extent matters are reasonably available, whether from documents, past employees, or other sources"). Corporate witnesses like Ms. Ginoza may testify about publication date of a prior art document. *Ultratec, Inc. v. Sorenson Commc'ns, Inc.*, No. 13-CV-346, 2014 WL 4829173, at *6 (W.D. Wis. Sept. 29, 2014) (finding that a corporate representative could testify as to "the publication date of one of its product handbooks" even though he lacked personal knowledge because "a Rule 30(b)(6) witness . . . could speak on matters reasonably available to the corporation").

Patent Owner also asserts Ms. Ginoza's testimony should be discounted because she does not provide the "facts or underlying data" for "her stated opinion" citing to Rule 42.65(a)—which only applies to ***expert*** opinion. Resp. at 46. Ms. Ginoza did not provide expert opinion; she was corporate representative testifying to ***facts***. The weight of the evidence in the record, which is unrebutted, clearly establishes that RFC 2401 was published in November 1998 and is prior art to the challenged claims.

V. Dr. Tamassia's Testimony Is Probative

Dr. Tamassia is a person of ordinary skill in the art, and he offered probative testimony on many of the factual inquiries underpinning an obviousness analysis: the level of skill and background knowledge of one skilled in the art, the scope and content of the prior art, and the motivation to combine the references. Given the depth of Dr. Tamassia's experience and the breadth of his analysis in this proceeding, his testimony can certainly "assist the trier of fact to understand the evidence or determine a fact in issue" and it should be accord substantial weight. Fed. R. Evid. 702; *cf. Sundance, Inc. v. Demonte Fabricating Ltd*, 550 F.3d 1356, 1364 (Fed. Cir. 2008) (stating that only a witness qualified in the pertinent art can offer testimony on any of the factual questions underlying obviousness). Patent Owner asserts this testimony should be given no weight because Dr. Tamassia did not opine on the ultimate question of obviousness or perform a claim-by-claim analysis of the challenged claims. *See* Resp. at 51. But no rule requires an expert to opine on the ultimate question of obviousness or on every potentially relevant fact at issue for his opinion to be admissible or entitled to weight.[2] *See* Fed. R.

[2] Patent Owner cites a number district court cases involving expert testimony in the context of, *e.g.*, infringement, juries, and summary judgment, that are inapposite. *E.g.*, *Schumer v. Lab. Computer Sys., Inc.*, 308 F.3d 1304 (Fed. Cir 2002) (finding

Evid. 702. Dr. Tamassia's opinions can help the Board understand the evidence and determine a fact at issue, and should be considered by the Board.

Patent Owner also incorrectly asserts Petitioner cannot prove the challenged claims are obvious without expert testimony specifically addressing each claim element. No statute or rule requires such testimony. The Board has repeatedly held "[t]estimony from a technical expert can be helpful to show what would have been known to a person of ordinary skill in the art and explain the significance of elements in a claim," but it "is not a prerequisite for establishing unpatentability by a preponderance of the evidence, . . . just as it is not a prerequisite for a[n] [IPR] petition." *See, e.g.*, *Guangdong Xinbao Elec. Appliances Holdings v. Adrian Rivera*, IPR2014-00042, Paper 50 at 22-23 (Feb. 6, 2015). Patent Owner's reliance on *Brand v. Miller*, 487 F.3d 862 (Fed. Cir. 2007) is misguided—the *Brand* court recognized that "the Board's expertise appropriately plays a role in interpreting record evidence." *Id.* at 869. Patent Owner also ignores *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064 (Fed. Cir. 2015), where the Federal Circuit stated that in an IPR there was no requirement for an expert to "guid[e] the Board as to how it should read prior art" as "Board members, because of expertise, may more often find it easier to understand and soundly explain the teachings and suggestions of

---

the expert testimony was insufficient because the "burden of proving invalidity [by clear and convincing evidence] on summary judgment is high").

prior art without expert assistance." *Id.* at 1079; *see* 35 U.S.C. § 6. Quite simply, the Board is more than capable of doing the "thinking" necessary to analyze the references and to compare those teachings to the claims at issue. *See Titanium Metals Corp. of America v. Banner*, 778 F.2d 775, 776-79 (Fed. Cir. 1985).

Finally, Patent Owner's attack is particularly bold given Dr. Monrose's improperly narrow focus on alleged deficiencies in the Petition and Dr. Tamassia's deposition transcript instead of the prior art and challenged claims. *See, e.g.*, Ex. 1066 at 30:9-14 ("So my analysis . . . only [addresses] what is pointed to by the petitioner … and whether that … can satisfy the limitations"), 21:1-2, 130:18-131:1, 132:8-13 ("I made no opinion of what the term [intercepting] requires"). Such testimony is improper. 37 CFR 42.65(a); *see LG Display Co., Ltd, v. Innovative Display Techs. LLC*, IPR2014-01362, Paper 32 at 15-16 (Feb. 8, 2016) (discounting testimony intended to rebut the Petition because it did not consider the prior art).

VI. Conclusion

For the forgoing reasons, Petitioner requests the Board to maintain its finding that Beser and RFC 2401 renders obvious the challenged claims of the '009 patent.

Dated: March 18, 2016

Respectfully Submitted,

/ Jeffrey P. Kushan /

Jeffrey P. Kushan
Reg. No. 43,401
Sidley Austin LLP
1501 K Street NW
Washington, DC 20005

CERTIFICATE OF SERVICE

Pursuant to 37 CFR 42.6(e), I hereby certify that on this 18th day of March 2016, a true and correct copy of this Petitioner's Reply Brief, including all attachments and exhibits, has been served in its entirety on the following counsel for Patent Owner:

Joseph E. Palys
E-mail: josephpalys@paulhastings.com

Naveen Modi
E-mail: naveenmodi@paulhastings.com

Jason E. Stach
E-mail: Jason.stach@finnegan.com

Dated: March 18, 2016

Respectfully submitted,

/Jeffrey P. Kushan /
Jeffrey P. Kushan
Reg. No. 39,772
Attorney for Petitioner