

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2016-01585
Patent 8,904,516 B2

Before *Vice Chief Administrative Patent Judge* MICHAEL P. TIERNEY,
KARL D. EASTHOM and STEPHEN C. SIU, *Administrative Patent Judges*

EASTHOM, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

A. Background

Petitioner, Apple Inc., filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1–9, 11–23, and 25–28 (the “challenged claims”) of U.S. Patent No. 8,904,516 B2 (Ex. 1001, “the ’516 patent”). Patent Owner, VirnetX Inc., filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

Subsequent to institution (Paper 9, “Inst. Dec.”), Patent Owner filed a Patent Owner Response (Paper 14, “PO Resp.”), and Petitioner filed a Reply (Paper 19, “Pet. Reply”). Patent Owner also filed a Motion to Exclude evidence (Paper 21), Petitioner filed an Opposition (Paper 24), and Patent Owner filed a Reply to the Opposition (Paper 26).

The record includes a transcription of the Oral Hearing held on November 2, 2017. Paper 31. The Board has jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision issues pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–9, 11–23, and 25–28 of the ’516 patent are unpatentable.

B. Related Matters

Petitioner and Patent Owner provide listings of district court actions, other *inter partes* reviews, and *inter partes* reexamination proceedings challenging related patents. *See* Pet. ix–xiii, Paper 4, 2–16; *see also* *VirnetX, Inc. v. Cisco Systems, Inc.*, 767 F.3d 1308, 1316–19 (Fed. Cir. 2014) (addressing ancestor *VirnetX* patents); *VirnetX Inc. v. Apple Inc.*, 665 F. App’x 880 (Fed. Cir. 2016) (affirming *Apple Inc. v. VirnetX Inc.*, Cases IPR2014-00237 & 238 (PTAB May 11, 2015) (final written decisions “’237

FWD,” “’238 FWD,” or generally, “’237 IPR,” “’238 IPR”) (appealed by VirnetX))¹; *VirnetX Inc. v. Apple Inc.*, 671 F. App’x. 786 (Fed. Cir. 2016) (affirming *Apple Inc. v. VirnetX Inc.*, Cases IPR2014-00403, IPR2014-00404 (PTAB July 29, 2015) (appealed by VirnetX); *Apple Inc. v. VirnetX Inc.*, Cases IPR2014-00481 & 482 (PTAB August 24, 2015) (appealed by VirnetX))²; *Apple Inc. v. VirnetX Inc.*, Case IPR2015-00811 (PTAB Sept. 8, 2016) (appealed by VirnetX); *Apple Inc. v. VirnetX Inc.*, Case IPR2015-00812 (PTAB Aug. 30, 2016) (appealed by VirnetX); *Apple Inc. v. VirnetX Inc.*, Cases IPR2015-00870 & 871 (PTAB Sept. 28, 2016) (appealed by VirnetX); *Apple Inc. v. VirnetX Inc.*, Cases IPR2016-00331 & 332 (PTAB June 22, 2017) (as to the former, final written decision “’331 FWD” (Paper 29), or generally, “’331 IPR)) (appealed by VirnetX). At least the ’237 FWD and the ’331 FWD involve materially the same claim construction and prior art issues as the instant case as discussed further below.

C. Instituted Grounds of Unpatentability

We instituted on the ground that the combination of Beser³ and RFC 2401⁴ would have rendered obvious claims 1–9, 11–23, and 25–28 of the ’516 patent. Petitioner relies on the Tamassia Declaration (Ex. 1003). In

¹ Our reviewing court affirmed the ’237 FWD and the ’238 FWD without reaching the merits of the ’237 FWD. See 665 F. App’x. at 889 (citing *In re Gleave*, 560 F.3d 1331, 1338 (Fed. Cir. 2009) (“declining to address alternative grounds of invalidity when the court upholds one such ground”)).

² The court affirmed the four final written decisions without reaching the merits of the ’404 and ’482 proceedings. See 671 F. App’x at 787 (finding “no error in the Patent Trial and Appeal Board’s . . . claim constructions or findings in the 403 and 481 proceedings).

³ U.S. Patent No. 6,496,867 B1 (Ex. 1007).

⁴ S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, Request for Comments: 2401, BBN Corp., November 1998 (Ex. 1008).

response, Patent Owner relies on the Monroe Declaration (Ex. 2009), which Patent Owner submitted in the related '237 IPR.

D. The '516 Patent

The '516 patent describes secure methods for communicating over the Internet. Ex. 1001, Abstract, 10:7–12. According to “BACKGROUND OF THE INVENTION” as described in the '516 patent, “[a] tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet.” *Id.* at 1:38–40. In general, “two security issues may be called data security and anonymity, respectively.” *Id.* at 1:57–59. At least one prior art system provides anonymity by hiding the originating terminal address. *See id.* at 2:47–57 (describing “[s]till another anonymity technique” using “groups of proxies called crowds”). A system disclosed in the '516 patent hides the identity of the destination address by encrypting a packet portion that indicates the true final destination of the packet. *See id.* at 2:4–9, 10:7–49. With respect to data security (i.e., as opposed to anonymity or packet address security), the '516 patent admits “[d]ata security is usually tackled using some form of data encryption.” *Id.* at 1:60–61.

To provide anonymity regarding the “true destination address,” one disclosed, but unclaimed, aspect of the system “preferably” uses “an IP hopping function” (*id.* at 40:27–28), and employs, in one embodiment, “Tunneled Agile Routing Protocol (TARP)” (*id.* at 3:19–32) routers 122–127, described as “special routers or servers” along the hopping path, which “are similar to regular IP routers 128–132” (*id.* at 10:8–10). *See id.* Fig. 2. TARP routers determine the “next-hop in a series of TARP router hops” (*id.* at 10:18–19) in the path and the final destination, by authenticating or

decrypting transmitted encrypted parts of packets to find the next-hop TARP router address. *Id.* at 3:40–67, 10:12–35. “Once the outer layer of encryption is removed, the TARP router determines the final destination. Each TARP packet 140 undergoes a minimum number of hops to help foil traffic analysis.” *Id.* at 3:51–54. “The hops may be chosen at random.” *Id.* at 3:54. “The fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message.” *Id.* at 3:60–63. As noted above, the system also may encrypt data in the packets. *See id.* at 1:60–61, 4:11–16.

As a “second improvement,” the ’516 patent also describes “the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.” *Id.* at 39:31–33. The challenged claims here also do not recite or require a VPN.

To create a VPN automatically, the ’516 patent describes employing a modified Domain Name Server, which may include a conventional Domain Name Server (DNS) and a DNS proxy. *Id.* at 40:28–30.

Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name “Yahoo.com,” the user’s web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user’s browser and then used by the browser to contact the destination web site.
Id. at 39:34–40.

The DNS proxy of the modified DNS server intercepts DNS lookup requests, determines whether the user has requested access to a secure site (using for example, a domain name extension or an internal

table of secure sites), and if so, whether the user has sufficient security privileges to access the requested site. *Id.* at 40:34–40. If the user requests access to a secure site to which it has insufficient security privileges, the DNS proxy returns a “host unknown” error to the user. *Id.* at 40:57–60. If the user requests access to a secure site to which it has sufficient security privileges, the DNS proxy requests a gatekeeper to create a VPN between the user’s computer and the secure target site. *Id.* at 40:36–52. The DNS proxy then returns to the user the resolved address passed to it by the gatekeeper, which need not be the actual address of the destination computer. *Id.* at 40:47–52.

The (unclaimed) VPN embodiment also is “preferably implemented using the IP address ‘hopping’ features,” (i.e., changing IP addresses based upon an agreed upon algorithm) as described above, “such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted.” *Id.* at 40:13–17.

E. Illustrative Challenged Claim 1

Independent claims 1 and 15 recite similar limitations respectively in system and method format. *Compare* Ex. 1001, 56:13–32, *with id.* at 57:8–27. All other challenged claims depend from claims 1 or 15.

Illustrative claim 1 of the challenged claims follows:

1. A system for connecting a first network device and a second network device, the system including one or more servers configured to:
 - intercept, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on an identifier associated with the second network device;

determine, in response to the request, whether the second network device is available for a secure communications service; and

initiate an encrypted communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service,

wherein the secure communications service communicates using the encrypted communication link, the first network device is a device at which a user uses the secure communications service to access the encrypted communication link, and;

the one or more servers includes one or more processors.

Ex. 1001, 56:13–32.

II. ANALYSIS

A. Claim Construction

In an *inter partes* review, the Board construes claims in an unexpired patent by applying the broadest reasonable interpretation in light of the specification. 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016) (upholding the use of the broadest reasonable interpretation standard under 37 C.F.R. § 42.100(b)). Under this standard, absent any special definitions, claim terms or phrases carry their ordinary and customary meaning, as would be understood by one of ordinary skill in the art, in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

1. “*intercept . . . a request*”

Relying on the ’516 patent Specification and citing to the ’237 FWD, Petitioner proposes construing the claim 1 phrase “intercept . . . a request” as “receiving a request pertaining to a first entity at another entity.” Pet. 10 (citing ’237 FWD, 10–12; Ex. 1003 ¶ 62) (emphasis omitted). Claim 15

recites a similar “intercepting a request” phrase. We adopted this construction in the Institution Decision, and we maintain it for the reasons provided therein and as summarized below. *See* Inst. Dec. 6–9.⁵

Patent Owner disagrees with this construction, but contends “[n]o construction is necessary.” PO Resp. 3. Patent Owner also contends that “[i]f the Board decides to provide a construction, it should modify its current construction.” *Id.* Patent Owner proposes that the phrase means “receiving a request to look up an internet protocol address and, apart from resolving it into an address, performing an evaluation on it related to establishing a virtual private network communication link.” *Id.* Patent Owner contends that its “construction appropriately captures the notion of performing an additional evaluation on a request to look up an IP address related to establishing a secure communication link, beyond conventionally resolving it and returning the address.” *Id.* at 6.

Patent Owner’s contentions are not persuasive. Patent Owner fails to explain sufficiently why the notion of “performing an additional evaluation”

⁵ Claim 1 at issue in the ’237 IPR (U.S. Patent No. 8,504,697) (the “’697 patent”) recites a similar clause: “intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device.” ’237 FWD 4. The Board employed the same construction therein. *Id.* at 10–12; note 6 *infra*. The ’697 and ’516 patents have common ancestor patents at issue in *Cisco*, 767 F.3d at 1308; i.e., both patents ultimately continue through one or more applications of U.S. Patent No. 7,921,211, which is a continuation of U.S. Patent No. 7,418,504 (“’504 patent”), which is a continuation-in-part of U.S. Patent No. 6,502,135—three of the four patents at issue in *Cisco*. *See* 767 F.3d at 1313. (The fourth patent at issue in *Cisco*, is U.S. Patent No. 7,490,151 (“’151 patent”), a division of the ’135 patent.)

constitutes an implicit part of the claimed intercept clause. Addressing similar arguments by Patent Owner, the Board made a similar determination in the '237 FWD. *See* '237 FWD 12 (“the record shows that the additional functionality urged by Patent Owner should not be imported into the intercepting phrase”).

To support its construction, Patent Owner points to embodiments drawn to a VPN, which includes DNS proxy 2610. PO Resp. 5. Patent Owner also argues “the claimed embodiments differ from [a] conventional DNS, in part, because they apply an additional layer of functionality to a request to look up a network address beyond merely resolving it and returning the network address.” *Id.* (citing Ex. 2009 ¶ 24).

According to Patent Owner, these “example” “additional . . . functionality” features include the following:

For example, the DNS proxy 2610 may intercept the request and “determine[] whether access to a secure site has been requested,” “determine[] whether the user has sufficient security privileges to access the site,” and/or “transmit[] a message to gatekeeper 2603 requesting that a virtual private network be created between 40 user computer 2601 and secure target site 2604.”

Id. (quoting Ex. 1001, 40:34–43; citing Ex. 2009 ¶ 24).

Patent Owner concludes “[t]he Board’s preliminary construction overlooks these aspects that distinguish the ‘intercepting’ phrase from conventional DNS.” *Id.* at 6.

Contrary to Patent Owner’s arguments, none of the challenged claims recite a VPN, a DNS proxy, a non-conventional DNS, or setting up a VPN link. Furthermore, the additional disclosed functions of a DNS or VPN fail

to show that the “intercept” clause at issue requires the unclaimed additional functionality.

In addition, the disclosed VPN embodiment cited by Patent Owner supports Petitioner’s proposed claim construction, as DNS server 2602 performs the intercept by “receiving a request pertaining to a first entity [2604 or 2611] at another entity [2602].” As the ’516 patent discloses, in one embodiment, a “single server” 2602 having “the functions of DNS proxy 2610 and DNS server 2609” (Ex. 1001, 41:4–6, Fig. 26) “intercepts all DNS lookup functions” (*id.* at 40:34–36). In other words, pursuant to requests for a connection to a secure or unsecure device (first entity), intercepting DNS server 2602 (another entity) returns the IP address of the first entity after looking up the domain name. *See id.* at 40:24–52; Pet. 11 (“Because the request is seeking an address corresponding to a destination (*e.g.*, site 2604 or 2611), it pertains to an entity other than DNS proxy 2010 or DNS server 2609. Thus, the ’516 patent uses the term ‘intercept’ as meaning receipt by an entity of a message pertaining to a different entity.”).

Based on the foregoing discussion, we maintain Petitioner’s proposed construction as adopted in the Institution Decision. The phrase “intercept . . . a request” means “receiving a request pertaining to a first entity at another entity.” As indicated above (note 1), this claim construction comports with our previous final decisions (*e.g.*, ’237 FWD and ’331 FWD).⁶ Patent

⁶ *See* ’237 FWD 12 (reaching materially the same construction for a similar phrase). As also noted in the ’237 FWD (a final judgment affirmed by our reviewing court, *supra* note 1), “Patent Owner concedes that ‘[t]he *Decision’s construction* [of intercepting a request] *addresses* a common aspect of *a conventional DNS and the disclosed embodiments*, namely that a request to look up an address of one entity may be received at another

Owner does not present arguments or evidence showing a reason to modify the previous construction, and Patent Owner does not argue its proposed claim construction is dispositive.

2. Other Terms

Petitioner and Patent Owner each proffer proposed constructions of several claim terms. Pet. 9–14; PO Resp. 2–11. Neither party identifies a dispositive term for construction. No other claim term or clause needs express construction. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (only terms in controversy require an explicit construction and only to the extent necessary to resolve the controversy). To the extent any term requires explicit construction, we rely on our previous constructions in the ’237 FWD, with the evidence and arguments here and those cases materially the same. *See* Pet. 9–14; PO Resp. 2–11; ’237 FWD 5–15; note 5 (same common ancestor patent).

B. Prior Art Printed Publication Status of RFC 2401

Patent Owner asserts that Petitioner fails to show that RFC 2401 was publicly accessible as of November 1998 (the date recited on each of its pages). PO Resp. 34 (citing Ex. 1008). On this basis, according to Patent Owner, Petitioner cannot rely upon RFC 2401 as prior art to meet its burden of showing obviousness of the challenged claims over the combination of Beser and RFC 2401. *See id.*

The determination of whether a given reference qualifies as a prior art “printed publication” involves a case-by-case inquiry into the facts and circumstances surrounding the reference’s disclosure to members of the

entity.” ’237 FWD 24 (quoting ’237 Patent Owner Response 26) (emphases added).

public. *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004). On its face, RFC 2401 is a dated “Request for Comments” from the “Network Working Group,” discussing a particular standardized security protocol for the Internet. Ex. 1008, 1. Moreover, RFC 2401 describes itself as a “document [that] specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. . . . Distribution of this memo is unlimited.” *Id.* These indicia suggest that the document was accessible by the interested public (over the Internet), in order to obtain feedback prior to implementation of the standard it describes.

To bolster its showing, Petitioner provides evidence suggesting that RFC 2401 would have been accessible to the interested public. For example, Petitioner relies on testimony by Dr. Tamassia, and at least two articles dated prior to February 2000, referencing RFC 2401 availability on a website. Pet. 23–24 (citing Ex. 1003 ¶¶ 117–19, 124–25; Ex. 1064, 9; Ex. 1065, 3). As one example, Ex. 1064, an August 16, 1999 magazine article, discusses RFC 2401 and IPsec protocols and states “[a]ll of these documents are available on the IETF website.” Ex. 1064, 9.

Petitioner explains that RFC 2401 describes the IPsec protocol promulgated by the Internet Engineering Task Force (IETF). Pet. 25–26. Petitioner provides the Ginoza Declaration, by Sandy Ginoza, who, acting as a designated representative of the IETF, previously testified that RFC 2401 was published on the RFC Editor’s website and was publicly available in November 1998. *Id.* at 24–25 (citing Ex. 1060 ¶¶ 105–07; Ex. 1063, 39:14–40:24). Petitioner provides additional documentary evidence in the form of an October 1996 RFC 2026 publication (Ex. 1036, 5–6 (explaining that any

interested person can obtain RFC documents from a number of Internet hosts using anonymous FTP, gopher, WWW, and other document-retrieval systems)). Pet. 23 (citing Ex.1036, 3, 5). The additional documentary evidence further corroborates the indicia of availability on the face of RFC 2401. Exhibit 1036, RFC 2026, states it reflects “generally-accepted practices” for RFC documents and states any interested person can obtain RFCs “from a number of Internet hosts.” Ex. 1036, 4, 6. “They [the procedures described in the document] provide ample opportunity for participation and comment by all interested parties.” *Id.* at 4 (“The goal of technical competence, the requirement for prior implementation and testing, and the need to allow all interested parties to comment all require significant time and effort.”).

Patent Owner characterizes Petitioner’s showing as insufficient. PO Resp. 34–39. Patent Owner contends that Sandy Ginoza and Dr. Tamassia lack personal knowledge about the publication of RFC 2401, and challenges other evidence as too general and lacking a sufficient foundation. *See* PO Resp. 34–38 (discussing Pet. 24–26, Ex. 1036, 4–5; Ex. 1060–65; Ex. 2022, 22: 7–19). Patent Owner does not contest Petitioner’s characterization of the two magazine articles, Exhibits 1064 and 1065, other than to refer to them as follows: “Exhibit 1064 is allegedly an article from InfoWorld magazine (dated August 16, 1999) and Exhibit 1065 is allegedly an article from NetworkWorld magazine (dated March 15, 1999).” PO Resp. 36. As Petitioner argues, the articles show that “the skilled person would have known that RFCs such as RFC 2401 could be downloaded from the IETF’s website.” Reply Br. 18 n.2.

In addition, RFC 2026 states it reflects “generally-accepted practices” for RFC documents and states any interested person can obtain RFCs “from a number of Internet hosts.” See PO Resp. 38 & n.6 (citing Ex. 1036, 4, discussing Inst. Dec. 11); Ex. 1036, 4, 6. Patent Owner contends that Petitioner has not shown that this evidence of “generally accepted practices” “is accurate.” *Id.* Patent Owner notes that the document represents “flexible” standards, so that “there is no assurance that the procedures of RFC 2026 that were quoted by Petitioner were actually applied.” *Id.* at 38.

We find Dr. Tamassia’s testimony as to public accessibility of RFCs based on his general knowledge as a user of RFCs to be credible, especially given the independent support of RFC 2026 (Ex. 1036).⁷ See Ex. 1003 ¶¶ 116–23; Ex. 2019, 103:1–12 (testifying his “business includes having viewed RFCs, having discussed RFCs”), 106:11–17 (describing an RFC document); Ex. 1036, 5–6. Moreover, RFC 2401’s contents are consistent with the publication process described by RFC 2026 and Dr. Tamassia, including the inclusion of a date “November 1998” on the top right corner of the first page of the document. Ex. 1008, 1. In addition, this document—a request for suggestions and improvements for an Internet standards protocol, having no indication of being a mere draft or internal paper—is precisely the type of document whose very purpose is public disclosure, including on the Internet. Both of the magazine articles, Exhibits 1064 and 1065, further corroborate the indicia of availability on the face of RFC 2401, although they are not necessary to our finding of public accessibility. We do not rely

⁷ As addressed below, Patent Owner objects and moves to dismiss a number of Exhibits based on hearsay and relevancy. See Paper 21 (Motion to Exclude).

on the testimony of Sandy Ginoza, Exhibits 1060 and 1063, which Patent Owner seeks to exclude as discussed further below.

In making our determination, we note least one District Court characterized RFCs as having “been written and circulated”: “[M]uch of the development and technical management of the Internet has been by the consensus of Internet users. This is evidenced . . . by IETF and the more than 2000 RFC’s which have been written and circulated.” (quoting *PGMedia, Inc. v. Network Sols., Inc.*, 51 F. Supp. 2d 389, 406 (S.D.N.Y. 1999) (internal citation omitted)).⁸

“A given reference is ‘publicly accessible’ upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it.” *SRI Int’l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006)). We find that Petitioner has established, by a preponderance of the evidence, that RFC 2401 (dated November 1998) was disseminated and made available to persons of ordinary skill interested in computer networking and security to be deemed “publicly accessible” at the relevant time. Therefore, on this record, we determine RFC 2401 qualifies as a prior art printed publication under 35 U.S.C. § 102(b).

C. Tamassia Declaration (Ex. 1003)

Patent Owner argues that the entirety of the Tamassia Declaration should be given little or no weight because Dr. Tamassia “failed to consider,

⁸ See ’331 FWD (Paper 29), 13 (citing the case).

let alone opine on, how any of the claim features are disclosed in asserted references.” PO Resp. 42. Patent Owner also contends “the technology involved is undisputedly complex,” and “[t]he cited references are similarly complex, and require explanatory expert testimony.” *Id.* at 45.

Petitioner responds that Dr. Tamassia has “offered probative testimony on many of the factual inquiries underpinning an obvious[ness] analysis” that “can certainly ‘help the trier of fact to understand the evidence or determine a fact in issue.’” Pet. Reply 19 (quoting Fed. R. Evid. 702).⁹ Petitioner also contends “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.” *Id.* at 20.

Patent Owner does not articulate a persuasive reason for giving Dr. Tamassia’s declaration, as a whole, little or no weight in our analysis. We agree with Petitioner that the panel can determine the appropriate amount of weight to afford to expert testimony without requiring the expert to opine on every relevant factual and legal issue. The cases upon which Patent Owner relies do not show otherwise. For example, Patent Owner cites *Schumer v. Lab. Comput. Sys., Inc.*, 308 F.3d 1304, 1315 (Fed. Cir. 2002), for the proposition that “[expert] testimony . . . *must* identify each claim element, state the witnesses’ interpretation of the claim element, and explain in detail how each claim element is disclosed in the prior art reference.” PO Resp. 43 (emphasis by Patent Owner).

⁹ The parties do not dispute the panel’s preliminary findings regarding qualifications of a person of ordinary skill in the art, maintained here after considering the record anew. *See* Inst. Dec. 14–15 (citing *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (prior art can reflect the appropriate level of ordinary skill in the art)).

Patent Owner's quotation of *Schumer* omits introductory words necessary to the meaning of the quoted sentence. In its entirety, the quoted portion of *Schumer* states the following:

Typically, testimony concerning anticipation must be testimony from one skilled in the art and must identify each claim element, state the witnesses' interpretation of the claim element, and explain in detail how each claim element is disclosed in the prior art reference. The testimony is insufficient if it is merely conclusory.

Schumer, 308 F.3d at 1315–16 (emphasis added). The Federal Circuit then adds that it is not the task of the courts to “attempt to interpret confusing or general testimony to determine whether a case of invalidity has been made out” and “if the testimony relates to prior invention and is from an interested party, as here, it must be corroborated.” *Id.* at 1316. Instead of requiring a specific format for the content of all testimony regarding invalidity as asserted by Patent Owner, this portion of *Schumer* confirms that a tribunal should not rely upon conclusory, overly general, confusing, and self-interested testimony. *Id.*; see also *Koito Mfg. Co., Ltd. v. Turn-Key-Tech, LLC*, 381 F.3d 1142, 1152 (Fed. Cir. 2004) (“General and conclusory testimony, such as that provided by Dr. Kazmer in this case, does not suffice as substantial evidence of invalidity.”). Patent Owner does not show that the whole of Dr. Tamassia's testimony suffers from any of these failings.

As Petitioner notes, in *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064 (Fed. Cir. 2015), the Federal Circuit states that in IPRs, “Board members, because of expertise, may more often find it easier to understand and soundly explain the teachings and suggestions of prior art without expert assistance.” Pet. Reply 21 (quoting *Belden*, 805 F.3d at 1079). Relying on

Belden, the court dismissed Patent Owner’s similar argument in its appeal of the related ’238 FWD, holding “even if the record contains expert testimony, the law does not require the PTAB to rely upon it.” *VirnetX*, 665 F. App’x at 884 (quoting Patent Owner’s argument: “[B]ecause [according to *VirnetX*] ‘the technology involved is undisputedly complex,’ *VirnetX* avers that the PTAB could not have made ‘unpatentability findings in the absence of any supporting expert evidence.’”) (nonprecedential). The ’237 IPR and ’238 IPR (challenging the same patent) involved the same secure communications technology as involved here (*supra* note 5).

Under 35 U.S.C. § 316(e), the preponderance of the evidence standard governs in determining whether Petitioner establishes unpatentability. We exercise discretion to determine the appropriate weight to accord the evidence presented, including expert opinions, based on the underlying facts supporting the opinion. We accord relevant portions of Dr. Tamassia’s testimony the appropriate weight based on that particular testimony and supporting evidence.

D. Obviousness Over Beser and RFC 2401

1. Overview of Beser

Beser describes a system that establishes an IP (internet protocol) tunneling association on a public network between two end devices. *See* Ex. 1007, Abs.

Figure 1 of Beser follows:

FIG. 1

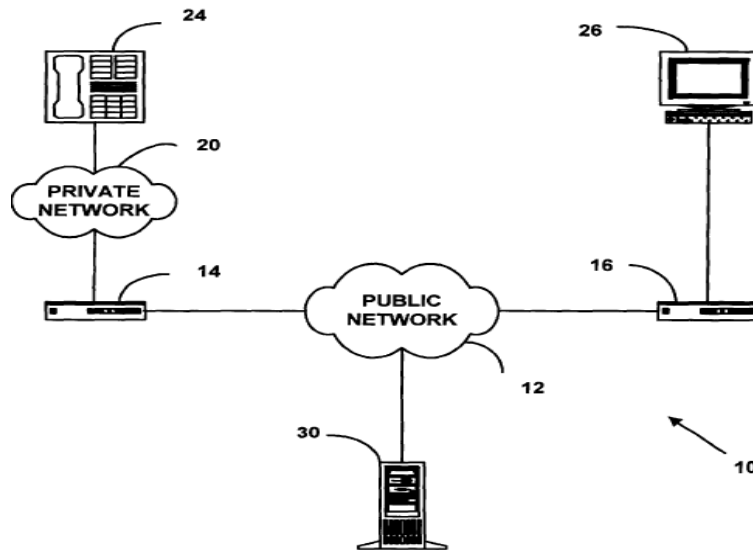


Figure 1 of Beser illustrates a network system, including public network 12, network devices 24 and 26, private network 20, trusted third-party network device 30, and modified routers or gateways 14 and 16. Ex. 1007, 3:60–4:19, 43–44. Beser describes network devices 24 and 26 as telephony devices, multimedia devices, VoIP devices, or personal computers. *Id.* at 4:43–52.

Beser’s system “increases the security of communication on the data network” by providing and hiding, in packets, “private addresses” for originating device 24 and terminating device 26 on the network. *See id.* at Abs., Fig. 1, Fig. 6. To begin a secure transaction, requesting device 24 sends a request to initiate a tunneling connection to network device 14. *Id.* at 8:21–47. This request includes a unique identifier for the terminating end of the tunneling association—terminating device 26. *Id.* at 7:64–8:3. The packets used to transfer this unique identifier across the public network

“may require encryption or authentication to ensure that the unique identifier cannot be read on the public network.” *Id.* at 11:22–25. Beser discloses, as background prior art, known forms of encryption for the information inside these packets, including IP Security (“IPsec”). *Id.* at 1:54–56. Once network device 14 receives the request, it passes the request to trusted-third-party network device 30. *Id.* at 8:3–4, 8:48–9:5.

Trusted-third-party network device 30 contains a directory of users, such as a DNS, which retains a list of public IP addresses associated at least with second network device 16 and terminating devices 26. *See id.* at 11:32–58. DNS 30 associates terminating network device 26, based on its unique identifier in the request, with a public IP address for router device 16. *See id.* at 11:26–36. Trusted-third-party network device 30 then assigns, by negotiation, private IP addresses to requesting network device 24 and terminating device 26. *Id.* at 9:29–35, 12:16–19. The negotiated private IP addresses are “isolated from a public network such as the Internet,” and “are not globally routable.” *Id.* at 11:62–65.

2. Overview of RFC 2401

RFC 2401 describes security services using IPsec protocols on the Internet (Ex. 1008, 3) including “access control, connectionless integrity, data origin authentication, [and] . . . confidentiality (encryption)” (*id.* at 4). According to RFC 2401, one of the IPsec goals is to provide “confidentiality (encryption).” *Id.* at 4. Using IPsec protocols

allows the user (or system administrator) to control the granularity at which a security service is offered. For example, one can create a single encrypted tunnel to carry all the traffic between two security gateways or a separate encrypted tunnel

can be created for each TCP connection between each pair of hosts communicating across these gateways.

Id. at 7.

3. *Claims 1, 2, 12, 15, 16, and 26*

i) *Petitioner's Contentions*

Petitioner contends that Beser teaches or suggests most of the limitations of claims 1 and 15, with Beser and RFC 2401 teaching or suggesting encryption of data. *See* Pet. 36–47. Petitioner's showing for claim 15 tracks that of claim 1. *See id.* Petitioner asserts that Beser's streaming audio/video and other examples that include multimedia and VoIP, in light of end-to-end encryption teachings based on the combination of Beser and RFC 2401, would have rendered obvious claims 1 and 15. *See* Pet. 36–46.

Addressing the preambles claims 1 and 15, Petitioner contends that the claimed first network device reads on Beser's originating end device 24, and that the claimed second network device reads on Beser's terminating end device 26. *See id.* at 36 (citing Ex. 1007, 8:15–20, 21:52–62, 22:2–22; Ex. 1003 ¶ 126, 167–68); Ex. 1007, Fig. 1. Petitioner points out that Beser discloses various end devices including WebTV devices and VoIP devices that communicate over a private tunneling association established by trusted-third-party network device 30 aided at least by first network device 14. *See* Pet. 38 (citing Ex. 1007, 8:21–49, 8:65–9:1, 10:22–23, 11:45–58; Ex. 1003 ¶¶ 151, 152, 169, 174–77).¹⁰

¹⁰ Note that Beser's first 14 and second 12 network devices do not correspond to the claimed "first" and "second" network devices; rather, Petitioner reads those claimed devices on Beser's originating 24 and terminating 26 devices, as just noted. Pet. 36–37.

Regarding the respective “intercept” and “intercepting” clauses of claims 1 and 15, Petitioner explains that Beser’s trusted-third-party network device 30 (which includes a DNS), first network device 14, and second network device 12, work together such that devices 30 and 14 look up private and public IP addresses based on a request from originating device 24 that includes a unique domain name for the claimed target device—terminating end device 26. *See id.* at 37–39 (citing Ex. 1007, 4:9–11, 8:21–47, 10:22–23, 10:37–42, 10:55–11:5, 11:26–36, 11:45–58, Figs. 6, 9; Ex. 1003 ¶¶ 151–52, 169, 174–77, 182–83); Ex. 1007, 13:49–65, 14:2–14, 16:1–37. According to Petitioner, Beser’s first network device 14 and trusted-third-party device 30 constitute “another entity” that intercepts the request pertaining to first entity 26 according to the claim construction of “intercept” as set forth above. Pet. 38–39; *supra* Section II.A (Claim Construction).

Petitioner also contends the request by originating device 24 constitutes “a request to look up an internet protocol (IP) address of the second network device” 26 as claim 1 recites. *See id.* at 39. The Petition at one point identifies two IP addresses: “the IP address of second network device 16 that is associated with the unique identifier and the terminating device 26, (Ex. 1007, 11:26–36, 11:45–58), and a private IP address for terminating device 26, (*id.*, 9:29–30, 12:16–19, 14:14–27, Figs. 6 & 9).” *Id.* (citing Ex. 1003 ¶¶ 175, 182–83, 192–94).

The Petition also identifies a third IP address, the public IP address for terminating device 26:

Beser explains that the trusted-third-party network device can be a domain name server that functions according to industry standards (Ex. 1007, 4:55–63, 11:32–36; Ex. 1003 ¶¶ 155–58), but is modified to maintain a database correlating each

registered unique identifier to “the IP 58 address of a particular second network device 16” and may also include “public IP 58 addresses for the terminating telephony device 26,” (Ex. 1007, 11:48–52).

Pet. 40 (citing Ex. 1007, 8:65–9:1, 11:26–58; Ex. 1003 ¶¶ 159–62).

In summary, as Petitioner indicates, Beser teaches that trusted-third-party network device 30, operating as a modified DNS 30, includes, in a directory database or otherwise, stored public IP addresses for router 16 and terminal device 26, and other data and functionality to associate devices 16 and 26 together. In other words, trusted-third-party network device DNS 30, includes the “IP 58 addresses for the terminating . . . device[s] 26,” and uses “data structures . . . known to those skilled in the art . . . for the association of the unique identifiers [for terminating devices 26] and IP 58 addresses for the . . . network devices 16”—including domain names as unique identifiers, as noted above. See Ex. 1007, 11:48–55, 4:55–63, 11:2–5, 11:32–36; Ex. 1003 ¶¶ 153–158.

Regarding the respective “determine” and “determining” clauses of claims 1 and 15, Petitioner relies partly on its showing with respect to DNS 30 functions as described above, and contends that “Beser teaches that the trusted-third-party network device [30] determines whether the unique identifier in a request specifies a destination that can establish a secure tunnel by checking its internal database of registered users or devices.” Pet. 40 (citing Ex. 1007, 11:30–36, 11:45–58; Ex. 1003 ¶ 162). According to Petitioner, “[t]his is done ‘*in response to the request*’ and is the same type of ‘determining’ disclosed in the ’516 patent.” *Id.* (citing Ex. 1001, 40:28–35).

Petitioner contends that Beser’s negotiating devices (14, 30, and 16, see Ex. 1007, Fig. 9), as modified by RFC 2401, thereby facilitate a

connection with terminating end device 26 over a secure network created in response to interception (by device 30, or devices 14 and 30) of a request to look up an internet address based on a domain name for end device 26, and determines as a result that end device 26 is a device with which a secure communication link can be established, as claim 1 requires. *See* Pet. 40–42 (citing Ex. 1007, 9:6–11, 9:26–30, 11:9–44, 11:59–62; Ex. 1003 ¶¶ 162–63, 175–77).

Petitioner explains that, as combined with the secure aspects of RFC 2401, if the unique identifier or domain name is not registered, trusted-third-party network device 30 will not negotiate an IP tunnel and instead “will process the request normally” and “will simply route subsequent packets from the originating device without attempting to establish a secure IP tunnel.” Pet. 41 (citing Ex. 1007, 8:21–50; Ex. 1003 ¶¶ 150–52). Petitioner explains “registered devices are those that support the Beser tunneling technique,” so that determining if a device is registered for a tunnel connection satisfies the “determine” clause. *See id.* (citing Ex. 1007, 11:59–62); *see also* Ex. 1007, 9:6–11, 9:26–30, 11:9–44, 11:59–62; Ex. 1003 ¶¶ 162–63, 175–77, 233–37. In other words, according to Petitioner, in the combined system suggested by Beser and RFC 2401, a registered device “supports secure communications (*i.e.*, it supports Beser’s IP tunnel configured [as combined] to provide end-to-end encryption).” *Id.* (citing Ex. 1003 ¶¶ 233–37); *see also* Pet. 30–35 (discussing encryption and reasons to include encryption in Beser’s system). Dr. Tamassia points out that Beser discloses authentication and encryption, and discloses connecting to establish connections to, or between, corporate offices. *See* Ex. 1003

¶ 225, 227. Petitioner shows by a preponderance of evidence that Beser, with or without RFC 2401, teaches or suggests the steps outlined above.

Further regarding encryption and determination as recited in the encryption clauses of claims 1 and 15 (i.e., respectively “initiate” or “initiating” “an encrypted communication link . . . based on a determination that the second network device is available for the secure communications service . . . using the encrypted communication link . . . the first network device . . . to access the encrypted communication link”), Petitioner persuasively shows that based on a determination as claimed, “it at least would have been obvious to configure the Beser IP tunneling scheme to include end-to-end encryption of all IP traffic based on the teachings of RFC 2401, in addition to using private network addresses for the traffic sent between the originating and terminating end devices.” *See id.* at 43 (citing Ex. 1003 ¶ 233; Ex. 1008, 25). Petitioner notes Beser discloses, in discussing background art, that the “IPsec” (IP Security) protocol (which RFC 2401 discloses), and a “sender may encrypt the information inside the IP packets before transmission, e.g., with IP Security (‘IPSec’).” Pet. 30–31 (quoting Ex. 1007, 1:54–56; citing Ex. 1003 ¶ 232).

Petitioner also sets forth several reasons why the ordinary artisan would have used encryption in Beser’s tunneling system based on the recited determination. *See* Pet. 30–35. Petitioner generally contends it would have been obvious to employ encryption to ensure that data and/or anonymity can be made more secure, concerns that Beser and RFC 2401 teach or suggest. *See* Pet. 30–35, 42–46. Petitioner also contends that Beser discloses encryption employed to hide addresses in its tunneling scheme, criticizes prior art systems that do not use encryption, discusses challenges to data

encryption, and implies a trade-off between power and data quality for audio and video streaming. *See* Pet. 30–35, 42–46; Ex. 1007, 1:54–2:40, 11:22–25, 18:2–5, 20:11–14.

Petitioner also contends that

a person of ordinary skill would have understood that standard techniques, such as IPsec, can and should be used to implement the Beser scheme, as this is the practice that Beser identifies is conventionally followed. Ex. 1003 ¶¶ 217–20; Ex. 1007, 1:54–56, 2:12–14; *see also id.*, 11:22–25, 18:2–5, 20:11–14. In particular, a person of ordinary skill would have been specifically motivated to encrypt IP traffic within the IP tunnel of Beser pursuant to the guidance in RFC 2401, which describes the IPsec protocol referenced in Beser.

Id. at 33 (citing Ex. 1003 ¶¶ 219, 227–29; Ex. 1007, 1:54–56; Ex. 1008).

Petitioner contends that Beser “also indicates that its IP tunneling schemes are compliant with standards-based processes and techniques (*e.g.*, IPsec), and can be implemented using pre-existing equipment and systems” and that “IP tunnels are and should ordinarily be encrypted, even in the streaming media example.” *Id.* at 30–31 (citing Ex. 1007, 1:54–56, 4:55–5:2, 11:22–25, 18:2–5; Ex. 1003 ¶¶ 221–24).

Petitioner contends that a person of ordinary skill would have recognized good reasons for readily incorporating IPsec encryption teachings into Beser’s system. *Id.* at 33–34 (citing Ex. 1003 ¶ 233).

Petitioner describes similarities in basic configurations of Beser and RFC 2401. *Id.* at 34 (characterizing Beser and RFC 2401 as each disclosing “one tunnel between two security gateways such as edge routers, and another tunnel between the two end devices”) (citing Ex. 1003 ¶¶ 229–31; Ex. 1008, 25, Ex. 1007, Fig. 1).

In summary with respect to encryption, Petitioner shows persuasively that it would have been obvious to encrypt data in Beser's tunneling system in order to protect the data, a mechanism so well-known at the time of the invention as a major component of security that RFC 2401 established IPSec protocols for it, which Beser discusses. Ex. 1007, 1:54–56 (“Of course, the sender may encrypt the information inside the IP packets before transmission, e.g. with IP Security (‘IPSec’).”); Ex. 1008, 7 (“IPsec allows the user (or system administrator) to control the granularity at which a security service is offered.”); Ex. 1001, 1:60–61 (admitting “[d]ata security is usually tackled using some form of data encryption.”).

Petitioner cites Beser's computers and servers, including Beser's trusted-third-party server 30 embodiment, as teaching or suggesting the “one or more servers” limitation recited in claim 1. See Pet. 46–47 (citing Ex. 1007, 4:9–11, 10:37–42, 10:55–11:5; Ex. 1003 ¶¶ 134–35, 145, 155–59).¹¹

Petitioner's showing with respect to independent claims 1 and 15, in light of the record and summary above, establishes by a preponderance of evidence that claims 1 and 15 would have been obvious.

Claims 2 and 16 depend from claims 1 and 15, respectively. Claim 2

¹¹ The preamble of claim 1 recites “the system including one or more servers configured to,” followed by listed functions in the body of claim 1. As noted in the Institution Decision, claim 1 does not require the servers necessarily to perform the recited functions, because the preamble indicates the system itself may be configured to perform the recited functions using other than one or more servers. Inst. Dec. 22–23 & n.8. Alternatively, Petitioner also shows sufficiently that Beser discloses or suggests one or more servers as a trusted-third-party device or other computers that perform serving functions. See Pet. 46.

further specifies that the secure communications service includes an “audiovideo conferencing service” that communicates “at least one of encrypted video data and audio data over the encrypted communication link.” Ex. 1001, 56:33–36. Claim 16 further specifies that the secure communications service includes a “video conferencing service” that communicates “at least one of encrypted video data and audio data over the encrypted communication link.” Ex. 1001, 57:28–31. In other words, claims 2 and 16 require encryption of at least one of audio data and video data respectively during an audio-video service and a video service.

Relying on Dr. Tamassia, citations to Beser and RFC 2401, and partly on its similar contentions with respect to claims 1 and 15, Petitioner persuasively contends that the combination suggests encrypting multi-media traffic to secure data, and that skilled artisans would have recognized that any problems associated with encryption could be overcome by providing sufficient computing power. Pet. 47–48 (citing Ex. 1007, 1:54–56, 2:22–24, 2:43–45, 4:43–54, 6:24–57, 9:64–10:2; Ex. 1003 ¶¶ 164–65, 208, 223–24, 227–28; Ex. 1055, 206:20–208:6 (citing Patent Owner’s expert in a related proceeding as conceding that increasing power could overcome encryption problems)).

Petitioner shows by a preponderance of evidence that providing encryption of video or audio data in Beser’s system as suggested further by RFC2401 would have been obvious, wherein Beser’s system provides multimedia devices such as Web-TV and VoIP services. See Ex. 1007, 4:47–50; Pet. 47–48 (citing Ex. 1007, 1:54–56, 2:22–24, 2:43–45, 4:43–54, 6:24–57, 9:64–10:2; Ex. 1003 ¶¶ 164–65, 208, 223–24, 227–28, 233; Ex. 1008, 4, 7, 10). As noted above, challenged claims 2 and 16 require

encryption of “audio data” within an “audio-video conferencing service,” without any specified audio or video data rate for the encrypted data. As Dr. Tamassia’s credible testimony shows,

[a] person of ordinary skill in the art would recognize that the concerns expressed in Beser in connection with encryption of high volumes of network traffic [i.e., multimedia] can be easily resolved by simply using more powerful equipment. Alternatively, systems may be configured to transmit multimedia content using less data (e.g., by using lower resolution video).

Ex. 1003 ¶ 224. Petitioner also persuasively shows that the IPsec protocol “was known to be highly adaptable, enabling it to accommodate computational burdens of a particular configuration by adjusting parameters of the IPsec protocol (e.g., adjusting the strength or type of encryption used).” Pet. 48 (citing Ex. 1008, 4, 7, 10; Ex. 1003 ¶ 208).

In addition, Dr. Tamassia credibly explains

[a] person of ordinary skill in the art reading Beser in February 2000 would also have understood that encryption should ordinarily be used even in high data volume applications, if possible. Beser only warns that it *may* not be possible to encrypt every packet and maintain transmission quality due to computer power limitations (e.g., during times of high network traffic). Ex. 1007 at 1:62–67, 2:15–17. Beser refers to the use of encryption in IP tunneling schemes as a conventional technique that is ordinarily used. See Ex. 1007 at 1:54–56, 2:12–14.

Ex. 1003 ¶ 223.

Addressing the related “end-to-end” encryption limitations recited in dependent claims 12 and 26, Petitioner relies partly on its showing with respect to independent challenged claims 1 and 15, and sets forth the following persuasive showing:

Beser suggests encryption of audio and video, and a person of ordinary skill considering Beser's IP tunneling scheme in view of RFC 2401 would have found it obvious to encrypt communications end-to-end. Ex. 1003, ¶¶227, 233. In the combined system, Beser's IP tunnel would have provided anonymity for communications, and IPsec, as shown in Case 3 of RFC 2401, would have provided end-to-end encryption. Ex. 1008, 25; Ex. 1003, ¶¶229–33. As discussed above (§§ IV.C.2, IV.C.4 [Pet. 30–35, 47–49]), the skilled person would have recognized such encryption was conventional, and any practical issues with certain data transmission scenarios could be overcome by providing more computing power, changing the resolution of any multimedia data transmitted, or changing the granularity of encryption. Ex. 1003, ¶¶208, 219–25.

Pet. 54–55.

Petitioner's showing regarding challenged independent claims 1 and 15, and challenged dependent claims 2, 12, 16, and 26, in light of the record and as summarized above, establishes by a preponderance of evidence that these challenged claims would have been obvious.

ii) Patent Owner's Arguments

*a. A Request to Look Up an Internet Protocol (IP)
Address of the Second Network Device Based on a
Domain Name Associated with the Second Network Device*

As noted above, claim 1 recites “intercept, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on an identifier associated with the second network device.” Claim 15 recites a similar “intercepting” feature. As construed above, “intercept . . . a request” means “receiving a request pertaining to a first entity at another entity.” *See supra* Section II.A.1. Patent Owner does not dispute Petitioner's persuasive showing that Beser discloses the “intercept” feature of claim 1, and the similar “intercepting” feature of claim

15. *See* PO Resp. 17–19.¹² Claim 1 does not specify which device performs an intercept.

Rather, Patent Owner challenges Petitioner’s showing with respect the following clause recited in claims 1 and 15: “a request to look up an internet protocol (IP) address of the second network device based on an identifier associated with the second network device.” *Id.* at 17–21. Patent Owner contends “[n]one of the processes in Beser transform the request to initiate a tunneling connection into a request to look up an IP address.” *Id.* at 21.

Patent Owner advances a number of related arguments. For example, Patent Owner argues Beser’s trusted-third-party device does not negotiate private addresses, and even if it does, “negotiation does not involve looking up any IP address, but rather involves *assignment* of a first private network address to the originating device and a second private network address to the terminating device.” *Id.* at 18–19 (citing Ex. 1007, 12:2–4; Ex. 2018 ¶ 43). Patent Owner concedes “*Beser . . . states that the database entry in the trusted-third-party network device 30 may include a public IP 58 address for the terminating telephony device 26.*” *Id.* at 19 (citing Ex. 1007, 11:50–55 (emphasis added)). But Patent Owner contends “*Beser* never suggests that this [domain name/public IP address] data structure is looked up when the tunnel request is received by device 30, let alone that the public address of telephony device 26 is specifically looked up.” *Id.* (citing Ex. 2018 ¶ 44). Patent Owner contends Beser “only teaches that when a trusted-third-party

¹² To the extent Patent Owner may argue it raised this “intercept” issue here, we addressed it in the related ’331 FWD and the ’237 FWD, which involved materially the same evidence and arguments, and we incorporate that discussion and findings here. *See* ’331 FWD 27–29; ’237 FWD 22–28 (finding Beser discloses materially the same limitation).

network device 30 is informed of a request to initiate a tunnel, it *associates* a public IP address of a second network device 16 with the unique identifier of terminating telephony device 26.” *Id.* at 19 (citing Ex. 1007, 11:26–32; Ex. 2018 ¶ 44) (emphasis added). Patent Owner similarly argues “the negotiation does not involve looking up any IP address, but rather involves *assignment* of a first private network address to the originating device and a second private network address to the terminating device.” *Id.* at 18–19 (citing Ex. 1007, 12:2–4; Ex. 2018 at ¶ 43).

Patent Owner also contends that Beser discloses a bifurcated DNS system that does not provide a look up with “alleged additional functionality.” *See id.* at 20–21 (arguing “there is simply no evidence suggesting that the alleged typical look up functionality of a DNS would apply to the alleged additional functionality of trusted third party network device 30”). By “additional functionality,” Patent Owner implies it refers to Beser’s “tunneling application that can detect packets that need special processing.” *See id.* at 20 (citing Ex. 1003 ¶ 161). Patent Owner concludes that “[n]one of the processes in *Beser* transform the request to initiate a tunneling connection into a request to look up an IP address.” *Id.* at 21.

These arguments appear to attempt to draw a distinction between “look up” and “associates” (or “assigns”) that does not exist in light of the ’516 patent Specification. Beser’s tunneling system must “look up” an IP address based on a domain name (or other unique identifier) in order to associate or assign an IP address or other addresses with the requested terminating telephony device 26. *See* Ex. 1007, 10:37–11:58, Figs. 5–7; Reply Br. 7–8; *infra* notes 14–15 (look up DNS functionality was well known and disclosed as conventional in Beser). Like Patent Owner, Dr.

Monrose does not explain the basis for any distinction. See Ex. 2018 ¶ 44 (testifying Beser “associates a public IP address of a second network device 16 with the unique identifier of a terminating telephony device 26” after being “informed of a request to initiate a tunnel”—without stating why that association does not inform a skilled artisan that the association means the public IP address is “looked up”).

Dr. Monrose’s testimony, combined with Beser’s disclosure that trusted-third-party device 30, a “domain name server” (Ex. 1007, 11:34), may include a “*database entry . . . includ[ing] a public IP 58 address[] for the terminating telephony device 26*” (*id.* at 11:50–52 (emphasis added)) shows Beser teaches using that public IP 58 address, so it must look it up. See Ex. 1007, 11:34, 50–55; *infra* notes 14–15 (DNS functionality well known). In other words, Dr. Monrose’s testimony supports Petitioner’s showing that Beser’s system includes “a request to look up an internet protocol (IP) address of the second network device [26 in Beser] based on an identifier associated with the second network device [unique identifier for device 26].”

As Petitioner also contends, “Beser discloses embodiments where trusted device 30 performs the negotiation with the first and second network devices (14 & 16).” Pet Reply 8–9 (citing Ex. 1007, 9:29–30, 12:16–19, 14:19–27, Figs. 6, 9; Pet 20–21, 34).¹³ Beser’s “trusted-third-party 30 may

¹³ The intercept clause does not require a single device to intercept the request. To the extent Patent Owner makes an implied argument related to the intercept clause (*see supra* note 11), Petitioner persuasively addresses it as follows:

This request is intercepted by each of first network device 14 and trusted-third-party network device 30. *Id.* In IPR2014-

be . . . a domain name server” or other typical database structure. Ex. 1007, 4:9–11; *accord* Ex. 1007, 10:41–57, 11:33–34. The “request includes a unique identifier for the terminating telephony device 26” that may be “a dial-up number, an electronic mail address, or a domain name.” Ex. 1007, 10:4–6, 10:38–41.

Given Beser’s teachings, a skilled artisan would have understood that Beser’s trusted-third-party device 30 discloses or at least suggests DNS functionality working with the tunneling application to associate one or more (private and public) IP addresses for the requested device. *See* Pet. 19–22, 39–41; Ex. 1007, 4:7–42, 8:21–52, 9:26–30, 11:9–12:19; Figs. 1, 6, 9; Ex. 1003 ¶¶ 156–63, 170–71, 176–83.¹⁴ As Petitioner contends, and as discussed further below, Beser’s system employs the tunneling application to instigate negotiation, whereby trusted-third-party device 30 responds to that request and “associates” the domain name or other unique identifier of

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, 24 (May 11, 2015).
Pet. Reply 5; ’237 FWD 22–28 (finding Beser discloses materially the same limitation).

¹⁴ Beser’s trusted-third-party device 30, a “domain name server” (Ex. 1007, 11:34), may include a “*database entry . . . includ[ing] a public IP 58 address[] for the terminating telephony device 26*. Many data structures that are known to those skilled in the art are possible *for the association of the unique identifiers and IP 58 addresses for the second network devices 16*” (*id.* at 11:50–55 (*emphases added*)). Therefore, Beser’s DNS 30 implicitly looks up the public IP 58 addresses of devices 16 and 26 based on a domain name (unique identifier) of terminating device 26—in order to associate the two devices.

terminating device 26 with device 16 and a public IP address of device 16 and a public and private IP address of device 26. *See* Ex. 1007, 11:26–32; Pet. 21–22, 39 (discussed further below); Pet. Reply 7; Ex. 1007, 11:51–55 (disclosing a “public IP 58 addresses for the terminating . . . device 26. *Many data structures that are known to those skilled in the art are possible for the association of the unique identifiers and IP 58 addresses for the second network devices 16*”) (emphasis added); *supra* note 14 (discussing the passage), *infra* note 15 (admitting conventional DNS functions provide a look up function).

The ’516 patent and the record support Petitioner’s showing that DNS look up functions or other similar look up functions were conventional and well-known.¹⁵ Notwithstanding Patent Owner’s arguments, based on the record, Beser discloses (or at least suggests) the recited look up function, because a DNS and similar known database structures disclosed by Beser typically must look up stored data base information in order to associate the IP address with a unique identifier. *See* Ex. 1007, 11:9–62, *supra* notes 14, 15.

Quoting Beser, as Petitioner summarizes persuasively, in addition to the public address look up of terminating device 26 that Beser teaches as described above, Beser discloses two other look ups of terminating device

¹⁵ According to the ’516 patent, “[c]onventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host.” Ex. 1001, 39:34–36. In this conventional scheme, “[w]hen the user enters the name of a destination host, a request DNS REQ is made . . . to look up the IP address associated with the name.” *Id.* at 39:44–46.

26 (i.e., its private IP address, and the public IP address of device 16 that also satisfies the disputed intercept of a request for a look up clause):

The tunneling request sent by originating device 24 is a “*request to lookup an [IP] address*” because in response to the request, trusted device 30 looks up two IP addresses: the IP address of second network device 16 that is associated with the unique identifier and the terminating device 26, (Ex. 1007, 11:26–36, 11:45–58), *and a private IP address for terminating device 26*, (*id.*, 9:29–30, 12:16–19, 14:14–27, Figs. 6 & 9). Ex. 1003, ¶¶175, 182–83, 191; *see also* § IV.[C].[3].c [Pet. 39–42], below (analyzing the “determining” step). After the request is processed by Beser’s system, originating device 24 receives an IP address for terminating device 26. Ex. 1007, 21:48–52; Ex. 1003, ¶¶192–94. This is consistent with IPR2014-00237, where the Board found, “Beser’s tunneling request, which includes a domain name, is a request for a look up of an IP address.” [23]7 Final Written Decision, 24, 26 n.6.

Pet. 39 (emphasis added).¹⁶

Therefore, Petitioner contends persuasively that the tunneling request in Beser constitutes a request for a look up, because trusted-third-party device 30 “looks up” a private IP address for terminating device 26 in part by negotiating with device 16 for it, or device 16 looks it up. *See also* Pet. Reply 9 (citing packet 164, which contains a public IP 58 address for device 16, and return packet 166, which contains a private address for device 26 and the public address for device 16) (citing Ex. 1007, Fig. 9 (packets 164 & 166), 13:34–64, 13:66–14:18; Pet. 20–21, 38). In addition to showing Beser teaches a request to look up the public and private addresses for terminating

¹⁶ “As Beser explains, the database contains the list of authorized devices, and each entry in the database includes the unique identifier, the ‘IP 58 address of a particular second network device 16,’ and the ‘public IP 58 addresses for the terminating telephony device 26.’” Pet. 20 (quoting Ex. 1007, 11:48–52).

device 26 as required by claims 1 and 16, Petitioner argues persuasively that the public IP address for device 16 also constitutes an IP address “of” terminating device 26. *See* Pet. 39 (quoted above); Pet. Reply 9.¹⁷ Patent Owner concedes that Beser’s DNS 30 associates the public IP address of device 16 with terminating device 26. *See* PO Resp. 19 (“Beser only teaches that when a trusted-third-party network device 30 is informed of a request to initiate a tunnel, *it associates a public IP address of a second network device 16 with the unique identifier of terminating telephony device 26.*” (emphasis added)). As Petitioner also notes, the ’516 “[S]pecification provides that the IP address looked up ‘need not be *the actual* address of the destination computer.’” Pet. Reply 8 (quoting Ex. 1001, 40:51–52).

Petitioner establishes by a preponderance of evidence that Beser discloses or at least suggests intercepting a request to look up IP addresses to assign them either as part of a normal DNS function where no security would be desired for a device in a local private network, and also, using the same or similar DNS functionality and its tunneling application to determine if a device in a corporate or other private network would be available for tunneling (with end-to-end encryption), in order to enhance security in a corporate or private network. *See* Ex. 1003 ¶¶ 159–163; Ex. 1007, 2:1–17 (security desired, encryption may require additional power), 3:4–9 (security desired), 3:60–4:24 (private networks 20), 8:1–9:62 (unique identifier, distinctive bits for tunneling), 11:32–36, 10:37–41 (domain name as unique identifier), 11:33–58 (DNS or other known data structures), Fig. 1 (system). Even if Beser only teaches or suggests the latter functionality, Petitioner

¹⁷ Any one of the three alternatives relied upon by Petitioner satisfies the challenged claims.

shows by a preponderance of evidence that Beser satisfies the intercept and determine clauses of the challenged claims. *See* Pet. 17–22 (discussing Beser), 37–42 (addressing claim limitations); Pet. Reply 5–8 (responding to Patent Owner’s arguments).

b. Reason to Combine and Encryption

Patent Owner argues that Beser and RFC 2401 would not have been combined as asserted by Petitioner to arrive at an “encrypted communication link” as recited in challenged claims 1 and 15. PO Resp. 21–27 (“Petitioner relies on RFC 2401 for the teaching that data sent between two devices in a tunnel should be encrypted.”). As noted above, claims 2 and 16 require encryption of at least one of audio data and video data respectively during an audio-video service and a video service. Claims 12 and 26 require “end-to-end” encryption between the first and second network devices.

According to Patent Owner, Beser teaches away from using encryption as claimed in claims 1, 2, 12, 15, 16, and 26. PO Resp. 24, 27–28. Patent Owner contends Beser “explains that streaming data flows, such as multimedia and Voice-over-Internet-Protocol (‘VoIP’), ‘require a great deal of computing power to encrypt or decrypt the IP packets on the fly’” and “[t]he strain of such computations ‘may result in jitter, delay, or the loss of some packets.’” *Id.* at 22 (quoting Ex. 1007, 1:62–65; citing Ex. 2018 ¶ 54). Patent Owner also contends that Beser’s method “hide[s] addresses [of sources and targets] within the payload of tunneled messages to increase communication security without increasing computational burden.” *Id.* at 23 (citing Ex. 1007, 2:36–40, 2:43–3:14, 9:49–51; Ex. 2018 ¶ 57).

According further to Patent Owner, the Institution Decision does not characterize Beser’s teachings regarding computer power and encryption correctly:

[t]he Institution Decision asserts that *Beser* “recognizes that encryption may cause challenges, [but] also suggests that any challenges may be overcome by providing more computer power and/or less quality.” (Inst. Dec. at 25.) This position reflects a misunderstanding of *Beser*. If adding computing power to every computational problem was a solution, there would have been no need for Beser’s tunneling solution.

Id. at 22 (citing Ex. 2018 ¶ 55). Patent Owner also contends that “*Beser* dismisses the idea of encryption entirely, noting that the ‘expense of added computer power might also dampen the customer’s desire to invest in VoIP equipment’ at all.” *Id.* at 23 (quoting Ex. 1007, 1:65–67; citing Ex. 2018 ¶ 55).

Patent Owner also contends “*Beser* notes the *problems* with allocating more computing power to encryption, such as ‘jitter, delay, or the loss of some packets.’” *Id.* at 22 (quoting Ex. 1007, 1:60–65). Patent Owner also contends Beser only teaches using encryption for hiding addresses and cites IPsec as prior art—part of the “Background of the Invention.” *Id.* at 24 (citing Ex. 1007, 1:54–67; Ex. 2018 ¶ 59). According to Patent Owner, Beser “does not use encryption in transmitting data over [its] established tunnel and, in fact teaches away from doing so.” *Id.*

Patent Owner further contends as follows:

The Institution Decision asserts that “[t]his argument [by Patent Owner] does not address the reason for using data encryption in Beser’s system—to increase data security.” (Inst. Dec. at 27.) But the purpose of the encryption in Beser is simply to hide address information on the public network prior

to Beser's tunnel establishment; once the tunnel is created, the originating and terminating device information is hidden and encryption would not only be redundant, it would contravene Beser's express objective of increasing security without increasing computational burden. (Ex. 2018 at ¶ 60.) So Beser does not use encryption in transmitting data over the established tunnel and, in fact, teaches away from using encryption in transmitting data.

Id. at 25.

Patent Owner's arguments are not persuasive. Patent Owner simply does not address Petitioner's argument and showing, as further outlined in the Institution Decision (*see* citation by Patent Owner *supra*), that Beser's system serves to protect addresses, without disturbing the well-known prior art solution for protecting data (i.e., encryption). Beser does provide a low power solution for hiding *addresses* without encryption as Patent Owner generally contends, but Beser, in light of RFC 2401, also suggests using the solution of hiding addresses with relatively higher power encryption in order to protect the packet *data*. *See* Reply Br. 11–12 (arguing and citing supporting evidence, including by Dr. Monroe that increasing power solves encryption problems (Ex. 1055, 206:20–208:6; Ex. 1003, ¶¶ 224–25); Ex. 1003 ¶¶ 224–25 (persons of ordinary skill would have recognized that adding more computing power or using a lower resolution media stream solves data encryption issues addressed in Beser)). Contrary to Patent Owner's arguments, which mischaracterize Beser, Beser teaches an “increased *strain on computer power* [i.e., as opposed to *increased computer power*] may result in jitter, delay, or the loss of some packets.” Ex. 1007, 1:63–65 (emphasis added).

In other words, Beser teaches the opposite of what Patent Owner states. Increasing computer power *solves*, rather than *creates*, the problems of jitter, delay, or the loss of packets. *See id.*; Ex. 1003 ¶¶ 223–24. The fact that Beser notes that adding power increases cost supports this finding and does not support Patent Owner’s allegation that Beser teaches away from encryption. *See* Ex. 1007, 1:65–67 (increased cost for computer power may “dampen the customer’s desire to invest in VoIP equipment”). “That a given combination would not be made by businessmen for economic reasons does not mean that persons skilled in the art would not make the combination because of some technological incompatibility. Only the latter fact would be relevant.” *In re Farrenkopf*, 713 F.2d 714, 718 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. United States*, 702 F.2d 1005, 1013 (Fed. Cir. 1983)); *see also* *Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1328 (Fed. Cir. 2008) (“market-force skepticism also lacks the requisite nexus to the claimed invention” and therefore does not show non-obviousness), *abrogation on other grounds recognized by Travel Sentry, Inc. v. Tropp*, 877 F.3d 1370 (Fed. Cir. 2017).

Beser discusses two prior art security issues, the same two issues the ’516 patent discusses as well known—anonymity (solved by hiding addresses in packets) and data security (solved by encryption). *See* PO Resp. 23 (discussing anonymity), 23–24 (characterizing Beser as teaching “a tunneling association to hide addresses within the payload of the tunneled message”); *supra* Section I.D (discussing “BACKGROUND OF THE INVENTION”): “[T]wo security issues may be called data security and anonymity, respectively.” (quoting Ex. 1001, 1:57–59); Ex. 1007, 1:54–56 (packet data security via encryption), 2:36–40 (hiding addresses using

private addresses). Beser’s method of hiding *addresses* simply does not teach away from dealing with the *other* security issue involving data.

In other words, Beser teaches a method to hide addresses useful in systems that either protect data using encryption or do not protect data using encryption. *See* Ex. 1007, 2:36–40. Beser does not teach an alternative to encryption for *data* security, rather, Beser teaches a method for providing *address* anonymity. *See id.* at Abs.; Reply Br. 8–10; PO Resp. 23 (arguing Beser’s system “hid[es] the identities of . . . network devices”). And even if Beser does teach an alternative to *data* encryption (it does not), “[a] reference that ‘merely expresses a general preference for an alternative invention but does not criticize, discredit, or otherwise discourage investigation into’ the claimed invention does not teach away.” *Meiresonne v. Google, Inc.*, 849 F.3d 1379, 1382, 1383 (Fed. Cir. 2017) (quoting *Galderma Labs., L.P. v. Tolmar, Inc.*, 737 F.3d 731, 738 (Fed. Cir. 2013) (Miersonne reasons the prior art “does not say or imply that text descriptions are ‘unreliable,’ ‘misleading,’ ‘wrong, or ‘inaccurate,’ which might lead one of ordinary skill in the art to discard text descriptions completely.”)). The “mere disclosure of alternative designs does not teach away.” *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004).

Although Beser recognizes that the use of data encryption may cause (power) challenges, as noted above, Beser also suggests that these challenges may be overcome by providing more computer power and/or less quality (fewer packets per a normal data stream). *See* Ex. 1007, 1:54–67; Pet. 29–32; Pet Reply 11–12 (citing Ex. 1003 ¶¶ 224–25). As Petitioner notes, Dr. Monroe concedes the point. *See* Pet. Reply 11–12 (citing Ex. 1055, 206:20–208:6, 211:16–212:2). As noted, Petitioner also relies on Dr.

Tamassia's persuasive testimony. Pet. Reply 11 (citing Ex. 1003 ¶¶ 224–25 and summarizing Dr. Tamassia's testimony as follows: “adding more computing power or using a lower resolution media stream could solve any issues”).

Beser plainly corroborates what both experts agree upon: IP packets “may need to be encrypted,” but “[o]nce again, *due to computer power limitations*, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets.” Ex. 1007, 2:12–17 (emphasis added). That encrypting high data rate packets “may be inappropriate” “due to computer power limitations” simply informs skilled artisans that encryption would have been advantageous for protecting lower data rate packets with less power and higher data rate packets with more power. See Ex. 1003 ¶¶ 224–225 (citing and discussing Beser as suggesting “simply using more powerful equipment” to handle multimedia or simply using “lower resolution video” without adding any power).

Patent Owner's arguments conflate the two security issues (anonymity and data security) that the '516 patent and *Cisco* (*supra* note 5) show clearly consist of two distinct (and well-known) aspects of communications security. See Ex. 1001, 1:38–40 (“A tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet.”); *Cisco*, 767 F.3d at 1317–18 (“Security in this context refers to protection of data itself, to preserve the secrecy of its contents, while anonymity refers to preventing an eavesdropper from discovering the identity of a participating terminal.” (discussing background art as disclosed in a related VirnetX patent)); *supra* note 5 (discussing *Cisco*).

As Patent Owner notes, Beser provides a solution to hiding addresses, and in one embodiment, uses encryption to hide public addresses during the tunnel set up process. PO Resp. 21–22, 24 (“Beser explains that during the set-up of a tunneling association, encryption may be used to hide the identity of network device 16 (e.g., the router).” (citing Ex. 1007, 18:2–5)). But contrary to Patent Owner’s arguments, the reason to add encryption to protect *data* in the tunnel still exists even in the tunnel process for hiding *addresses*, and encryption of data was notoriously well known at the time of the invention, as RFC 2401, Beser, and the ’516 patent all make clear. See Ex. 1001, 1:60–66 (“Data security is usually tackled using some form of data encryption. . . . Many encryption methods are known.”);¹⁸ Ex. 1008, 7 (“one can create a single encrypted tunnel to carry all the traffic between two security gateways”); Ex. 1007, 2:23–24 (discussed next).

Beser makes a desire for encryption clear by specifically characterizing some prior art systems as creating “*security problems by preventing certain types of encryption from being used.*” Ex. 1007, 2:23–24 (emphasis added). In other words, Beser does not discourage encrypting data to make it secure; rather, Beser criticizes systems that cannot employ encryption of data if desired or required, and provides a solution for providing anonymity by using a tunnel technique with or without encryption of data. See Ex. 1007, 2:36–40 (describing “hiding the identities” in tunnels as an object of the invention). Patent Owner’s argument that Beser’s address hiding method avoids computationally expensive prior art network address

¹⁸ See *In re Baxter Travenol Labs*, 952 F.2d 388, 390 (Fed. Cir. 1991) (holding extrinsic evidence, including admissions, may be used to explain what a reference discloses in a reexamination proceeding).

translation methods similarly has nothing to do with providing data security, as Petitioner argues. *See* PO Resp. 23–24; Pet. Reply 13 (“Beser’s IP tunnel hides the identities of communicating devices, but in contrast to prior art IP tunnels, which were computationally expensive ([Ex. 1007], 2:33–35), Beser’s IP tunnel has a low ‘computational burden,’” (*id.*, 3:4–9). Because of its low computational burden, Beser’s method is flexible and can be combined with other security techniques.”)

As Petitioner persuasively adds in response to Patent Owner’s arguments that Beser describes encryption as allowing hackers to intercept media flow (PO Resp. 22), Beser’s address hiding tunnel method, combined with known IPSec flexible encryption methods (as taught by Beser and RFC 2401), obviously would have aided in preventing the use of any accumulated packets by hiding addresses and data. *See* Pet. Reply 13 (citing Ex. 1003 ¶¶ 223, 228; Ex. 1007, 1:56–58, 2:36–40, 2:43–45, 3:4–9, 4:55–5:2). Beser explains encryption can be employed in a prior art tunneling/VPN application (“encapsulating the IP packet to be tunneled within the payload field for another packet”) in order to “hide the source IP address” and “thwart[] the hacker.” Ex. 1007, 2:6–14. Beser then explains “[o]nce again, due to computer power limitations, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets.” *Id.* at 2:15–17 (emphasis added). This passage shows that using encryption with sufficient power thwarts the hacker and hides the data—especially with Beser’s tunneling method, which presents a lower computational burden than prior art packet tunneling methods but hides addresses needed by hackers. *See id.* at 1:54–2:17.

As noted above, Petitioner addresses the related “end-to-end” encryption limitations in dependent claims 12 and 26 by relying partly on its showing with respect to independent challenged claims 1 and 16. Petitioner persuasively explains that

Beser’s IP tunnel would have provided anonymity for communications, and IPsec, as shown in Case 3 of RFC 2401, would have provided end-to-end encryption. Ex. 1008, 25; Ex. 1003, ¶¶229–33. . . . [T]he skilled person would have recognized such encryption was conventional, and any practical issues with certain data transmission scenarios could be overcome by providing more computing power, changing the resolution of any multimedia data transmitted, or changing the granularity of encryption. Ex. 1003, ¶¶208, 219–25.

Pet. 54–55.

Other than relying on its teaching away arguments discussed above, Patent Owner does not dispute Petitioner’s showing regarding claims 12 and 26. *See* PO Resp. 28–29.

Petitioner reasonably shows such an extra layer of security (i.e., encryption) behind the physical security of a corporate firewall or private network would have been obvious in order to ensure data security. *See* Pet. 31–35; Ex. 1003 ¶¶ 229–230 (providing credible testimony that Beser’s reference to the IPSec protocol, and the teachings in RFC 2401 related to that protocol, suggest encryption “between a first and second network device or between the two end devices”), ¶¶ 228–34 (testifying the combination suggests end-to-end encryption to enhance security over the whole path); Reply Br. 10–14. Petitioner’s point is persuasive, because in the event a hacker or other nefarious listener breaches Beser’s private networks 20, an extra layer of security via encryption (in addition to physical security behind the corporate private network) would protect the data. *See* Ex. 1003 ¶¶ 229–

31 (testifying that RFC 2401 discloses end-to-end and tunnel encryption, describing a “Case 3” configuration with edge routers connecting private networks over a public network that mimics Beser’s system) (citing Ex. 1008, 25), ¶¶ 234–37 (describing how the combination suggests a configuration for end-to-end encryption); Ex. 1007, Fig. 1 (depicting private network 20 on the requesting end); Ex. 1007, 11:62–64 (“Private IP 58 addresses are addresses that are reserved for use in private networks that are isolated from a public network such as the Internet.”).¹⁹

In addition, in making its teaching away arguments with respect to the challenged claims, Patent Owner cites to alleged problems with teachings in Beser related to encryption of “streaming data flows, such as multimedia and Voice-over-Internet-Protocol (‘VoIP’),” which “require a great deal of computing power to encrypt or decrypt the IP packets on the fly.” PO Resp. 22 (citing Ex. 1007, 1:62–63). This argument is not commensurate in scope with the claims, because none of the claims requires encryption of streaming multimedia flows and none of the claims specifies any bandwidth or data rate for multimedia. For example, claims 2 and 16, as noted above, require encryption of “*at least one of encrypted video data and audio data*” (emphasis added). In any event, as Petitioner shows, “changing the resolution of any multimedia data transmitted,” adding power, or changing

¹⁹ In contrast to claims 12 and 16, independent challenged claims 1 and 15 do not require end-to-end encryption. *Cisco* refers to “physical security” on private networks that do not necessarily have encryption and notes that VirnetX’s patents describe encryption on public networks as a way to tackle data security. *Cisco*, 767 F.3d at 1322. *Cisco* also notes “the [related ’151] patent consistently differentiates between ‘security’ and ‘encryption.’ Both the claims and the specification of the ’151 patent make clear that encryption is a narrower, more specific requirement than security.” *See id.* at 1323.

the encryption granularity, solves any problems, and those problems readily would have been overcome by a person of ordinary skill given the relatively lower data rates involved with encrypting audio data. *See, e.g.*, Pet. 54–55 (citing Ex. 1003 ¶¶ 208, 219–25). As noted in the previous section, Dr. Tamassia credibly testifies that skilled artisans easily could have adjusted data rates or provided more computer power to provide a desired level of encryption. *See* Ex. 1003 ¶¶ 223–24. In addition, as Petitioner argues, “Patent Owner’s expert admit[ted] that a more powerful computer or lower recording fidelity would resolve any problems.” Pet. 48 (citing Ex. 1055, 206:20–208:6).

In summary, Petitioner articulates a persuasive rationale showing a person of ordinary skill would have found it obvious to combine the teachings of RFC 2401 with Beser to encrypt data in order to enhance security in a tunnel and into private networks, based on a determination that a requested target device would have been available for secure communications. Petitioner also sets forth a persuasive rationale showing that Beser’s combined system includes or suggests using a typical DNS functionality or similar look up techniques to determine that a requested target device is available for secure communications by, among other things, associating an identifier of the target device with a private and/or public IP address for it.

Based on the foregoing discussion and a review of the record, we determine that Petitioner demonstrates by a preponderance of evidence that the combination of Beser and RFC 2401 would have rendered claims 1, 2, 12, 15, 16, and 26 obvious.

4. Claims 3, 4, 17, and 18

Claims 3 and 17 depend respectively from claims 1 and 15 and recite “wherein the secure communications service includes [or is] a messaging service.” Ex. 1001, 56:37–38, 57:32–33. Claims 4 and 18 respectively depend from claims 3 and 17, and further recite that “wherein the messaging service includes [or is] an e-mail service.” Ex. 1001, 56:39–40, 57:34–35.

Petitioner contends that using e-mail in Beser’s system would have been obvious “because it already transmits other types of communication data such as audio and video.” Pet. 49–50. Petitioner points out that “Beser explains that the unique identifier included in a request can be an email address.” *Id.* (citing Ex. 1007, 10:55–11:5; Ex. 1003 ¶ 164). Petitioner also contends that “Beser . . . explains that a variety of originating and terminating end devices are compatible with its methods, including telephony and multimedia devices, and that ‘the ends of the data flow may be other types of network devices.’” *Id.* (quoting Ex. 1007, 4:43–54; citing Ex. 1003 ¶¶ 138–42). Petitioner cites another prior art document as evidence to show that “[t]ransmitting email over a secure communication link or VPN was well-known at the time of the invention.” *Id.* (citing Ex. 1052, Figs. 5A, 5B, 12:11–23; Ex. 1003 ¶ 164). In the Institution Decision, we characterized Petitioner’s showing, in part, as a simple substitution of one type of data for another. *See* Inst. Dec. 29–30. A person of ordinary skill would have been motivated to employ e-mail in Beser’s modified system for the same reason she would have employed any type of data—to ensure the security of the data and anonymity of the users. *See id.* (characterizing Petitioner’s rationale as tracking its rationale with respect to claims 1 and 15).

Patent Owner contends that Petitioner's showing is insufficient because it fails to show "why" or "how" one would use an email service in Beser's tunneling service. PO Resp. 30. Patent Owner also contends "a 'simple substitution' obviousness rationale requires, *inter alia*, a showing that the results of the substitution would have been predictable." *Id.* at 31 (citing *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007)). Patent Owner also contends that "*Beser* only suggests using an e-mail address for things *other than* an e-mail." *Id.* at 32 (citing Ex. 1007, 10:55–57).

Patent Owner's arguments do not undermine Petitioner's showing. Patent Owner does not contend that sending e-mail on an encrypted tunnel would have been unpredictable or that a skilled artisan would have been unable to implement an email service in Beser's encrypted system as modified by RFC-2401. *See id.* at 30–31. Contrary to Patent Owner's arguments, Petitioner presents, as summarized above, a persuasive rationale for a simple substitution of sending one type of data for another in a known application in order to make similar application data secure, thereby providing another way to communicate securely. As Dr. Tamassia testifies, Beser and RFC 2401 each suggests, or collectively suggest, encrypting multimedia, telephony, audio, video, and all types of data, including via communication between "personal computers running multimedia applications." *See* Ex. 1003 ¶¶ 141 (quoting Ex. 1007, 4:47–49), 164 (discussing email).

The record, including the prior art and testimony by both experts, shows an artisan of ordinary skill easily had the capability to include email in Beser's modified system, and would have for the reasons noted. *See* note

9 *supra*. Patent Owner agrees that a person of ordinary skill at least has the qualifications Petitioner advances. See Prelim. Resp. 2–4.

Accordingly, the record shows transmitting encrypted e-mail data would have been predictable and easily within the grasp of an ordinary artisan for the simple purpose of providing another type of secure data communication, as the references fairly suggest in disclosing IPsec. See Ex. 1003 ¶ 164 (“Email is a type of data like audio and video, and transmitting it via Beser’s secure IP tunnel would protect it in the same way.”); Pet. 49–50 (citing Ex. 1003 ¶ 164); Ex. 1008, 4–8 (IPsec encryption); *supra* Section II.D.1–3 (discussing IPsec teachings in each of Beser and RFC 2401); Pet. 33 (similar IPsec discussion).

Petitioner also establishes persuasively that Beser further discloses or suggests using e-mail services by disclosing “that the unique identifier is an electronic mail address.” Ex. 1007, 10:55–11:5; Pet. 49 (also citing Ex. 1052, Fig. 5A–B (stating the reference “show[s] a messaging server being accessed via VPN and IPsec”), 12:11–23 (stating it “describ[es] messaging servers providing email applications”)). As Petitioner contends, Exhibit 1052 constitutes further evidence of ordinary skill in the art concerning the known use of an e-mail application and/or data on a VPN. See Pet. 49–50 (citing Ex. 1003 ¶¶ 138–142, 164; Ex. 1052).

Based on the foregoing discussion, Petitioner demonstrates by a preponderance of evidence that claims 3, 4, 17, and 18 would have been obvious based on the combination of Beser and RFC 2401.

5. Claims 5–9, 11, 13, 14, 19–23, and 25, 27, and 28

Relying partially on the Tamassia Declaration, Petitioner presents persuasive articulated rationale and detailed mappings of claim elements, in

its showing that the combination of Beser and RFC 2401 would have rendered obvious challenged dependent claims 5–9, 11, 13, 14, 19–23, 25, 27, and 28, which ultimately depend from one of independent claims 1 and 16. *See* Pet. 50–57. As Petitioner shows, by way of summary, these claims simply add known subject matter elements involving communication services and/or present limitations that overlap limitations recited in claims 1 and 16 above. *See id.*

For example, dependent claims 5–8 and 19–21 recite the following known limitations: “telephony service” (claims 5 and 19) (Ex. 1001, 56:42, 58:2), a “mobile device” (claims 8 and 22) (Ex. 1001, 56:50–51, 58:10–11), telephony service modulation (claims 6 and 20) (Ex. 1001, 56:43–44, 58:3–4), and FDM, TDM, or CDMA modulation (claims 7 and 21) (Ex. 1001, 56:45–48, 58:5–8). *See id.* at 50–57 (addressing the limitations persuasively, citing *inter alia*, Beser’s VoIP devices, personal computers, facsimile and audio applications, cable modem, portable device, and known cable modem modulation types, and citing Ex. 1003 ¶¶ 79, 138–44).

Claims 9 and 23 each recite “wherein the identifier associated with the second network device is [associated with] a domain name.” Ex. 1001, 56:52–54, 58:12–13. Claims 11 and 25 recite “wherein the determination that the second network device is available for the [a] secure communications service is a function of [the result] of a domain name lookup.” Ex. 1001, 56:61–64, 58:21–23. Claim 13 recites “one or more servers are configured to intercept the request by receiving the request to determine whether the second network device is available for a secure communications service.” Ex. 1001, 57:1–4. Claim 27 recites a similar limitation but more generally does not require “one or more servers.” Ex.

1001, 58:27–30. Claim 14 recites “wherein the one or more servers configured to intercept the request are separate from the first network device.” Ex. 1001, 57:5–7. Claim 28 recites a similar limitation but more generally requires “another network device” instead of “one or more servers.” Ex. 1001, 58:31–33.

Similar to its showing with respect to claims 1 and 15, Petitioner persuasively relies on Beser’s unique identifier as a part of a request that the trusted-third-party network device, which includes a DNS server, uses to determine if terminating device 26 is available for the secure service. See Pet. 52–57 (citing *inter alia*, its earlier showing regarding claims 1 and 15, and citing Ex. 1007, Figs. 1, 6, 8:1–3, 8:21–47, 8:58–[6]0, 9:6–11, 9:26–30, 9:46–49, 11:30–36, 11:45–12:19; Ex. 1003 ¶¶ 130, 162, 168–69, 174–78, 182, 208, 219–25, 227, 229–33; Ex. 1008, 25; Ex. 1001, 40:34–40 (comparing the determination made in the ’516 patent)).

Petitioner shows separately and persuasively that Beser and RFC 2401 would have rendered the subject matter of these dependent claims obvious. See Pet. 52–57 (addressing limitations related to a domain look up, a separate intercepting server, and receiving a request to make the recited determination). Rather than attempting to repeat Petitioner’s persuasive showing, including supporting citations to the record, we incorporate and adopt it as our own findings and conclusions and refer to it generally in summary as noted herein.

In response, Patent Owner relies on its arguments presented with respect to claims 1 and 15 and does not otherwise particularly dispute Petitioner’s persuasive showing. See PO Resp. 32–33. We informed Patent Owner “that any arguments for patentability not raised in the Response may

be deemed waived.” Paper 10, 3 (emphasis deleted). Apart from its arguments with respect to claims 1 and 15, including the prior art status of RFC 2401 (addressed above), Patent Owner has waived arguments directed particularly to these challenged dependent claims, notwithstanding that Petitioner carries the burden of showing unpatentability.

Based on the record as summarized above, Petitioner shows by a preponderance of evidence that claims 5–9, 11, 13, 14, 19–23, and 25, 27, and 28 would have been obvious based on the combination of Beser and RFC 2401.

E. Collateral Estoppel

Petitioner contends collateral estoppel prevents Patent Owner from re-litigating identical issues involved in seven cases that the Federal Circuit affirmed. Pet. Reply 2–3 (citing Paper 8). In Paper 8, Petitioner noted “the Federal Circuit affirmed the final written decisions issued in IPR2014-00237 and IPR2014-00238 finding claims 1–11, 14–25, and 28–30 of U.S. Patent No. 8,504,697 unpatentable.” Paper 8, 1.

Patent Owner argues that 37 C.F.R. § 42.73(d)(3) does not act as a prohibition against arguments to defend a patent in an IPR proceeding and the conditions for common law estoppel are not met. See PO Resp. 11–13. Our reviewing court recently held that “prior [IPR] decisions, having been affirmed by our court, are binding in this proceeding, as a matter of collateral estoppel, and the [parties] could hardly argue otherwise.” *Maxlinear, Inc. v. CF Crespe*, 888 F.3d 1373, 1376 (Fed. Cir. 2018).

Similar to the situation outlined by the court in *Maxlinear*, the ’237 FWD and the ’238 FWD each constitute a final judgment of claims, but unlike the situation in *Maxlinear*, 888 F.3d at 1376–77, the instant

proceeding involves a different patent and different claims than the patent and claims determined to be invalid in the '237 FWD and the '238 FWD. *See supra* note 1, Section 1B (citing *VirnetX Inc. v. Apple Inc.*, 665 F. App'x 880 (Fed. Cir. 2016) (affirming the '237 FWD and the '238 FWD holding unpatentable claims 1–11, 14–25, and 28–30 of related U.S. Patent No. 8,504,697 (the “'697 patent”)); *Maxlinear*, 888 F.3d at 1376–77 (“The preclusive effect of the prior adjudications, and subsequent affirmations, has finally resolved the issue of the unpatentability of independent claims 1 and 17 and dependent claim 20 in this proceeding.”).

The parties have not provided input as to whether the '697 patent claims held invalid by our reviewing court embrace the same material scope as the '516 patent claims challenged here. *See Ohio Willow Wood Co. v. Alps South, LLC*, 735 F.3d 1333, 1342 (Fed. Cir. 2013) (“Our precedent does not limit collateral estoppel to patent claims that are identical.”); *Bourns, Inc. v. U.S.*, 537 F.2d 486, 492 (Ct. Cl. 1976) (finding “collateral estoppel [is] applicable to unadjudicated claims where it was shown that the adjudicated and unadjudicated claims presented identical issues”); *S. Corp v. U.S.*, 690 F.2d 1368, 1369 (Fed. Cir. 1982) (en banc) (holding decisions of the Court of Claims are binding precedent).

Under these circumstances, because we independently determine herein that Petitioner shows the challenged claims in the '516 patent would have been obvious, it is unnecessary to reach the collateral estoppel issue.

III. PATENT OWNER’S MOTION TO EXCLUDE

Patent Owner seeks to exclude Exhibits 1008, 1032–36, 1038–40, 1045–48, 1053, 1060, 1063–65, and 1072–74. Paper 21 (“Motion” or “Mot.”). Petitioner opposes the Motion. Paper 24 (“Opposition” or

“Opp.”). Patent Owner replies to the Opposition. Paper 26 (“Reply to Opp.”).

As movant, Patent Owner bears the burden of proof to establish entitlement to the requested relief. *See* 37 C.F.R. § 42.20(c). For the reasons stated below, Patent Owner’s Motion is *dismissed* as *moot* in part and *denied* in part.

1. Exhibits 1008 and 1036

Patent Owner moves to exclude Exhibit 1008 as inadmissible hearsay. Patent Owner contends Petitioner relies on the date, “November 1998,” on the cover of Exhibit 1008 for the truth of the purported matter asserted. Mot. 2. Petitioner asserts “RFC 2401 (Ex. 1008) was published by the Internet Engineering Task Force (IETF) in **November 1998.**” Pet. 23 (citing Ex. 1008, 1; Ex. 1003 ¶¶ 124–25).

Patent Owner similarly moves to exclude Exhibit 1036. Exhibit 1036, RFC 2026, states it reflects “generally accepted practices” for RFC documents and states any interested person can obtain RFCs “from a number of Internet hosts.” Ex. 1036, 4, 6. Patent Owner generally argues “Petitioner relies on Exhibits 1032–1036 and 1074 for the truth of the purported matter asserted,” “no hearsay exception applies,” and the Exhibits “should be excluded.” Mot. 2.

Petitioner replies that Exhibit 1036 bears a publication date of October 1996 and “meet[s] the age requirements and authentication criteria to constitute ancient documents” under Fed. R. Evid. 803(16) and 901(b)(8). Opp. 6. Petitioner also contends “[a]ll of the [RFC] exhibits are available to download on the RFC Editor website, which is a place they would likely be, if authentic.” *Id.* at 7 & n.1 (“Available at www.rfc-editor.org; see

<http://ietf.org/rfc.html> (‘When in doubt, the RFC Editor site is the authoritative source page [for RFCs].’’)).

We adopt Petitioner’s showing that Exhibit 1036 qualifies as an ancient document and is “what [it] appear[s] to be.” See Opp. 6–7. Patent Owner replies a “purported date on a document is not conclusive to prove it is [an] ancient document.” Reply to Opp. 3 (citing *In re McGary’s Estate*, 258 P.2d 770 (Colo. 1953)). Patent Owner also contends that Petitioner’s “procedure may provide an authentic copy as it is available today, but cannot retroactively show that Apple’s PDF is an authentic copy of the version that was available on the dates stamped on the Apple’s PDF (assuming any version was actually available at that time).” *Id.*

Regarding the latter argument, the website relied upon by Petitioner lists RFC 2036 with the same date appearing on Exhibit 1036 (i.e., “October 1996”). See https://www.rfc-editor.org/search/rfc_search_detail.php?rfc=RFC+2036&pubstatus%5B%5D=Any&pub_date_type=any.” The website also show RFC 2401 bears the “November 1998” date. Regarding the former argument about authenticity, Petitioner does not rely solely on the date, and contends, *inter alia*, as follows:

Dr. Tamassia explains that RFCs are the official publication channel for Internet standards, with the publication process described in RFC 2026 (Ex. 1036), Ex. 100[3] at ¶¶ 1[1]6–[12]3, which 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. 100[3] at ¶1[1]7. Dr. Tamassia testifies from his personal knowledge that RFCs list their publication date in the top corner of the first page (Ex. 100[3] at ¶1[20])

Opp. 10.²⁰ In addition, Petitioner notes persuasively that the PTO and other tribunals have recognized RFC publications as authoritative, well-known Internet publications:

RFC documents, such as those at issue here, are perhaps one of the most well-known sources of technical information in the art at issue in this proceeding. *See, e.g.*, Control No. 95/001,789, Action Closing Prosecution (Sept. 9, 2012) (“Regarding the RFC(s), these publications are among the most authoritative publications for Internet systems and protocols.”); *PGMedia, Inc. v. Network Sols., Inc.*, 51 F. Supp. 2d 389, 406 (S.D.N.Y. 1999) (“[M]ore than 2000 RFC’s which have been written and circulated” as part of development of the Internet).

Opp. 12.

The dates on Exhibit 1008 and Exhibit 1036 do not constitute hearsay, because they are not assertions that IETF published RFC 2401 or RFC 2026 on a certain date. *See Seabery N. Am. Inc. v. Lincoln Glob., Inc.*, Case IPR2016-00840, slip. op. at 5–6 (PTAB Oct. 2, 2017) (Paper 60, 5–6 & n.2) (reasoning dates do not constitute hearsay because they are not assertions) (quoted below).

With further respect to Exhibit 1008, RFC 2401, in addition to a Copyright Notice” of “1998,” title (“Security Architecture for the Internet Protocol”), and table of contents, it bears the following date and other identifying information on the first page:

Network Working Group
Request for Comments: 2401
Obsoletes: 1825
Category: Standards Track

S. Kent
BBN Corp
R. Atkinson
@Home Network

²⁰ Petitioner incorrectly cites to Ex. 1005 and paragraphs therein. This constitutes harmless error as Dr. Tamassia testifies in the same manner at the noted paragraphs in Exhibit 1003.

November 1998

Ex. 1008, 1.

Similar information appears on the first page of Exhibit 1036, RFC 2026 (date “October 1996”). Ex. 1036, 1. All of this information serves to identify and authenticate each document.

Regarding hearsay, in *Seabery*, the Board persuasively reasoned as follows:

We agree with the view [of other PTAB panels] that the dates [of publications] are not hearsay because they are not assertions. . . . We are supported in this by cases such as *United States v. Snow*, 517 F.2d 441, 445 (9th Cir. 1975), where a red tape bearing the defendant’s name affixed to a briefcase where a gun was found was admitted as circumstantial evidence that the defendant possessed the weapon. To the same effect are *United States v. Koch*, 625 F.3d 470, 480 (8th Cir. 2010) (computer flash drive with manufacturer’s label “China” not inadmissible hearsay to prove place of manufacture); and *United States v. Bowling*, 32 F.3d 326, 328 (8th Cir. 1994) (manufacturer’s name stamped on firearm not hearsay). We are persuaded by these cases that dates appearing in Exhibit 1003, like the examples in those cases, are circumstantial evidence of publication and not assertions that publication occurred on a date certain. We, therefore, overrule the objection and admit the dates for this purpose.

See IPR2016-00840, Paper 60, 5–6 & n.2 (alternatively relying on the residual exception to hearsay). For the same reasons enunciated in *Seabery*, Patent Owner does not establish that the dates (October, 1996; November 1998) constitute hearsay, because these dates are not assertions of a publication. Rather, they constitute evidence helping to identify the documents and include circumstantial evidence that IEFT made the RFC 2401 and RFC 2026 publications available respectively in November 1998

and October 1996. The following notices, “Copyright Notice” and “Copyright (C) The Internet Society (1998). All Rights Reserved,” on the RFC 2401 document provides further corroboration and circumstantial evidence of the date and authenticity. *See* Ex. 1008, 1.

Petitioner also shows, in the alternative, that Exhibit 1008 satisfies Fed. R. Evid. 807(a) under the residual exception to hearsay. *Opp.* 7–14. We adopt Petitioner’s showing as persuasive, albeit, without relying on Exhibits 1060, 1063, and 1072. *See Opp.* 8–14 (addressing factors under Fed. R. Evid. 807(a, b)).

2. Exhibits 1060, 1063–65, and 1072

Patent Owner moves to exclude Exhibits 1060, 1063–65, and 1072 as inadmissible hearsay. *Mot.* 3–7. Exhibit 1060, a declaration originally submitted in litigation before the International Trade Commission, contains testimony from Sandy Ginoza, Director of the RFC Publisher, and representative of the Internet Engineering Task Force (IETF), in support of Petitioner’s contention that RFC 2401 qualifies as a printed publication as of November 1998. *See* Ex. 1060 ¶¶ 1–4; *Mot.* 3. Exhibit 1063 is a “transcript of Ms. Ginoza’s February 8, 2013 deposition that was taken as part of the ITC action.” *Mot.* 3 (citing *Pet.* 24–25). Exhibits 1064 and 1065, both magazine articles dated 1999, describe how to obtain RFC publications. *See* *Motion* 3. Exhibit 1072, a book, entitled *IMPLEMENTING IPSEC* (1999), includes a copy of RFC 2401 in its appendix. *See Opp.* 10. Because we need not rely Exhibits 1060, 1063, and 1072 to decide the issue of whether RFC 2401 qualifies as a printed publication, we dismiss the motion as to these Exhibits as moot.

With respect to Exhibits 1064 and 1065, Patent Owner contends “the purported dates on these references as being true representations of the publication dates constitutes hearsay.” Motion 4. Patent Owner does not contest the underlying statements in the articles as relied upon by Petitioner regarding the availability of RFC 2401. *See* Opp. 3 (“Petitioner relied on Exhibits 1064 and 1065 to show that an interested ordinary artisan, exercising reasonable diligence, would have known how to locate RFC 2401.”); Pet. Reply 18 n. 2 (“These articles also show that the skilled person would have known that RFCs such as RFC 2401 could be downloaded from the IETF’s website.”); Opp. 9–10 (noting the trade magazine articles mention the same website for finding RFC documents, including RFC 2401).

Exhibits 1064 and 1065 support Petitioner’s showing. The articles show that an artisan of ordinary skill would have understood from the statements made therein that RFC 2401 would have been available, including on a specific website. For example, Exhibit 1064 implores artisans of ordinary skill to “check out RFC 2411 (the document roadmap) and RFC 2401 (the security architecture)” and states “[a]ll of these documents [including RFC 2401] are available on the ETF Web site: www.ietf.org/rfc.html.” Ex. 1064, 9. Exhibit 1065 sets forth a similar imperative statement: “[s]ee the IETF documents RFC 2401 . . . and RFC 2411 . . . at www.ietf.org/rfc/rfc/rfc2411.txt.”). Ex. 1065, 3. In any event, Patent Owner does not challenge this aspect as hearsay.

Rather, Patent Owner apparently challenges the publication dates on the magazine covers as hearsay. For the reasons stated above under the reasoning of *Seabery*, IPR2016-00840, Paper 60, 5–6 & n.2, the dates on the

magazine covers are not assertions and therefore are not hearsay. *See* Ex. 1064, 1 (bearing date and nomenclature “August 16, 1999, Volume 21, Issue 33” and also bearing a mail date stamp on the bottom of “JAN 24 00”); Ex. 1065, 1 (bearing date and nomenclature “March 15, 1999, Volume 16, Number 11”). These dates, like the volume and issue numbers, are not assertions of a date certain of publication. Similar to the facts underlying cases cited in *Seabery*, the dates, like the volume and issue numbers, serve to identify the particular magazine issue and constitute circumstantial evidence of the date of publication.

Accordingly, Patent Owner has not met its burden on its Motion to exclude Exhibits 1064 and 1065 as hearsay. Under an alternative showing, Petitioner shows the magazine articles satisfy the residual hearsay exception. *See* Opp. 9–14 (addressing factors under Fed. R. Evid. 807(a)). We adopt Petitioner’s showing as sufficient. *See id.* In addition, these articles include circumstantial guarantees of trustworthiness as written prior to litigation by disinterested parties in periodical trade magazines that almost qualify as ancient documents (i.e., almost 20 years old). *See* Fed. R. Evid. 803 (16) (ancient authentic documents of 20 years old are not hearsay). As noted above, both magazine articles bear specific volumes and issue numbers along with the publication dates. *See* Ex. 1064 (Aug. 16, 1999, vol. 21, iss. 33); Ex. 1065 (March 15, 1999, vol. 16, no. 11). As also noted above, the articles corroborate each other as they mention the same website for the availability of RFC documents, including RFC 2401. Exhibits 1008, 1064 and 1065 corroborate each other as showing the availability of RFC 2401 at the same timeframe. *See* Opp. 10–12 (quoting, *inter alia*, *PGMedia, Inc. v. Network Sols., Inc.*, 51 F. Supp. 2d 389, 406 (S.D.N.Y. 1999) (“[M]ore than

2000 RFC's which have been written and circulated' as part of development of the Internet"). Based on the foregoing, Patent Owner's Motion to Exclude Exhibits 1064 and 1065 is denied, and Patent Owner's Motion to Exclude Exhibits 1060, 1063, and 1072 is dismissed as moot.

2. Exhibits 1032–35, 1038–40, 1045–48, 1053, and 1073–74

Patent Owner seeks to exclude the above-listed Exhibits as inadmissible hearsay. Mot. 3–4. Because we do not rely on any of the Exhibits listed above, Patent Owner's Motion to Exclude 1032–35, 1045–48, and 1073–74, is dismissed as moot. Petitioner's expert, Mr. Tamassia, relies on Exhibits 1038–40 and 1053 as a basis to formulate his opinion. See Opp. 3. Patent Owner does not dispute that Exhibits 1038–40 and 1053 present the kinds of facts and data that Mr. Tamassia reasonably would rely upon in forming an opinion. See Reply to Opp. 1–3. As a result, Exhibits 1038–40 and 1053 need not be independently admissible. See Fed. R. Evid. 703; *Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc.*, 711 F.3d 1348, 1373 (Fed. Cir. 2013).

IV. CONCLUSION

For the foregoing reasons, Petitioner establishes by a preponderance of evidence that claims 1–9, 11–23, and 25–28 of the '516 patent are unpatentable for obviousness.

V. ORDER

In consideration of the foregoing, it is hereby

ORDERED that claims 1–9, 11–23, and 25–28 of U.S. Patent No. 8,904,516 B2 are unpatentable;

FURTHER ORDERED that Patent Owner's Motion to Exclude is *dismissed as moot* with respect to Exhibits 1032–35, 1045–48, 1060, 1063,

IPR2016-01585
Patent 8,904,516 B2

1072–74 and is *denied* with respect to Exhibits 1008, 1036, 1038–40, 1053, and 1064–65.

FURTHER ORDERED that, because this Final Written Decision is final, a party to the proceeding seeking judicial review of the Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Jeffrey P. Kushan
Scott M. Border
Thomas A. Broughan, III
SIDLEY AUSTIN LLP
jkushan@sidley.com
sborder@sidley.com
tbroughan@sidley.com

PATENT OWNER:

Joseph E. Palys
Naveen Modi
PAUL HASTINGS LLP
josephpalys@paulhastings.com
naveenmodi@paulhastings.com