

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-00868
Patent 8,516,131 B2

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

ANDERSON, *Administrative Patent Judge*.

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

I. INTRODUCTION

Apple Inc. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1–10, 13–22, and 25–27 of U.S. Patent No. 8,516,131 B2 (Ex. 1003, “the ’131

patent”). VirnetX Inc. (“Patent Owner”)¹ filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). We have jurisdiction under 35 U.S.C. § 314. On October 1, 2015, we granted the Petition and instituted trial on claims 1–10, 13–22, and 25–27 of the ’131 patent. Paper 8 (“Institution Decision” or “Inst. Dec.”)

After institution of trial, Patent Owner filed a Patent Owner Response (Paper 23, “PO Resp.”), and Petitioner filed a Reply (Paper 26, “Reply”). Additionally, Patent Owner filed a Motion to Exclude evidence (Paper 30, “Motion,” “Mot.”). In support of its Petition, Petitioner proffered the Declaration of Dr. Roberto Tamassia (“Tamassia Declaration,” Ex. 1005). The deposition of Dr. Tamassia was taken by Patent Owner and filed by both parties. (“Tamassia Deposition,” Ex. 1071).² Patent Owner proffered the Declaration of Dr. Fabian Monroe. (“Monroe Declaration,” Ex. 2018). The deposition of Dr. Monroe (“Monroe Deposition,” Ex. 1066) was taken in this proceeding and in *Apple v. VirnetX Inc.*, IPR2014-00237, Final Written Decision (PTAB May 11, 2015) (Paper No. 41) (“’237 FWD” or generally “’237 IPR”)) (on appeal at the Federal Circuit).³

An oral hearing was held on June 27, 2016. The transcript of the hearing has been entered into the record. Paper 38 (“Tr.”).

¹ The Petition also names Science Application International Corporation as Patent Owner. However, the Patent Owner Response names only VirnetX Inc.

² Patent Owner filed the Tamassia Deposition as Exhibit 2019. We refer only to Exhibit 1071 unless otherwise noted.

³ The deposition of Dr. Monroe (Ex. 1067) from the ’237 IPR was also filed here but neither party cites to Exhibit 1067.

We have jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). We conclude, for the reasons that follow, that Petitioner has shown by a preponderance of the evidence that claims 1–10, 13–22, and 25–27 of the '131 patent are unpatentable.

A. The '131 Patent

The '131 patent describes a system and method for transparently creating a secure communications link between a client device and a target device. Ex. 1003, Abstract, Figs. 26, 27 (elements 2601, 2604). Secure communication is based on a protocol called the “Tunneled Agile Routing Protocol” or “TARP.” *Id.* at 3:16–19. Once the encrypted communications channel is created, the devices are configured to allow encrypted communications between themselves over the encrypted communications channel. *Id.* at 40:36–45. Figure 26 of the '131 patent is reproduced below.

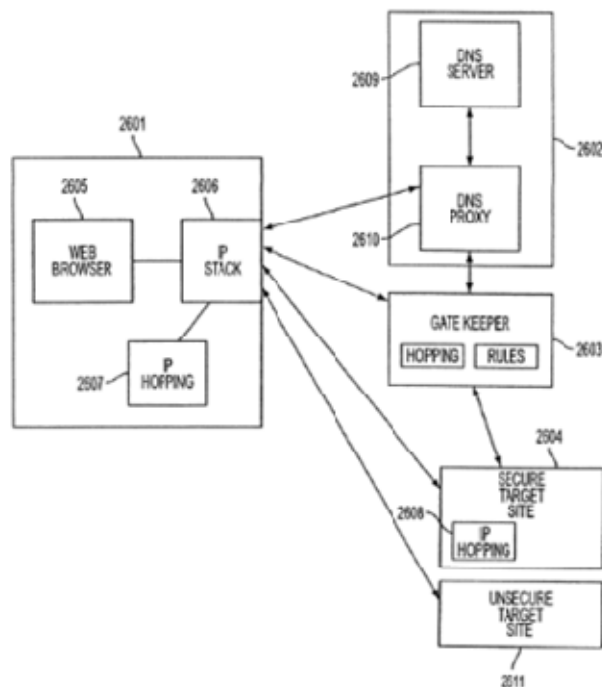


FIG. 26

Referring to Figure 26, reproduced above, user's computer 2601 is a conventional client, e.g., a web browser. Ex. 1003, 40:26–28. Gatekeeper server 2603 is interposed between modified Domain Name Server (“DNS”) 2602 and secure target site 2604. *Id.* at 40:30–35. The DNS includes both conventional DNS server function 2609 and DNS proxy 2610. *Id.* Conventional IP protocols allow access to unsecure target site 2611. *Id.* at 40:58–59.

In one described embodiment, establishing the encrypted communications channel includes intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device. Ex. 1003, 40:36–54. It further includes determining whether the request to look up the IP address corresponds to a device that accepts an encrypted channel connection with the client device. *Id.* at 40:36–59. Gatekeeper 2603 facilitates and allocates the exchange of information for secure communication, such as using “hopped” IP addresses. *Id.* at 40:67–41:3.

The DNS proxy server handles requests for DNS look-up for secure hosts. Ex. 1003, 41:11–15. If the host is secure, then it is determined whether the user is authorized to connect with the host. *Id.* at 41:20–23. If the user is authorized to connect, a secure Virtual Private Network (VPN) is established between the user's computer and the secure target site. *Id.* at 41:35–38.

B. Illustrative Claim

Petitioner challenges claims 1–10, 13–22, and 25–27 of the '131 patent. Claim 1 is an independent apparatus claim and claim 15 is an

independent method claim. All remaining claims depend directly or indirectly from claim 1 or 15. Method claim 15 is reproduced below.

15. A method executed by a first network device for communicating with a second network device, the method comprising:

 sending a request to look up an internet protocol (IP) address of a second network device based on a domain name associated with the second network device;

 following interception of the request and a determination that the second network device is available for the secure communications service, receiving an indication that the second network device is available for a secure communications service, the requested IP address of the second network device, and provisioning information for a secure communication link;

 connecting to the second network device over the secure communication link, using the received IP address of the second network device and the provisioning information for the secure communication link; and

 communicating at least one of video data and audio data with the second network device using the secure communications service via the secure communication link.

Ex.1003, 57:11–30.

C. Instituted Ground of Unpatentability

We instituted on the ground that claims 1–10, 13–22, and 25–27 were unpatentable under 35 U.S.C. § 103 over Beser⁴ and RFC 2401.⁵ Inst. Dec. 19.

⁴ US 6,496,867 B1, issued December 17, 2002, to Nurettin B. Beser and Michael Borella (“Beser,” Ex. 1007).

⁵ S. Kent & R. Atkinson, *Security Architecture for the Internet Protocol*, Request for Comments: 2401, 1–66 (November 1998) (BBN Corp.) (“RFC 2401,” Ex. 1008).

II. ANALYSIS

A. Claim Construction

In an *inter partes* review, the Board construes claim terms in an unexpired patent under their broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2019). Under this standard, absent any special definitions, claim terms or phrases are given 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). The Board construed claim terms similar to those at issue here in several other proceedings challenging patents related to the '131 patent. *See, e.g.*, '237 FWD; *Apple Inc. v. VirnetX Inc.*, IPR2014-00481, Final Written Decision (PTAB Aug. 24, 2015) (Paper 35) (“’481 FWD” or generally “’481 IPR”)(on appeal at the Federal Circuit); *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1317–19 (Fed. Cir. 2014) (addressing ancestor Patent Owner patents having similar claim terms).

Petitioner and Patent Owner each proffer proposed constructions of several claim terms. *See* Pet. 9–17; PO Resp. 4–26. Regardless of the preceding, Petitioner contends that the only terms Patent Owner argues are not disclosed by Beser and RFC 2401 are “interception” and “virtual private network link.” Pet. Reply 1–2 (citing PO Resp. 4–5, 18–24). Patent Owner disagrees with the Institution Decision where we construed “secure communication link” and “provisioning information.” PO Resp. 1–2; *see* Inst. Dec. 7–9. In addition to the terms identified by Petitioner, Patent Owner argues its proposed constructions the following terms: “interception

of the request,” “secure communication link,” “provisioning information,” and “virtual private network link.” PO Resp. 4–24. Patent Owner identifies an additional four terms which it categorizes as either not requiring construction or as consistent with Petitioner’s proposed constructions. *Id.* at 25–26.

We have compared Patent Owner’s arguments in its Response to the terms it identifies for construction. Specifically, Patent Owner argues Beser and RFC 2401 do not disclose: (1) “intercepting from the client device a request to look up an Internet Protocol (IP) address” or “intercepting” (the “intercepting limitation”);⁶ and (2) a “virtual private network link” recited by claim 10.⁷ However, as discussed in II.I. of this Decision, Patent Owner does not argue the construction of “virtual private network link” as a basis for patentability of claim 10.

No other argument in the Response is based on a term Patent Owner proposes for construction. We, therefore, agree with Petitioner that the only terms that may require construction are “intercepting from the client device a request to look up an Internet Protocol (IP) address” and “virtual private network link.” See Pet. Reply 1–2; see also *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (claim terms need only be construed to the extent necessary to resolve the case).

1. “interception” (claims 1, 9, 14, 15, 26, and 27)

Independent method claim 15 recites “following interception of the request and a determination that the second network device is available for

⁶ PO Resp. 32–36.

⁷ PO Resp. 45–46.

the secure communications service.” Claims 9, 14, 15, 26, and 27 also recite “interception of the request” or “interception.”

Petitioner proposes a construction from the institution decision in the ’237 IPR, “receiving a request pertaining to a first entity at another entity.” Pet. 10–11. This construction was adopted in the ’237 IPR. *See* ’237 FWD, 10–12.

Quoting Patent Owner in the ’237 IPR, we noted that Patent Owner “disagrees with this construction” (’237 PO Resp. 23), but “believes that no construction is necessary” (*id.* at 26), because “it does not appear that the construction of ‘intercepting’ will bear on the outcome of the issues in this *inter partes* review” (*id.* at 23). ’237 FWD, 11. The ’237 IPR and this proceeding involve the same issue with respect to this term and the asserted prior art. Patent Owner does not dispute the relevance of the ’237 IPR, including the construction of the intercepting limitation. *See* PO Resp. 33, n.3 (referencing our construction of the intercepting limitation in the ’237 IPR). Patent Owner states in the instant proceeding that “no construction is necessary.” PO Resp. 4 (Table, “Patent Owner’s Proposed Construction”). Nevertheless, Patent Owner urges that if we construe the term, then we should adopt Patent Owner’s construction: “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 secure communication link.” *Id.*

To support its proposed alternative construction in this proceeding, Patent Owner argues its alternative construction “appropriately captures the notion of performing an additional evaluation on a request to look up an IP address related to establishing an encrypted communications channel,

beyond conventionally resolving it and returning the address.” PO Resp. 5 (citing Prelim. Resp. 25–28⁸). Patent Owner’s arguments and the record show that Patent Owner’s proposed construction adds unnecessary functionality to “intercepting a request” and violates the plain language of the claim. According to Patent Owner’s arguments, another recited phrase in the independent claims (claims 1 and 15), captures the functionality, in particular, the “determination” clause of those claims. *Id.* More specifically, Patent Owner argues in the determination clause of claims 1 and 15 “a determination is made as a result of the request [to look up an IP address] that the second network device is a device that is available for the secure communication service.” *Id.* We are not persuaded that functionality in another limitation of the independent claims supports Patent Owner’s proposal. Indeed, that the additional functionality Patent Owner proposes is covered elsewhere in the same claim would make Patent Owner’s proposed construction of the intercepting limitation duplicative and/or confusing.

The parties agree that the intercepting limitation (at least) involves receiving a request at some intermediate device. PO Resp. 4; Pet. 9–10. Patent Owner’s proposed construction does not create any distinction between receiving and intercepting. According to Petitioner’s proposed construction, an “interception” by (intermediate) proxy DNS includes “receiving a request at a device other than the device specified in the request.” Pet. 10 (citing Ex. 1005 ¶ 98). Petitioner contends that the DNS

⁸ To the extent it attempts to do so, it is improper for Patent Owner to incorporate the Preliminary Response in its Response by reference. 37 C.F.R. § 42.6(a)(3). To the extent the arguments are repeated in the Response, they are proper and will be considered.

proxy 2610 “‘intercepts’ all DNS lookup functions to examine whether access to a secure site has been requested.” *Id.* (citing Ex. 1003, 40:36–42, Figs. 26, 27). Furthermore, as quoted above, Patent Owner agreed in the ’237 IPR that Petitioner’s construction captured “the disclosed embodiments.” ’237 PO Resp. 26. In essence, Petitioner’s construction captures the notion of interception as disclosed in the ’131 patent, by requiring receiving to “pertain” to another entity.

Based on the foregoing discussion, the record shows that the additional functionality urged by Patent Owner should not be imported into the intercepting limitation, and Petitioner’s construction tracks the claim and Specification. Accordingly, as set forth in the ’237 IPR Final Written Decision, the broadest reasonable construction of the intercepting limitation is “receiving a request pertaining to a first entity at another entity.”

b. “virtual private network (VPN) link” (claim 10)

We did not construe “virtual private network link” in the Institution Decision. In the institution decision of the ’481 IPR, involving the related ’180 patent,⁹ we interpreted “virtual private network communication link”¹⁰ to mean “a transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping.” ’481 IPR,

⁹ U.S. Patent No. 7,188,180 is a continuation-in-part of U.S. Patent No. 6,502,135. ’481 IPR, Ex. 1001, (60). The ’131 patent is also a continuation-in-part of US Patent No. 6,502,135. Ex. 1003, (63).

¹⁰ The additional term “communication” does not affect the construction. The addition of “communication” at most makes it clear that the “link” is one for “communication.”

Institution Decision, slip op. at 6–7 (PTAB Sept. 3, 2014)(Paper 11). Petitioner adopts the construction from the ’481 IPR Institution Decision. Pet. 16 (citing Ex. 1005 ¶ 117). Patent Owner argues that Petitioner’s proposed construction “contradicts the plain language of the claims, is internally inconsistent, [and] is inconsistent with the ’131 patent specification and prosecution history and is inconsistent with its own prior statements.” PO Resp. 18–19. Instead, Patent Owner asserts the correct construction should be “[a] path between two devices in a virtual private network.” *Id.* at 18 (citing Ex. 2018 ¶¶ 31–39). Notwithstanding the preceding, Patent Owner argues a “virtual private network link” should have certain characteristics including: a virtual private network; a network; “authentication” and address hopping” alone do not establish a “virtual private network link.” encryption is required;” and the link must be “direct.” *Id.* at 19–24. For purposes of this Decision, we need not resolve the dispute between the parties on this term because, as discussed in II.I. below, we determine that Petitioner has shown, by a preponderance of the evidence, that this limitation, under either party’s proposed construction, would have been obvious over the combination of Beser and RFC 2401.

OBVIOUSNESS-BESER AND RFC 2401

Petitioner alleges claims 1–10, 13–22, and 25–27 would have been obvious over Beser and RFC 2401. Pet. 26–57. Petitioner’s evidence includes the Tamassia Declaration, which describes Beser and RFC 2401. Ex. 1005 ¶¶ 312–402, 421–441.

B. Level of Ordinary Skill in the Art

Petitioner’s expert, Dr. Tamassia, states that a person of ordinary skill in the art would have “a good working knowledge of networking protocols,

including those employing security techniques, as well as cryptographic methods and computer systems that support these protocols and techniques.” Ex. 1005 ¶ 148; see Pet. 8. Such a person would have gained this knowledge “either through several years of practical working experience or through education and training” or some combination of both. *Id.*

Patent Owner’s expert, Dr. Monroe, states that “a person of ordinary skill in the art [at the relevant time] would have had a master’s degree in computer science or computer engineering, as well as two years of experience in computer networking with some accompanying exposure to network security.” Ex. 2018 ¶ 13. Dr. Monroe adds that his “view is consistent with VirnetX’s view that a person of ordinary skill in the art requires a master’s degree in computer science or computer engineering and approximately two years of experience in computer networking and computer security.” *Id.*

We are persuaded that Patent Owner’s description of the background of a person of ordinary skill in the art is not lower than or inconsistent with Petitioner’s description. Instead, Patent Owner’s definition requires a particular educational background, but appears to result in the same level of expertise as Petitioner’s definition. Based on the testimony of the parties’ experts as well as our review of the ’131 patent and the prior art involved in this proceeding, we conclude that a person of ordinary skill in the art would have a master’s degree in computer science or computer engineering and approximately two years of experience in computer networking and computer security—or the equivalent, obtained through practical work experience and training.

*C. Tamassia Declaration*¹¹

Patent Owner argues that the entirety of Dr. Tamassia's Declaration should be given little or no weight because "he failed to consider, let alone opine on, how any of the claim features are disclosed in asserted references." PO Resp. 47. Petitioner responds that Dr. Tamassia has "offered probative testimony on many of the factual inquiries underpinning an obviousness analysis" that "can certainly 'assist the trier of fact to understand the evidence or determine a fact in issue.'" Reply 22–23 (citing Fed. R. Evid. 702). Petitioner adds that "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 23.

Patent Owner has not articulated a persuasive reason for giving Dr. Tamassia's Declaration, as a whole, little or no weight in our analysis. We agree with Petitioner that experts are not required to opine on every relevant factual and legal issue in order to be accorded substantial weight. The cases Patent Owner relies on do not persuade us otherwise. For example, Patent Owner cites *Schumer v. Laboratory Computer Systems, 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. 48. Patent Owner's quotation, however, mischaracterizes *Schumer* by omitting introductory words necessary to the meaning of the quoted sentence. In its entirety, the quoted portion of *Schumer* states the following:

¹¹ We address Patent Owner's motion to exclude certain paragraphs of Exhibit 1005 in a separate section, below.

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.* So, instead of laying out a specific, required format for the content of all testimony regarding invalidity, as asserted by Patent Owner, this portion of *Schumer* confirms the unremarkable proposition that conclusory, overly general, confusing, and self-interested testimony should not be relied upon. *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 has not shown that the whole of Dr. Tamassia’s testimony suffers from any of these failings.

Under 37 C.F.R. § 42.1(d), we apply the preponderance of the evidence standard in determining whether Petitioner has established unpatentability. In doing so, it is within our discretion to determine the appropriate weight to be accorded the evidence presented, including expert opinion, based on the disclosure of the underlying facts or data upon which that opinion is based. Thus, we decline to make a determination about Dr. Tamassia’s opinion, as a whole. Rather, in our analysis we will consider, as it arises, relevant

portions of Dr. Tamassia's testimony and determine the appropriate weight to accord that particular testimony.

D. Prior Art Printed Publication Status of RFC 2401

Patent Owner asserts that Petitioner has not sufficiently established that RFC 2401 qualifies as a printed publication as of its alleged publication date. PO Resp. 51–59. We look to the underlying facts to make a legal determination as to whether a document is a printed publication. *Suffolk Techs., LLC v. AOL Inc.*, 752 F.3d 1358, 1364 (Fed. Cir. 2014). The determination of whether a document is a “printed publication” under 35 U.S.C. § 102(b) involves a case-by-case inquiry into the facts and circumstances surrounding its disclosure to members of the public. *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004). Public accessibility is a key question in determining whether a document is a printed publication and is determined on a case-by-case basis. *Suffolk Techs.*, 752 F.3d at 1364. To qualify as a printed publication, a document “must have been sufficiently accessible to the public interested in the art.” *In re Lister*, 583 F.3d 1307, 1311 (Fed. Cir. 2009) (internal citation and quotation omitted).

In our Institution Decision, we found that RFC 2401 included indicia suggesting a reasonable likelihood that the document was made public because (1) RFC 2401 is a dated “Request for Comments” from the “Network Working Group,” discussing a particular standardized security protocol for the Internet, and (2) it 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.” Inst. Dec. 10 (citing Ex 1008, 1). On this basis,

we determined that Petitioner had met its burden for a threshold showing to proceed to trial. *Id.*

In support of Petitioner’s position, the testimony from the Tamassia Declaration is that RFCs are “prepared and distributed under a formalized publication process overseen by one of several Internet standards or governing bodies,” such as the IETF. Ex. 1005 ¶ 186. Dr. Tamassia goes on to discuss an RFC that discusses the RFC development and publication process itself—RFC 2026, dated October 1996. *Id.* ¶¶ 187–190; Ex. 1036. Dr. Tamassia testifies that “[t]he publication date of each RFC is contained in the RFC, typically in the top right corner of the first page of the document” and “[t]his is the date it was released for public distribution on the Internet.” *Id.* ¶ 190. RFC 2026 also explains that anyone can obtain RFCs from a number of Internet hosts and each RFC “is made available for review via world-wide on-line directories.” Ex. 1036, 4–6.

Patent Owner argues that Petitioner cannot rely on evidence it has proffered to support this finding. First, Patent Owner argues that testimony by Dr. Tamassia should not be accorded any weight because Dr. Tamassia has not been established to have personal knowledge that RFC 2401 was actually released to the public in November 1998, nor has Dr. Tamassia “been established as someone familiar with, let alone an expert in, the workings of the Internet Engineering Task Force (IETF)[—]the body responsible for the RFCs.” PO Resp. 53–54.¹²

¹² Patent Owner also argues we should give Dr. Tamassia’s testimony on this issue no weight because the Petition does not cite to these paragraphs. PO Resp. 53 n.5. Patent Owner, itself, however, directed the Board’s attention to this testimony on this issue in its Preliminary Response (Paper 6, 3), and

We find Dr. Tamassia's testimony as to public accessibility of RFCs in general to be credible, especially given the independent support of RFC 2026 (Ex. 1036). As part of routine discovery (37 C.F.R. § 42.51(b)(1)(ii)), Patent Owner had the opportunity to cross-examine Dr. Tamassia and did so, taking the Tamassia Deposition and making it of record. See Ex. 2016. Patent Owner does not point us to any discussion of this issue in the Tamassia Deposition. RFC 2401's contents are consistent with the publication process described by RFC 2026 and Dr. Tamassia, including a date "November 1998" indicated on the top right corner of the first page of the document. Moreover, a request for suggestions and improvements for an Internet standards protocol, having no indication of being a mere draft or internal paper, is the type of document whose very purpose is public disclosure.

"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 sufficiently disseminated to persons of ordinary skill interested in computer networking and security to be deemed "publicly accessible" at the relevant time.

thus clearly has had adequate notice of its contents such that it may respond with no issue of prejudice.

Therefore, on this record, we determine RFC 2401 qualifies as a prior art printed publication under 35 U.S.C. § 102(b).

E. 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, Abstract. Figure 1 of Beser is reproduced below.

FIG. 1

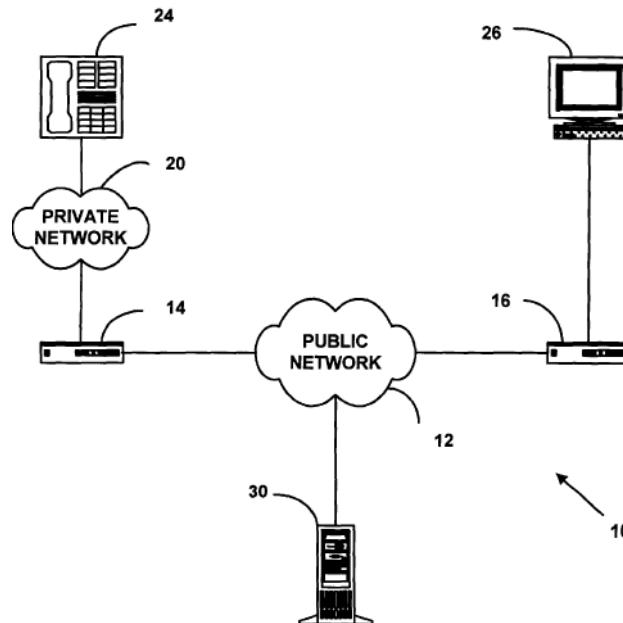


Figure 1 of Beser, reproduced above, illustrates a network system, including public network 12, network devices 24 and 26, private network 20, trusted third-party network device 30, and modified routers or gateways 14 and 16. Ex. 1007, 3:60–4:18. Beser describes network devices 24 and 26 as telephony 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 Abstract, Figs. 1, 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 12.” *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 on 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.

F. Overview of RFC 2401

RFC 2401 describes the security services offered by the IPsec protocols, including “access control, connectionless integrity, data origin

authentication, [and] . . . confidentiality (encryption).” Ex. 1008, 3–4. RFC 2401 describes IPsec further, as follows:

IPsec 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.

The “security services use shared secret values (cryptographic keys). . . . (The keys are used for authentication/integrity and encryption services.)” *Id.*

G. Claims 1 and 15

Claim 1 recites “a network device” and claim 15 recites a “method executed by a first network device for communicating with a second network device.” The two claims include the same “operative limitations.” Pet. 34. Both Petitioner and Patent Owner argue claims 1 and 15 together. Pet. 34–47; PO Resp. 30–38. Petitioner addresses separately the system elements of claim 1. Pet. 47–49. We, therefore, analyze the two independent claims 1 and 15 together referencing claim 15 unless otherwise stated.

1. Petitioner’s Assertions

Petitioner asserts that Beser teaches each of the limitations of claims 1 and 15 except “encryption.” Pet. 34–49, 42–47 (re: encryption). Patent Owner does not argue any limitation of claims 1 or 15. Specifically, as per

the preamble of claim 15,¹³ Petitioner argues that Beser’s originating end device is equivalent to the claimed “first network device” (claim 15) and “network device” (claim 1) and Beser’s terminating end device is equivalent to the claimed “second network device.” *Id.* at 34–35 (citing Ex. 1007, 8:15–20, 21:52–62, 22:2–22; Ex. 1005 ¶¶ 312, 380–81).

Petitioner also argues that Beser discloses the first step of claim 15, sending a “request to look up an internet protocol (IP) address” of a second network device. Petitioner contends that Beser teaches sending a request from the originating to the terminating end device. *Id.* (citing Ex. 1007, 7:64–8:1, 9:64–10:41; Ex. 1005 ¶ 354). Petitioner argues the request contains a unique identifier, i.e., a domain name, associated with the terminating end device and the trusted third-party device can be a domain name server. *Id.* at 35–36 (citing Ex. 1007, 4:9–11, 10:37–42, 10:55–11:5, Ex. 1005 ¶ 357).

The second step of claim 15 recites “interception of the request” and a “determination that the second network device is available for . . . secure communications.” Petitioner argues “interception” occurs when all of the data packets received at the first network device are evaluated. Pet. 37 (citing Ex. 1007, 8:21–47; Ex. 1005 ¶¶ 337–338, 355, 360). If the first network device determines that a data packet contains a request to initiate an IP tunnel, that packet is forwarded to the trusted-third-party network device

¹³ Petitioner proceeds on the basis that the preamble is limiting. Patent Owner does not make a contrary argument. The preamble recites, in part, a “method executed by a first network device for communicating with a second network device,” which provides antecedent basis for those terms. We agree the preamble is limiting.

for special processing. *Id.* (citing Ex. 1007, 4:7–42, 8:21–47; Ex. 1005 ¶¶ 338, 360). Petitioner concludes that when the trusted-third-party network device receives the request, it “intercepts” the request and looks up the IP address associated with the domain name. *Id.* (citing Ex. 1007, 4:8–11, 8:4–7, 10:38–41, 11:26–55; Ex. 1005 ¶¶ 348, 361–363).

Petitioner argues that the Specification describes that “a DNS proxy ‘determine[]’ whether access to a secure site has been requested “by reference to an internal table of [secure] sites.” Pet. 38 (citing Ex. 1003, 40:36–42; ’237 IPR, Paper 15, 15 (“determining . . . whether the second network device is available for a secure communications” as including “one or more of 1) whether the device is listed with a public internet address, and if so, allocating a private address for the second network device, or 2) some indication of the relative permission level or security privileges of the requester”). Petitioner argues the domain name server of Beser maintains 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.” Pet. 38 (citing Ex. 1007, 11:48–52; Ex. 1005 ¶¶ 361, 363, 365). Petitioner contends the “determination” described above in the ’131 patent is the same as Beser’s teaching that the trusted-third-party network device “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.” *Id.* at 38–39 (citing Ex. 1007, 11:30–36, 11:45–58; Ex. 1005 ¶¶ 348, 361, 363, 365).

The third step of claim 15 after the “interception” and “determination” step is receiving an “*indication that the second network device is available*

for [a/the] secure communications service.” Petitioner argues the step is taught in Beser’s teaching that the trusted-third-party network device negotiates with the first and second network devices to establish the IP tunnel. Pet. 40 (citing Ex. 1007, 9:6–11; 9:26–30, 11:9–44; Ex. 1005 ¶¶ 361–363, 368).

The next recited step of claim 15 is “receiving . . . the requested IP address of the second network device.” Beser teaches that “[t]he assignment of private network addresses to the ends of the tunneling association may also include transmitting the private network addresses to the network devices at the ends of the tunneling association where the private network addresses are stored on these end devices.” Ex. 1007, 21:48–52. Petitioner relies on the preceding disclosure to meet the limitation. Pet. 41.

Claim 15 next recites receiving “provisioning information” for a “secure communication link.” Petitioner relies on the construction of “secure communication link” as requiring the use of “obfuscation methods,” such as “encryption.” Petitioner relies on RFC 2401, in combination with Beser, to show encryption as per RFC 2401 and “secure communications link” as per Beser. Pet. 42–44.

Claim 15 concludes with connecting and communicating over the secure communications link. Again, Beser is relied on for the connection and RFC 2401 is relied on for encryption. Pet. 44–47.

Concerning the preamble of claim 1 and the recited “storage device” and “processor,” Petitioner relies on Beser. Beser discloses a CPU and memory. Ex. 1007, 5:15–18. Beser also discloses programmed computers with processing elements and storage media containing code that configures how those devices function. Ex. 1007, 4:43–52, 5:15–47. Petitioner relies

on these disclosures to meet the limitations. Pet. 47–49 (additionally citing Ex. 1005 ¶ 331). Regarding the claimed “multimedia applications,” Petitioner argues Beser discloses “facsimile or audio applications.” *Id.* at 48–49 (citing Ex. 1007 at 4:47–52; Ex. 1005 ¶¶ 326–327).

2. Undisputed Limitations

Patent Owner does not dispute every allegation made in the Petition relating to the steps of claim 1 or the limitations of claim 15. As detailed above, we have reviewed the evidence and argument of the undisputed allegations. We find that Petitioner has shown by a preponderance of the evidence that those steps and limitations which are not disputed in the Response are disclosed by Beser in combination with RFC 2401.

3. Patent Owner’s Assertions

In general, Patent Owner contends that Beser alone does not disclose encryption but uses a “tunneling association.” PO Resp. 27 (citing Ex. 1007, 3:1–9, Ex. 2018 ¶ 42). As discussed above, the Petition acknowledges the Beser IP tunneling scheme does not teach encryption expressly but cites to RFC 2401 as teaching encryption. Pet. 42–44.

Some of Patent Owner’s arguments are based on Beser’s Figure 6, reproduced in the Response at page 29 and below:

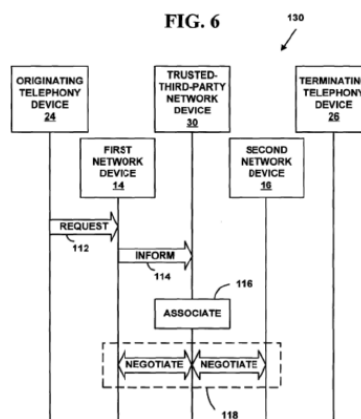


Figure 6 of Beser, reproduced above, illustrates first and second network devices 14 and 16, originating device 24, terminating telephony device 26, and trusted third-party network device 30. See Ex. 1007, 11:59–12:27. In order to communicate between the originating and terminating devices, the originating end device sends a tunnel initiation request to first network device 14. *Id.* at 7:65–67. The tunneling request includes a unique identifier for the terminating device. *Id.* at 8:1–3.

Referencing Figure 6, Patent Owner describes Beser as follows:

The trusted-third-party network device 30 associates a public IP address of a second network device 16 with the unique identifier of terminating telephony device 26. (Ex. 1007 at 8:4–7, 11:26–32; Ex. 2018 at ¶ 45.) The first and second network devices 14 and 16 then “negotiate” private IP addresses through the public network 12. (Ex. 1007 at 8:9–15, 11:58, Fig. 6 (step 118); Ex. 2018 at ¶ 45.)

PO Resp. 29.

Patent Owner contests two limitations of claim 15. The first is “send[ing] a request to look up an internet protocol (IP) address of a second network device based on a domain name associated with the second network device.” PO Resp. 30–32. The second limitation argued is “interception of the request.” *Id.* at 32–36. Patent Owner also argues: Beser and RFC 2401 do not show the “[f]eatures as [a]rranged in the [c]laims.” *Id.* at 36–38. Last, Patent Owner argues the person of ordinary skill in the art would not have combined Beser and RFC 2401. *Id.* at 38–44. Each argument is addressed below.

a. Sending a Request to Look up an Internet Protocol (IP) Address

Patent Owner's first argument is that Beser does not teach "send[ing] a request to look up an internet protocol (IP) address of a second network device based on a domain name associated with the second network device." Patent Owner asserts that the tunneling request of Beser is not a request to look up an Internet Protocol (IP) address." PO Resp. 30 (citing Ex. 2018 ¶ 47, Pet. 35). Patent Owner argues a tunneling request is a "pre-established way to initiate a tunnel between two devices" that does not involve looking up an IP address. *Id.* at 31 (citing Ex. 1007, 12:2–4; Ex. 2018 ¶ 49). Patent Owner argues the negotiation between the first and second network devices does not involve looking up an IP address. *Id.*

Patent Owner argues the first and second network devices, not the trusted-third-party network device as alleged in the Petition, "'negotiate' private IP addresses, including the private IP address for the originating and terminating device." PO Resp. 31 (citing Pet. 36, Ex. 1007, 8:9–15, 11:58, Fig. 6 (step 118); Ex. 2018 ¶ 49). In addition, Patent Owner argues that there is no look up of an IP address because Beser "involves *assignment* of a first private network address to the originating device and a second private network address to the terminating device." *Id.* (citing Ex. 1007, 12:2–4; Ex. 2018 ¶ 49.)

According to Patent Owner, although Beser teaches that a database includes an entry for the public IP address of the terminating device, that alone does not suggest anything is looked up, specifically the public address of terminating device 26. PO Resp. 31–32 (citing Ex. 1007, 11:50–55; Ex. 2018 ¶ 50). Rather, Patent Owner argues, "*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.” *Id.* at 32 (citing Ex. 1007, 11:26–32; Ex. 2018 ¶ 50). Patent Owner concludes that the claims recite that a request to look up an IP address is “intercepted allowing it *not* to be processed in the conventional manner.” *Id.* (citing Ex. 1003, 40:36–54; Ex. 2018 ¶ 51).

Petitioner responds that Beser’s trusted third-party device looks up two IP addresses. Reply 8 (citing Pet. 35–36). First, Petitioner asserts the database is a look up because it includes the IP address of second network device 16 that is associated with the unique identifier. *Id.* (citing Pet. 21–22, 35–36; Ex. 1007, 11:45–58). Second, when the tunneling sends a message to network device 16 there is a request for a look up of a private IP address for terminating device 26. *Id.* (citing Pet. 22–24, 35–36; Ex. 1007, 9:29–30, 12:16–19, 14:14–27, Figs. 6, 9). Thus, Petitioner concludes the originating device receives an IP address for the terminating device. *Id.* at 8–9 (citing Pet. 24; Ex. 1007, 21:48–52).

Petitioner also contends that Patent Owner “admits that trusted device 30 contains a database or similar structure that correlates each unique identifier to the public IP addresses of second network device 16 and terminating device 26.” Reply 9–10 (citing PO Resp. 32). Contrary to Patent Owner’s argument that the database does not suggest a look up or the public address of terminating device 26, Petitioner argues Beser “teaches that in Step 116 of Figure 5, trusted device 30 receives the tunneling request, ([Ex. 1007, 11:9–20]), and in response, it associates an IP address with the unique identifier by looking it up in its internal database.” *Id.* at 10 (citing Ex. 1007, 11:26–58).

Petitioner also contends that the claims only specify a request to lookup “based on a domain name ***associated*** with the second network device.” Reply 11 (citing Ex. 1003, 57:14–17¹⁴) (emphasis added). Further, Petitioner notes the ’131 patent explains the IP address looked up “need not be the actual address of the destination computer.” *Id.* (citing Ex. 1007, 40:53–54); *see also* Monroe Deposition, Ex. 1066, 63:25–64:24 (“it does say that the address [returned] could be different from the actual target computer”). Petitioner concludes that the “IP address of network device 16 is ‘associated with’ the unique identifier (*e.g.*, domain name) of terminating device 26,” as required by the claim language. *Id.*

Petitioner points out that Beser discloses embodiments where the trusted third-party device negotiates private IP addresses for the originating and terminating devices. Reply 11 (citing Ex. 1007, 9:29–30, 12:16–19, 14:19–27, Figs. 6, 9; *see* Pet. 21–22, 35–36). As a result, Petitioner argues that Patent Owner’s assertion that negotiation is performed by the first and second network devices relies on a different embodiment. *Id.* (citing PO Resp. 31; *Arthrocare Corp. v. Smith & Nephew, Inc.*, 406 F.3d 1365, 1372 (Fed. Cir. 2005) (no requirement that every possible embodiment of a prior art reference satisfy the claims)). Petitioner also argues that “second device 16 does not simply ‘assign’ an IP address – it looks one up by selecting an unused address out of a pool of IP addresses.” Reply 12 (citing Ex. 1007, 13:49–64; Pet. 20; ’237 IPR, Paper 41, 22–23 (finding Beser discloses such a request to look up an IP address)).

¹⁴ We have inserted a citation to claim 15’s language regarding “associated.” It appears Petitioner erroneously cites Ex. 1003, 55:18–20, which does not relate to any claim.

We agree with Petitioner’s analysis and determine that Petitioner has shown, by a preponderance of the evidence, that Beser’s tunneling request discloses the claimed request to look up an IP address. Contrary to Patent Owner’s argument, we find that the database of Beser at least implies looking up the public IP 58 address for terminating telephony device 26 to create its tunneling association. *See* Ex. 1007, 11:50–55 (“database entry may also include a public IP 58 addresses for the terminating telephony device”).

The argued distinction between “assignment” and “look up” is not persuasive. Even if second network device 16 “assigns” the IP address to terminating device 26, trusted device 30 “looks up” the IP address when it sends a message to network device 16 requesting a private IP address. What actually occurs in Beser is that “[t]he second private IP 58 address is selected from a second pool of private IP 58 addresses on the second network device 16.” *See* Ex. 1007, 13:49–51, Reply 12, Pet. 20.

A preponderance of the evidence supports Petitioner’s allegation that the unique identifier in the tunneling request is “associated” with the terminating end device. *See* Pet. 35–36 (citing Ex. 1007, 8:1–3, 10:37–11:8; Ex. 1005 ¶ 356). The unique identifier can be “a domain name associated with the second network device,” and the trusted third-party network device that processes the request can be a domain name server. *Id.* (citing Ex. 1007, 4:9–11, 10:37–42, 10:55–11:5; Ex. 1005, ¶ 357). We find these allegations support the claimed recitation that “a domain name [is] associated with the second network device.”

We find that Beser, receives a tunneling request and then “the trusted-third-party network looks up the public IP address associated with the

unique identifier and negotiates private IP addresses for the originating and terminating end devices.” *See* Pet. 36 (citing Ex. 1007, 11:26–36, 11:45–58, 12:28–32, 17:42–49; Ex. 1005 ¶¶ 361–363). We further find “the originating end device receives the private IP address associated with the terminating end device.” *Id.* (citing Ex. 1007, 14:51–62, 21:48–52; Ex. 1005 ¶ 378).

We credit Dr. Tamassia’s testimony cited above in support of our findings. Dr. Tamassia testifies that the trusted-third-party network device may compare the unique identifier to a database of entries, i.e., database of subscribers, to “determine whether the unique identifier correlates to an IP address associated with a second network device or a terminating end device, i.e., a user or end device that is able to communicate using an IP tunnel.” Ex. 1005 ¶ 361 (citing Ex. 1007, 9:6–11, 11:26–36, 11:45–58, 17:45–49). Dr. Tamassia also testifies the trusted-third-party network device may reference a database to determine if the unique identifier corresponds to a secure destination. *Id.* ¶ 363 (citing Ex. 1007, 11:32–36, 11:48–52). We expressly find that this evidence supports the allegation that Beser looks up the IP address associated with the terminating device.

Patent Owner’s principal argument is that Beser’s teaching of database entries for public IP address of the terminating device does not suggest anything is looked up, specifically the public address of terminating device 26. PO Resp. 31–32. This argument is not persuasive in view of the Tamassia Declaration testimony. *See* Ex. 1005 ¶ 361. Our review of the testimony of Dr. Monroe cited by Patent Owner does not alter our finding. *See* Ex. 2018 ¶ 47–51. The cited paragraphs contain conclusions without

sufficient underlying facts to give the testimony significant weight. 37

C.F.R. § 42.65(a). For example, Dr. Monroe opines:

In my opinion, none of the processes in Beser transform the request to initiate a tunneling connection into a request to look up an IP address. In my opinion, one of the novel aspects of the claims of the '131 patent is that, while a request to look up an IP address is transmitted, the request is intercepted allowing it not to be processed in the conventional manner. (*See, e.g.*, Ex. 1003 at 40:36-54.)

Ex. 2018 ¶ 51.

The preceding testimony appears to be partly based on Dr. Monroe's opinion that the Petition's allegations about what is shown in Beser are incorrect. *Id.* ¶ 48. The alleged errors are restatements of the Response. Specifically, Dr. Monroe disagrees that: (1) the trusted third-party device negotiates the private IP address of the terminating device (*id.* ¶ 49); and (2) the database looks up any data structure, specifically the IP address of the terminating device (*id.* ¶ 50). These arguments are only tangentially relevant to the step at issue. In any event, we agree with Petitioner's response to these arguments in its Reply as summarized above.

Furthermore, other than conclusions, Dr. Monroe's testimony does not adequately address the "unique identifier" basis for alleging that Beser teaches "send[ing] a request to look up an internet protocol (IP) address of a second network device based on a domain name associated with the second network device." Instead, the testimony is limited to the conclusion that Dr. Monroe "disagrees" and that "Beser . . . associates a public IP address of a second network device 16 with the unique identifier of terminating telephony device 26." *Id.* ¶ 50 (citing Ex. 1007, 11:26–32). Neither is persuasive.

b. Interception of the Request

Patent Owner's second argument is that Beser does not teach the request to look up an Internet Protocol (IP) address is "intercepted." PO Resp. 32–36. As discussed in detail above, Petitioner argues one "interception" occurs when all of the data packets received at the first network device which looks up the IP address associated with the domain name are evaluated. Pet. 37 (citing Ex. 1007, 4:8–11, 8:4–7, 8:21–47, 10:38–41, 11:26–55; Ex. 1005 ¶¶ 337–338, 348, 355, 360–363).

Patent Owner contends that Petitioner's expert, Dr. Tamassia, testified to an element of intent in the construction of "interception." PO Resp. 33 (citing Ex. Ex. 2019, 80:3–13). Based on the cited testimony, Patent Owner argues interception could be either "'intended for' receipt at a destination different from where the request is intercepted" or the destination where a request is "ordinarily received by another entity, and instead, it is received at the first entity." *Id.*

Notwithstanding that Patent Owner does not propose an intent element in its arguments for the construction of "interception," it argues this "construction" should be binding on Petitioner. Specifically, Patent Owner cites the Monroe Declaration for its testimony that "[n]either the first network device nor the trusted-third-party network device performs 'interception' when analyzed in a manner consistent with how Petitioner's expert understands the term." *Id.* (citing Ex. 2018 ¶ 53).

Patent Owner proceeds to argue Beser does not meet the two scenarios it somehow believes are the construction of "interception" we should follow here. PO Resp. 34–35. Based on its "construction," Patent Owner concludes that Beser does not teach the interception step. *Id.* at 36.

Patent Owner's contentions are not persuasive. Petitioner notes that Dr. Monroe "did not apply Petitioner's, Patent Owner's, or the Board's constructions, and in fact had no opinion on what the term 'intercepting' requires." Reply 14 (citing Ex. 1066, 124:23–127:13, 132:8–13). As set forth above, "interception" does not include an element of intent. See II.A.1. *supra*. Furthermore, no party proposed an "intent" element in the construction of the "interception" limitation in this proceeding. Pet. 9–10; PO Resp. 4 (listing both parties' claim construction proposals). Finally, we construed "interception" as it appears in the claims, i.e., "following *interception of the request* and a determination that the second network device is available for the secure communications service." Emphasis added. In section II.A.1., we construed the term to mean "receiving a request pertaining to a first entity at another entity." No intent element is present.

As touched on above, we find that Beser teaches two "interceptions." First, Beser's "request pertains to terminating device 26 but is received by network device 14, it is intercepted by network device 14." See Reply 12, Pet. 37. Second, "[i]f network device 14 determines the request needs special processing by detecting a unique sequence of bits in the packet, (Ex. 1007 at 8:34-43), network device 14 forwards the request, where it is received by trusted device 30." See *id.* at 12–13, Pet. 37 (citing Ex. 1007, 8:3–7, 8:48-49, Figs. 4, 6). Thus, both network device 14 and trusted-third-party device 30 "intercept" the "request to look up an internet protocol (IP) address."

We have discretion to weigh expert testimony. See *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1584 (Fed. Cir. 1996) (expert testimony

may be used only to help the court come to the proper understanding of the claims; it may not be used to vary or contradict the claim language). Our construction is based on the specification and plain and ordinary meaning of the claims. Compare II.A.1. to Ex. 1005 ¶ 98. In addition, we choose not to give weight to the deposition testimony because we agree that Dr. Tamassia “was at that point explaining the rationale underpinning his construction, and was neither proposing nor applying a different construction.” See Reply 15 (citing Ex. 2019, 79:9–80:13, 85:9–12, Ex. 1005 ¶ 97).

Even if “intercepting” were found to require receiving a request “intended for” another entity, that feature is disclosed by Beser. Beser discloses that the trusted device 30 evaluates the request by checking an internal table of secure devices (Ex. 1007, 11:45–58), which is the same process shown in the ’131 patent (Ex. 1003, 40:38–41).

c. Features not Shown as Arranged in the Claims

Patent Owner’s next argument is that Petitioner improperly relies on an “overlapping set of elements in Beser for two separate claimed features.” PO Resp. 36–38. Specifically, Patent Owner points to steps or limitations of claims 1 and 15 that recite “receiving.” Patent Owner points to the “interception” step of claim 15, which recites “receiving” followed by: “an indication that the second network device is available for a secure communications service, the requested IP address of the second network device, and provisioning information for a secure communication link.” *Id.* at 36. Patent Owner contends that Petitioner relies on receipt of “the private IP address of the terminating end device” to address both receiving “an indication” and receiving “the private IP address.” PO Resp. 36–37 (citing Pet. 41). Patent Owner argues using a single disclosed element in a prior art

reference cannot be used to teach “each and every element as set forth in the claims.” *Id.* at 37 (citing *In re Robertson*, 169 F.3d 743 (Fed. Cir. 1999) (other citations omitted)).

Petitioner asserts that Patent Owner’s analysis is wrong. Reply 15. We agree. First, as to receiving provisioning information, Beser is not what Petitioner relies on. The Petition alleges receiving provisioning information “would have been an obvious variation of Beser in view of RFC 2401.” Pet. 42. The Petition continues and alleges “a person of ordinary skill in the art would have considered it obvious to encrypt all IP traffic in the Beser IP tunneling scheme to include end-to-end encryption.” *Id.* The actual provisioning information sent and received is alleged to be either the packet sent between originating network device 24 and the first network device 14 of Beser, not “the private IP address of the terminating end” Patent Owner alleges, or the encryption key of RFC 2401. *Id.* at 43; PO Resp. 36–37 (citing Pet. 41).

As to receiving “an indication,” the Petition alleges “Beser’s originating device 24 sends out a tunneling request, it receives the private IP address of the terminating device 26 *as well as its own private IP address*.” See Reply 16 (citing Pet. 40–42; Ex. 1007, 21:48–62) (emphasis added). The Petition alleges this is an “indication” that the IP tunnel in Beser is able to communicate and ready for secure communication with the second device. *Id.* at 41 (citing Ex. 1005 ¶¶ 113, 379), Reply 16 (citing Pet. 40–42; Ex. 1007, 21:48–62). As with provisioning information, the Petition does not rely solely on receipt of “the private IP address of the terminating end device.”

Concerning receiving the IP address of the second device, the Petition cites to the teaching of Beser that “[t]he assignment of private network addresses to the ends of the tunneling association may also include transmitting the private network addresses to the network devices at the ends of the tunneling association where the private network addresses are stored on these end devices.” Pet. 41 (citing Ex. 1007, 21:48–52). The Petition cites to the preceding to conclude “[t]he originating end device therefore receives the private IP address of the terminating end device.” *Id.* (citing Ex. 1007, 14:57–62, 21:48–52; Ex. 1005 ¶ 378), Reply 16 (citing Pet. 41–42). While this step of claim 15 is met by “the private IP address of the terminating end device” Patent Owner alleges is problematic, it is the single instance of use.

We also note that the primary disclosure in the ’131 patent which would support the “receiving” steps is related to transmitting and receiving “TARP packets.” *See, e.g.*, Ex. 1003, 10:56–11:9, 13:36–44, 16:32–34, 19:32–37, 37:36–40. Beser also contemplates the transmission and receipt of IP or data packets. Ex. 1007, 4:2–5, 5:56–58, 7:5–9, 9:49–51. As cited in the Petition, Dr. Tamassia also relies on Beser’s packet transmissions for these limitations. *See* Ex. 1005 ¶ 378 (citing Ex. 1007, 21:48–62). Thus, we are persuaded that the claimed “receiving” steps are met by the transmission and receipt of packets.

d. Combination of Beser and RFC 2401

Petitioner provides several reasons explaining why an artisan of ordinary skill would have used end-to-end encryption, as disclosed and suggested by RFC 2401, in Beser’s similar network system, for example, to provide enhanced data security and anonymity in networks having similar

topology. Pet. 30–34. Petitioner notes that Beser itself suggests the encryption of data using the IPsec protocol, the same encryption protocol that RFC 2401 defines. *Id.* at 30 (citing Ex. 1007, 1:54–56; Ex. 1005 ¶¶ 421–423, 433). Petitioner argues Beser also describes its IP tunneling as compliant with standards, such as IPsec. *Id.* (citing Ex. 1007, 4:55–5:2; Ex. 1005 ¶¶ 320–321, 323, 424, 432, 436). Petitioner also argues Beser teaches that IP tunnels should ordinarily be encrypted. *Id.* (citing Ex. 1007, 1:54–56, 11:22–25, 18:2–5; Ex. 1005 ¶¶ 421–23, 427–28).

Petitioner concludes “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.” Pet. 31 (citing Ex. 1005 ¶¶ 427, 431; Ex. 1007, 1:54–56, 2:12–14; 11:22–25, 18:2–5, 20:11–14). Further, Petitioner concludes a person of ordinary skill would be 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.* (citing Ex. 1005 ¶¶ 427–428, 431, 437; Ex. 1007, 1:54–56; Ex. 1008).

Petitioner alleges a person of ordinary skill would have recognized RFC 2401 could be incorporated into the Beser system. Pet. 31 (citing Ex. 1005 ¶¶ 431–432, 436–38). In support of this premise, Petitioner notes that RFC 2401 in its “case 3” example “shows precisely the same network topology as Beser, with one tunnel between two security gateways such as edge routers, and another tunnel between the two end devices.” *Id.* at 31–32 (comparing Ex. 1008, 25 with Ex. 1007, Fig. 1; Ex. 1005 ¶¶ 434–435).

Patent Owner argues that Beser and RFC 2401 would not have been combined as asserted by Petitioner. PO Resp. 38–44. Patent Owner

contends that Beser explains that prior art Internet security systems “suffered from certain disadvantages.” *Id.* at 38–39 (citing Ex. 2018 ¶ 58); *see also* Ex. 1007, 1:54–2:35, 1:62–63 (describing the disadvantages of the prior art)). Patent Owner asserts we were under a “misunderstanding of *Beser*” in the Institution Decision where we preliminarily found that such problems could be overcome by providing more computer power. *Id.* at 39 (citing Ex. 2018 ¶ 60).

In support of the alleged misunderstanding, Patent Owner contends that Beser notes the problems with allocating more computing power to encryption, such as “jitter, delay, or the loss of some packets,” and, therefore, “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 39–40 (citing Ex. 1007, 1:60–67; Ex. 2018 ¶ 60). Patent Owner also contends that Beser only “proposes a method of hiding the addresses of originating and terminating devices”:

By hiding the identities of the network devices in this manner, *Beser* touts that its method is able to *increase* communication security *without increasing* computational burden. ([Ex. 1007,] 2:[38]–3:14.) Thus, one of ordinary skill in the art would understand that *Beser* is directed to providing a method for securing communications *other than* encryption. (See Ex. 2018 at ¶ 62.)

PO Resp. 40–41.

Patent Owner also disputes that Beser discloses that “IP tunnels are and should ordinarily be encrypted” because that statement relates to the prior art systems and not Beser. PO Resp. 41 (citing Ex. 2018 ¶ 63). The IPSec protocol also appears in the Background of the Invention. *Id.* (citing Ex. 1007, 1:54–67; Ex. 2018 ¶ 64).

Patent Owner explains that “*Beser* also teaches that encryption does not deter a determined hacker from deducing source and identity information, and so, once the tunnel is established, *Beser* eschews encryption in favor of hiding the identities within the tunnel.” PO Resp. 42. According to Patent Owner, 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.” *Id.* (citing Ex. 2018 ¶ 65). Patent Owner concludes “*Beser* acknowledges that in certain systems, certain types of *encryption cannot be used*” and *Beser* discloses security without encryption. *Id.* at 41–42 (citing Ex. 2018 ¶ 66).

We agree with Petitioner that a person of ordinary skill in the art would have understood that *Beser* alone teaches encryption. See Pet. 30. Accordingly, we do not agree with Patent Owner’s description of what a person of ordinary skill would have understood from *Beser*’s disclosure. Although *Beser* recognizes that the use of encryption may cause challenges, we find that *Beser* suggests that such problems may be overcome by providing more computer power and/or less quality. See Ex. 1007, 1:60–67. For example, *Beser* teaches that 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.” *Id.* at 1:63–65. Moreover, *Beser* never states that its technique of hiding addresses is intended as replacing, as opposed to supplementing, known security techniques such as encryption. In fact, *Beser* implies that a good system will allow multiple types of security solutions to

be used at the same time, by 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).

We credit testimony by Dr. Tamassia stating that “[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” and that such a person “would recognize that the concerns expressed in Beser . . . can be easily resolved by simply using more powerful equipment.” Ex. 1005 ¶¶ 427–428, Reply 3. Dr. Tamassia’s conclusion is supported by explanation and citation to the record. *Id.* ¶¶ 421–428 (citing Ex. 1007, *passim*; Ex. 1008, 7, 25). Dr. Monroe’s testimony does not persuade us to the contrary as it largely echoes Patent Owner’s unpersuasive attorney argument. *Compare* Ex. 2018 ¶¶ 57–66 with PO Resp. 38–44. We find that Beser, at most, mildly criticizes (tempered by an implied solution) a specific type of tunneling that employs encapsulation, encryption, and VoIP packets—i.e., “due to computer power limitations, this form of tunneling may be inappropriate for the transmission of multimedia or VoIP packets.” Ex. 1007, 2:15–17. In other words, Beser at least suggests that with adequate power or typical data transmissions, a tunnel (a VPN according to Beser) and encryption would be appropriate for providing security. Therefore, we find that Beser does not discourage encrypting data to make it secure; rather, Beser provides a solution for providing anonymity by using a tunnel technique with or without encryption of data, and if necessary, increasing computer power as needed.

Thus, notwithstanding Patent Owner’s arguments, a preponderance of evidence supports a finding that a person of ordinary skill reading Beser at

the relevant time would have understood that encryption should ordinarily be used to protect the contents of the communications in an IP tunnel. Petitioner, thus, establishes by a preponderance of the evidence that a person of ordinary skill would have found it obvious to combine the teachings of RFC 2401 with those of Beser to encrypt data in order to enhance data security in a tunnel that provides anonymity, based on a determination that a requested target device would have been available for a secure communication.

We determine Petitioner has shown by a preponderance of the evidence that claims 1 and 15 would have been obvious over Beser combined with RFC 2401.

H. Claims 3 and 16

Petitioner asserts that the combination of Beser and RFC 2401 teaches each of the limitations of claims 3 and 16. Pet. 49–50. Claims 3 and 16 depend from claims 1 and 15 respectively. The limitation in both is represented by claim 16’s recitation of “encrypting at least one of the video data and the audio data over the secure communication link.”

Petitioner argues:

a person of ordinary skill in the art would have considered it obvious to encrypt all IP traffic in the Beser IP tunneling scheme to include end-to-end encryption 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.

Pet. 49–50 (citing Pet. 30–34). Pages 30 through 34 of the Petition discusses under the heading “1. A Person of Ordinary Skill Would Have Found it Obvious to Encrypt IP Traffic in the Beser Scheme Based on the Teachings in Beser and RFC 2401.” *Id.* at 3. We also found in section II.G.2.d., above,

that a person of ordinary skill would have combined RFC 2401 with Beser to encrypt data in order to enhance data security in a tunnel that provides anonymity, based on a determination that a requested target device would have been available for a secure communication. Petitioner concludes it would have been obvious over Beser and RFC 2401 to encrypt audio and video data “*over the secure communications service.*” Pet. 50.

Patent Owner argues claims 3 and 16 are patentable for the same reasons we declined to accept in connection with claims 1 and 15. PO Resp. 44. Patent Owner then contends that “*Beser teaches away from using encryption, and Petitioner has not shown that one of ordinary skill in the art would combined the teachings of Beser with the encrypted tunnel of RFC 2401.*” *Id.* at 45 (citing PO Resp. 38–44). Pages 38 through 44 of the Response are Patent Owner’s arguments contending a person of ordinary skill would not have combined Beser and RFC 2401. As previously discussed, we rejected those arguments.

We determine Petitioner has shown by a preponderance of the evidence that claims 3 and 16 would have been obvious over Beser combined with RFC 2401.

I. Claim 10

Claim 10 depends from method claim 1 and recites additionally that “the secure communication link is a virtual private network link.” As discussed above, we construed “virtual private network link” to mean “a transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or

more of authentication, encryption, or address hopping that includes a portion of a public network.” *See* II.A.2. *supra*.

We agree with Petitioner’s analysis of claim 10. *See* Pet. 54–55. Patent Owner’s arguments are based on its proposed claim construction argument that a “virtual private network link” is “a path between two devices in a *virtual private network*.” *See* PO Resp. 18 (emphasis added). As noted above, we did not adopt Patent Owner’s claim construction. Specifically, Patent Owner argues “Beser is not just silent on whether its tunnel is a VPN communication link,¹⁵ Beser expressly teaches that its tunnel is not a VPN communication link.” *Id.* at 46 (citing Ex. 1007, 2:6–8, 2:43–66; Ex. 2018 ¶ 68).

Patent Owner’s arguments regarding the “virtual private network link” are essentially a repeat of its arguments that Beser and RFC 2401 would not have been combined as asserted by Petitioner. *See* PO Resp. 46. As discussed above, we do not agree with these arguments. We are not persuaded to the contrary by Dr. Monroe’s testimony on the issue, which largely mirrors Patent Owner’s Response. *See* PO Resp. 46; Ex. 2018 ¶ 68. To the extent that Beser criticizes VPN’s, we find that these statements refer explicitly to prior art VPN methods (*see* Ex. 1007, 2:6–17 (discussing the prior art in the BACKGROUND OF THE INVENTION section of the specification)). This language does not diminish Petitioner’s evidence that a person of ordinary skill in the art would find obvious the claimed “virtual private network link” based on the combined teachings of Beser and RFC 2401.

¹⁵ “VPN communication link” is a term from claims of related patents but is not in the claims of the ’131 patent.

Patent Owner argues claim 10's "virtual private network link" limitation is not shown by the combination of Beser and RFC 2401. But Patent Owner's argument is not based on any construction of "virtual private network link."

We determine Petitioner has shown by a preponderance of the evidence that claim 10 would have been obvious over Beser combined with RFC 2401.

J. Claims 2, 4–9, 13–14, 17–22, and 25–27

Petitioner asserts that the combination of Beser and RFC 2401 teaches each of the limitations of claims 2, 4–9, 13, 14, 17–22, and 25–27. We have reviewed Petitioner's evidence regarding these claims. *See* Pet. 50–57. According to Petitioner, Beser suggests each of the limitations added to independent claims 1 and 15 by the challenged dependent claims 2, 7, 14, 20, 22, and 27. *Id.* at 50–51, 57.

Claims 4 and 17 depend from claims 1 and 15 respectively, which were shown by the combination of Beser and RFC 2401. Claims 4 and 17 specify that the secure communications service includes a "telephony service." Petitioner cites to Beser's teaching that "the originating and terminating end devices can be 'telephony devices' including 'VoIP devices (portable or stationary) or personal computers running facsimile or audio applications.'" Pet. 50 (citing Ex. 1007, 4:43–52, Figs. 1 and 17).

Claims 5 and 18 depend from claims 4 and 17, respectively, and add as a limitation the telephony service uses "modulation." Claims 6 and 19 depend from claims 5 and 18, respectively, and recite "the modulation is based on one of frequency-division multiplexing (FDM), time-division multiplexing (TDM), or code division multiple access (CDMA)."

For the modulation limitation of claims 5 and 18, Petitioner first cites to Beser’s teaching that the first and second network device each can be a cable modem. Pet. 51 (citing Ex. 1007, 4:30–42). Petitioner then relies on the Tamassia Declaration for the types of modulation recited in claims 6 and 19, contending “[i]t was well known before February of 2000 that data transmitted via a cable modem inherently will be modulated, and that cable modems used various types of modulation, including FDM and TDM.” *Id.* (citing Ex. 1005 ¶ 335).¹⁶

Claims 8 and 21 depend from claims 7 and 20, which depend from claims 1 and 15 respectively. As detailed above, we find the limitations for claims 1 and 15 were shown by the combination of Beser and RFC 2401. As also stated above, the limitations of claims 7 and 20 are suggested by Beser.

Claims 8 and 21 further specify that the mobile device is “a notebook computer.” Petitioner alleges Beser teaches the originating and terminating end devices can be “personal computers.” Pet. 52 (citing Ex. 1007, 4:47–49; Ex. 1005 ¶ 327). Petitioner alleges “[a] person of ordinary skill in February 2000 would have understood that a ‘personal computer’ included both

¹⁶Petitioner alleges the effective filing date of the ’131 patent claims is no earlier than February 15, 2000. Pet. 7. Patent Owner does not dispute the allegation in this proceeding. Petitioner’s supporting evidence includes that the limitation “domain name” in claims 1 and 15 is first supported in U.S. Application 09/504,783 (now U.S. Patent 6,502,135), a prior related application filed on February 15, 2000. *Id.* at 7; see Ex. 1003, (63). Petitioner cites numerous other proceedings where “Patent Owner has not disputed that claims reciting a ‘domain name’ are not entitled to an effective filing date prior to February 15, 2000.” *Id.* at 7–8. We find that the record supports that, for purposes of this case, the effective filing date of the ’131 patent is February 15, 2000.

desktop and portable laptop computers (*i.e.*, notebook computers).” *Id.* (citing Ex. 1005 ¶ 327). Petitioner alleges “[i]t would have been obvious to a person of ordinary skill in the art to use a notebook computer because of its greater mobility.” *Id.* (citing Ex. 1005 ¶ 327).

Claims 9 and 26 depend from claims 1 and 15 respectively, which claims we have already determined are unpatentable. Claims 9 and 26 both recite “wherein the interception of the request consists of receiving the request to determine that the second network device is available for the secure communications service.” Petitioner alleges “[c]onfiguring the trusted-third-party network device to handle such an error condition [the second network device is not available for secure communication] would have been a simple engineering design choice, which would have been routinely made by a person of ordinary skill in the art.” Pet. 53 (citing Ex. 1005 ¶ 364).

Petitioner explains several alternatives that might occur depending on whether the unique identifier is recognized by the trusted-third-party device. *Id.* In any event, “if the unique identifier is not registered, the trusted-third-party network device would not negotiate an IP tunnel.” *Id.* (citing Ex. 1005 ¶ 363). Alternatively, Petitioner alleges that “if the trusted-third-party network device determines that the unique identifier in a request specifies a destination that can establish a secure tunnel, it will negotiate with the first and second network devices to establish the IP tunnel between those network devices.” Pet. 54 (citing Ex. 1007, 9:6–11, 9:26–30, 11:9–44; Ex. 1005 ¶ 368). In this scenario, the methods of Beser are performed and the same “determination” disclosed in the ’131 patent is undertaken. *Id.* (citing Ex. 1003, 40:39–45).

Claims 13 and 25 depend from claims 1 and 15 respectively, which we have already determined are unpatentable. Claims 13 and 25 recite “wherein the indication that the second network device is available for the secure communications service is a function of the result of a domain name lookup.” Petitioner alleges that if the trusted-third-party device determines the unique identifier specifies a destination that can establish a secure tunnel, the trusted-third-party network device will negotiate with the first and second network devices to establish the IP tunnel between those network devices. Pet. 55–56 (citing Ex. 1007, 9:6–11; 9:26–30, 11:9–44; Ex. 1005 ¶¶ 368). Alternatively, Petitioner contends that “if the unique identifier in a request is not recognized by the trusted-third-party network device or does not map to a device requiring negotiation of an IP tunnel, the trusted-third-party network device will not negotiate private IP addresses.” *Id.* at 56 (citing Ex. 1005 ¶¶ 364–67; Ex. 1003, 39:36–38). In either event, “[t]he ‘indication’ in Beser is therefore a function of the outcome of the trusted-third-party network device’s lookup in its internal database (*‘a function of the result of a domain name lookup’*).” *Id.*

In its Response, Patent Owner does not make specific arguments directed to the challenged dependent claims and instead argues that “*Beser* and RFC 2401 do not render obvious claims 2, 4-9, 13, 14, 17-22, and 25-27 for at least the reasons discussed above for independent claims 1 and 15, from which they depend.” PO Resp. 46.

We have reviewed both parties’ arguments and supporting evidence, including the disclosure of both references and the testimony of Dr. Tamassia and we agree with and adopt Petitioner’s analysis. Thus, we determine that Petitioner has shown, by a preponderance of the evidence,

that a person of ordinary skill in the art would have found dependent claims 2, 4–9, 13, 14, 17–22, and 25–27 obvious over Beser and RFC 2401.

K. Patent Owner’s Motion to Exclude

Patent Owner seeks to exclude Exhibits 1001, 1002, 1004, 1006, 1010–1041, 1043–1048, 1050–1054, 1060, 1063–1065, and 1069–1071, and Portions of Exhibit 1005. Mot. 1, Paper 30. As movant, Patent Owner has the burden of proof to establish that it is entitled to the requested relief. See 37 C.F.R. § 42.20(c). For the reasons stated below, Patent Owner’s Motion to Exclude is either *denied* or *dismissed*.

1. Exhibits 1060 and 1063–65

Patent Owner seeks to exclude Exhibits 1060 and 1063–65 as inadmissible hearsay. Paper 30, 2. Exhibit 1060 is a declaration originally submitted in litigation before the International Trade Commission. Ex. 1060. It contains testimony from Sandy Ginoza, a representative of IETF, in support of Petitioner’s contention that RFC 2401 qualifies as a printed publication as of November 1998. *Id.* Exhibit 1063 is a “transcript of Ms. Ginoza’s February 8, 2013 deposition that was taken as part of the ITC action.” Paper 30, 2 (quoting Paper 14, 5–6). Exhibits 1064 and 1065 are both magazine articles dated 1999 that relate to this same issue. Paper 14, 6–7. All four exhibits were entered into the record upon Petitioner’s Motion to Submit Supplemental Information Pursuant to 37 C.F.R. § 42.123(a). Paper 17; Paper 21.

Because we do not rely on any of these Exhibits to decide the issue of whether RFC 2401 qualifies as a printed publication, we dismiss this request as moot.

2. *Exhibits 1001, 1002, 1004, 1006, 1010–1035, 1037–1041, 1043–1048, 1050–1054, 1069, and 1071*

Patent Owner seeks to exclude the above listed exhibits as lacking relevance. Mot. 3. Exhibit 1036 is relevant to our discussion of RFC 2401 in section II.D. As to the remaining exhibits, because we do not rely on any evidence subject to the motion, the listed exhibits are irrelevant and we dismiss this request as moot.

3. *Portions of Exhibit 1005*

Patent Owner seeks to exclude portions of Dr. Tamassia's testimony in Exhibit 1005 as lacking relevance because they relate to Aventail. Paper 30, 4. Aventail is a reference relied on by Petitioner in IPR2015-00811 but not here. Because we do not rely on any paragraphs of Exhibit 1005 subject to the motion, the cited portions of Dr. Tamassia's testimony are irrelevant and we dismiss this request as moot.

4. *Exhibit 1036*

Patent Owner moves to exclude Exhibits based on the following argument: "Exhibits 1002–1004, 1006, 1010–1041, 1043–1048, 1050, 1051, 1053, 1069, and 1071 because *one or more of these exhibits* includes evidence that is inadmissible hearsay or the evidence in these exhibits is irrelevant to the instant proceeding." Paper 30, 1 (emphasis added). Patent Owner also argues as follows: "Exhibits 1002–1004, 1006, 1010–1041, 1043–1048, 1050, 1051, 1053, 1069, and 1071 should be excluded because they lack relevance." *Id.* at 5.

As indicated in the first above-quoted argument, Patent Owner does not argue specifically that Exhibit 1036 includes evidence of hearsay, because that argument applies to "one or more" of the other listed Exhibits.

Furthermore, Patent Owner does not explain why anything in Exhibit 1036 includes hearsay. *See* Paper 30, 1. Accordingly, Patent Owner fails to meet its burden on its Motion to Exclude Exhibit 1036 based on hearsay. *See* 37 C.F.R. § 42.20(c).

Patent Owner's second above-quoted argument is based on an asserted lack of relevance as to all the listed Exhibits, including Exhibit 1036. Patent Owner does not explain why Exhibit 1036 is not relevant. Therefore, Patent Owner fails to carry the burden on its Motion to Exclude Exhibit 1036. *See* 37 C.F.R. § 42.20(c). Furthermore, as discussed above, Dr. Tamassia relies on Exhibit 1036, and it provides evidence of procedures used in the publication of RFC documents. Therefore, Exhibit 1036 is relevant to show the public availability of RFC 1041. Accordingly, based on the foregoing discussion, we *deny* the Motion to Exclude Exhibit 1036

ORDER

For the reasons given, it is:

ORDERED that claims 1–10, 13–22, and 25–27 of U.S. Patent No. 8,516,131 B2 have been shown by a preponderance of the evidence to be unpatentable;

FURTHER ORDERED, Patent Owner's Motion to Exclude is *denied* as to Exhibit 1036 and *dismissed* as moot as to all remaining exhibits; and

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

IPR2015-00868
Patent 8,516,131 B2

PETITIONER:

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

PATENT OWNER:

Joseph E. Palys
Naveen Modi
Daniel Zeilberger
Chetan Bansal
PAUL HASTINGS LLP
josephpalys@paulhastings.com
naveenmodi@paulhastings.com
danielzeilberger@paulhastings.com
chetanbansal@paulhastings.com

Jason E. Stach
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
jasonstach@finnegan.com