UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-00811
Patent 8,868,705

PATENT OWNER VIRNETX INC.'S NOTICE OF APPEAL

Director of the United States Patent and Trademark Office
c/o Office of the General Counsel
Madison Building East, 10B20
600 Dulany Street
Alexandria, VA 22314-5793

Notice is hereby given, pursuant to 37 C.F.R. § 90.2(a), that Patent Owner VirnetX Inc. ("VirnetX") appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision entered on September 8, 2016, (Paper 44) (the "Final Written Decision") by the United States Patent and Trademark Office, Patent Trial and Appeal Board (the "Board"), and from all underlying orders, decisions, rulings, and opinions. A copy of the Final Written Decision is attached.

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), VirnetX indicates that the issues on appeal include, but are not limited to, the Board's determination of unpatentability of claims 1-34 of U.S. Patent No. 8,868,705 under 35 U.S.C. § 103, and any finding or determinations supporting or related to those rulings including, without limitation, the Board's application of the broadest reasonable interpretation standard, the Board's interpretations of the claim language, and the Board's interpretation of the references.

Simultaneous with this submission, a copy of this Notice of Appeal is being filed with the Board. In addition, the Notice of Appeal and the required fee are

being filed electronically with the Clerk of Court for the United States Court of Appeals for the Federal Circuit.

Respectfully submitted this 9th day of November, 2016.

By: /Naveen Modi/
Naveen Modi
Registration No. 46,224
Paul Hastings LLP
875 15th Street, N.W.
Washington, DC 20005
(202) 551-1700
naveenmodi@paulhastings.com

Counsel for VirnetX Inc.

CERTIFICATE OF SERVICE

The undersigned certifies that, in addition to being filed electronically through Patent Trial and Appeal Board End to End (PTAB E2E), the original version of this Notice of Appeal was filed by hand on November 9, 2016 with the Director of the United States Patent and Trademark Office, at the following address:

Director of the United States Patent and Trademark Office
c/o Office of the General Counsel
Madison Building East, 10B20
600 Dulany Street
Alexandria, VA 22314-5793

The undersigned also certifies that a true and correct copy of this Notice of Appeal and the required fee were filed electronically via CM/ECF on November 9, 2016, with the Clerk of Court for the United States Court of Appeals for the Federal Circuit.

The undersigned also certifies that a true and correct copy of this Notice of Appeal was served on November 9, 2016 on counsel of record for Petitioner Apple Inc. by electronic mail (by agreement of the parties) at the following address:

iprnotices@sidley.com
Sidley Austin LLP
1501 K Street, N.W.
Washington, DC 20005

Date: November 9, 2016

By: /Naveen Modi/

Naveen Modi
Registration No. 46,224
Paul Hastings LLP
875 15th Street, N.W.
Washington, DC 20005
(202) 551-1700
naveenmodi@paulhastings.com

Counsel for VirnetX Inc.

Trials@uspto.gov
571-272-7822

Paper No. 44
Entered: September 8, 2016

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-00811
Patent 8,868,705 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 1–34 of U.S. Patent No. 8,868,705 B2 (Ex. 1001, "the '705 patent"). VirnetX Inc. ("Patent Owner")[1] filed a Preliminary Response. Paper 6 ("Prelim. Resp."). On September 11, 2015, we granted the Petition and instituted trial on claims 1–34 of the '705 patent. Paper 8 ("Institution Decision" or "Inst. Dec.")

After institution of trial, Patent Owner filed a Patent Owner Response (Paper 25, "PO Resp."), and Petitioner filed a Reply (Paper 29, "Pet. Reply"). In addition, Petitioner proffered the Declaration of Dr. Roberto Tamassia ("Tamassia Declaration," Ex. 1005). The deposition of Dr. Tamassia was taken by Patent Owner and the deposition transcript was filed by both parties. ("Tamassia Deposition," Ex. 1068).[2] Patent Owner proffered the Declaration of Dr. Fabian Monrose. ("Monrose Declaration," Ex. 2016).[3] The deposition of Dr. Monrose was taken in this proceeding ("Monrose Deposition," Ex. 1066).

An oral hearing was held on June 8, 2016. The transcript of the hearing has been entered into the record. Paper 43 ("Tr.").

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

---

[1] The Petition also names Science Application International Corporation as Patent Owner. However, the Patent Owner Response names only VirnetX.
[2] Patent Owner filed the Tamassia Deposition transcript as Exhibit 2015. We refer only to Ex. 1068 unless otherwise noted.
[3] Patent Owner also filed a Declaration of Dr. Monrose from *Apple Inc. v. VirnetX Inc.*, IPR2014-00237 ("'237 IPR") ("Monrose Declaration '237," Ex. 2001). Patent Owner does not cite to Exhibit 2001.

reasons that follow that Petitioner has shown by a preponderance of the evidence that claims 1–34 of the ’705 patent are unpatentable

A. The ’705 Patent

The ’705 patent describes a system and method for transparently creating an encrypted communications channel between a client device and a target device. Ex. 1001, 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 40:66–41:9. Figure 26 of the ’705 patent is reproduced below.

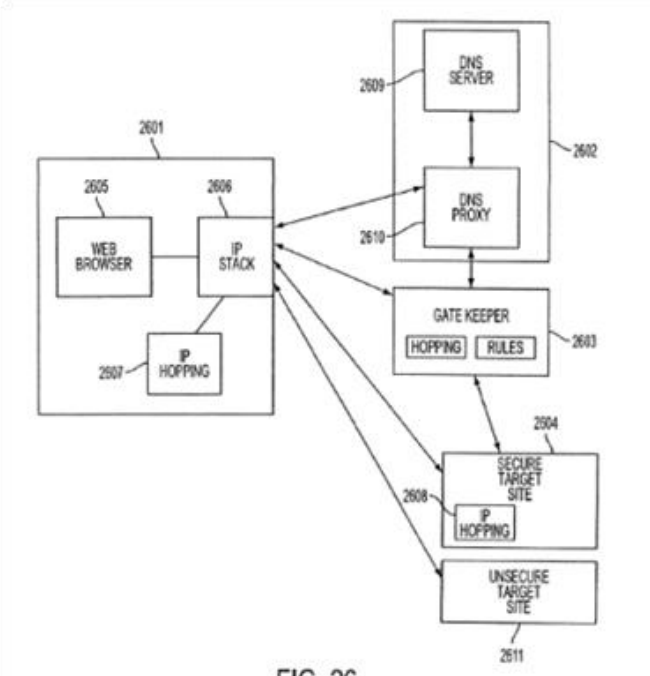

FIG. 26

Referring to Figure 26, user’s computer 2601 is a conventional client, e.g., a web browser. Ex. 1001, 39:58–60. Gatekeeper server 2603 is interposed between modified Domain Name Server (“DNS”) 2602 and secure target

site 2604. *Id.* at 39:62–66. 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 39:66–67.

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. 1001, 40:1–19. 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 40:1–29. Gatekeeper 2603 facilitates and allocates the exchange of information for secure communication, such as using "hopped" IP addresses. *Id.* at 40:32–35.

The DNS proxy server handles requests for DNS look-up for secure hosts. Ex. 1001, 40:43–45. If the host is secure, then it is determined whether the user is authorized to connect with the host. *Id.* at 40:51–53. 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 40:66–41:2.

B. Illustrative Claim

Petitioner challenges claims 1–34 of the '705 patent. Claim 1 is an independent method claim and claim 21 is an independent system claim. All remaining claims depend directly or indirectly from claim 1 or 21. Claim 1 is reproduced below.

> 1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the

target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:

(1) 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;

(2) determining whether the request to look up the IP address transmitted[4] in step (1) corresponds to a device that accepts an encrypted channel connection with the client device; and

(3) in response to deterring in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel.

Ex. 1001, 55:43–67.

C. Instituted Grounds of Unpatentability

We instituted on the following grounds asserted by Petitioner under 35 U.S.C. § 103: (1) claims 1–3, 6, 14, 16–25, 28, 31, 33, and 34 as obvious

[4] Patent Owner asserts "transmitted" was printed in error and that the limitation was amended to include "intercepted" instead of "transmitted." Prelim. Resp. 30 n.3 (citing Ex. 1002, 638–639, 641, 655–656). In our Order dated December 9, 2015 (Paper 24), we authorized Patent Owner to file a request for a certificate of correction changing the word "transmitted" in claims 1 and 21 to "intercepted." Paper 24, 3. In addition, we observed that the parties stipulated that the change of wording was not of patentable significance. *Id.* Patent Owner filed a Certificate of Correction. Ex. 2017.

under 35 U.S.C. § 103 over Aventail[5] and RFC 2401[6]; (2) claims 8–10, 12, 15, 30, and 32 as obvious under 35 U.S.C. § 103 over Aventail, RFC 2401, and RFC 2543[7]; (3) claims 4, 5, 7, 26, 27, and 29 as obvious under 35 U.S.C. § 103 over Aventail, RFC 2401, and Brand[8]; and (4) claims 11 and 13 as obvious under 35 U.S.C. § 103 over Aventail, RFC 2401, RFC 2543, and Brand. Inst. Dec. 24.

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, 2142 (2016) (affirming the Patent Office's authority to issue regulations establishing and governing *inter partes* review under 35 U.S.C. § 316(a)(4)). Under this standard, absent any special definitions, claim terms or phrases are given their

---

[5] Exhibits 1009–1011 are manuals documenting software created by Aventail Corporation. Both parties use "Aventail" in citing to the documentation for the client software, Exhibit 1009. Exhibit 1009 is the primary exhibit cited. We will use "Aventail" or "Aventail Connect" when referring to Exhibit 1009. *See* Aventail Connect v3.01/v2.51 Administrator's Guide (Ex. 1009), Aventail Connect v3.01/v2.51 User's Guide (1996-1999) (Exhibit 1010), and Aventail ExtraNet Center v3.0 Administrator's Guide (NT and UNIX) (Exhibit 1011).

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

[7] Handley, M., et al., *SIP: Session Initiation Protocol*, published March 1999 ("RFC 2453," Ex. 1013).

[8] US 5,237,566, issued Aug. 17, 1993, to Robert C. Brand and Stanford L. Mantiply ("Brand," Ex. 1012).

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 similar claim terms in the Final Written Decision for the '237 IPR. *See* '237 IPR, slip op. 5–15 (PTAB May 11, 2015) (Paper No. 41) ("'237 FWD"). *See also VirnetX, Inc. v. Cisco Systems, Inc*., 767 F.3d 1308, 1317–19 (Fed. Cir. 2014) (addressing ancestor *VirnetX* patents having similar claim terms).

Petitioner and Patent Owner each proffer proposed constructions of several claim terms. *See* Pet. 8–14, PO Resp. 2–15. Both parties argue for the construction of four terms: "secure domain name" (PO Resp. 4–8, Pet. Reply 2–3); "encrypted communications channel" (PO Resp. 8–10, Pet. Reply 3); "provisioning information" (PO Resp. 10–13, Pet. Reply 4); and "intercept[ing] . . . a request to look up an Internet Protocol (IP) address" (PO Resp. 13–15, Pet. Reply 4). Our review of Patent Owner's arguments confirms these four terms form the basis for Patent Owner's patentability arguments. *See* PO Resp. 23, 25, 26, 28.

The additional terms proposed initially for construction in the Petition are: "domain name;" "modulated/unmodulated transmission;" and "phone." *See* Pet. 10, 13–14. As of now, these terms are not in dispute and construction is not required to resolve the issues before us. We do not identify any additional terms for construction.

1. "secure domain name" (claims 3, 10, 25)

Dependent claims 3 and 10 depend respectively from claims 1 and 8, which depends from claim 1. Claim 25 depends from claim 21. Claims 3, 10, and 25 each recite "wherein the domain name is a secure domain name." Relying, in part, on a related *inter partes* proceeding, Petitioner argues

"secure domain name" is "a name that corresponds to a secure computer network address." Pet. 11 (citing IPR2015-00481, "'481 IPR").[9] Petitioner contends its proposed construction is consistent with the Specification. *Id.* (citing Ex. 1001, 51:6–42 ("a 'secure domain name' [is] a domain name that corresponds to the secure network address of a secure server 3320"). Petitioner notes additional disclosures from the Specification in support of its construction. *Id.* (citing Ex. 1001, 40:1–7, 7:39–42). Finally, Petitioner refers to testimony from the Tamassia Declaration, which relies on the same portions of the Specification to conclude that the term has "a more general meaning of being a name that corresponds to a particular device on a secure computer network (i.e., one that would have an address on that secure computer network)." *Id.* (citing Ex. 1005 ¶ 73).

Patent Owner acknowledges Petitioner's proposed construction was adopted in the '237 IPR. PO Resp. 4. However, Patent Owner argues "secure domain name" means "a non-standard domain name that corresponds to a secure computer network address and cannot be resolved by a conventional domain name service (DNS)." *Id.* (Table). Patent Owner's proposed construction was an agreed construction from the related district court litigation. *Id.* (citing *VirnetX Inc. v. Apple Inc.*, Case 6:10-cv-00417-LED (E.D. Tex. Dec. 21, 2011), Joint Claim Construction Chart, 19–20, Ex. 2002). Patent Owner cites to the Specification as also supporting its proposal, specifically including that the "secure domain name" is a

[9] The full citation is *Apple Inc. v. VirnetX, Inc.*, IPR2014-00481 ("'481 IPR"), Institution Decision, slip. op. at 8 (PTAB Sept. 3, 2014) (Paper 11); *see also* '481 IPR, Final Written Decision, slip op. at 13–14 (Aug. 24, 2015) (Paper 35) (declining to modify construction).

"nonstandard domain name." *Id.* (citing Ex. 1001, 7:29–31, 7:39–42, 50:22–31, 51:6–10, Figs. 33, 34). Testimony from the Monrose Declaration is also cited as support that "SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses." *Id.* at 5 (citing Ex. 2016 ¶¶ 15–16).[10]

Patent Owner further contends it disclaimed Petitioner's proposed construction in a now completed *inter partes* reexamination of a related patent. PO Resp. 5 (citing Control No. 95/001,270, Response to Office Action, 5 (Apr. 19, 2010), Ex. 2008; Control No. 95/001,270, Right of Appeal Notice, 4 (Dec. 3, 2010), Ex. 2006). Patent Owner acknowledges this is a prosecution history disclaimer argument which "generally only binds the patent owner." *Id.* at 6–7 (citing *Tempo Lighting, Inc. v. Tivoli, LLC*, 742 F.3d 973, 978 (Fed. Cir. 2014)). Patent Owner urges the prosecution history should be consulted in subsequent reviews of the patent in determining the broadest reasonable interpretation. *Id.* at 7 (citing *Microsoft Corp. v. Proxyconn, Inc.*, 789 F.3d 1292, 1298 (Fed. Cir. 2015); *Straight Path IP Grp., Inc. v. Sipnet EU S.R.O.*, 806 F.3d 1356, 1362 (Fed. Cir. 2015)). We start with the language of claims 3, 10, and 25. These dependent claims recite that the domain name is a "secure domain name." The plain meaning of those words is found in Petitioner's proposed construction, "a name that corresponds to a *secure* computer network address." The language is clear and straightforward and any construction

[10] The Monrose Declaration '810 has one opinion based on the Specification, that "[o]ne of ordinary skill in the art would understand based on the disclosure of the '705 patent that to obtain the URL for a 'secure domain name,' 'a secure domain name service (SDNS)' must be queried." Ex. 2016 ¶ 17.

under the broadest reasonable interpretation standard should not lead us away from that clarity. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1314 (Fed. Cir. 2005) (en banc) ("In some cases, the ordinary meaning of claim language as understood by a person of skill in the art may be readily apparent even to lay judges, and claim construction in such cases involves little more than the application of the widely accepted meaning of commonly understood words.").

We turn now to the Specification. The patent may set out a particular meaning of a claim term so long as it does so "with reasonable clarity, deliberateness, and precision." *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). "Without an express intent to impart a novel meaning to claim terms, an inventor's claim terms take on their ordinary meaning." *York Prods., Inc. v. Central Tractor Farm & Family Ctr.*, 99 F.3d 1568, 1572 (Fed. Cir. 1996).

The '705 patent states that "[a]lternatively, software module 3409 can replace the top-level domain name of server 3304 with any other non-standard top-level domain name." Ex. 1001, 50:22–31 (emphasis added). The column 50 quote follows a description of standard domain names like .com, including adding "s" for secure. *Id.* In addition to the preceding, the Specification discloses an example of "replac[ing] the top-level domain name . . . with a secure top-level domain name." Ex. 1001, 50:22–25; *see also id.* at 51:6–42 (a "secure domain name" is a domain name that corresponds to the secure network address of a secure server 3320), 40:1–7 (evaluating domain names in DNS requests to determine whether access to a secure site has been requested), 7:39–42 ("[e]ach secure computer network address is based on a non-standard top-level domain name, such as .scom,

.sorg, .snet, .sedu, .smil and .sint"). Thus, the Specification does not expressly state that the "secure domain name" must be "non-standard," only that it is secure, which is encompassed in Petitioner's proposed construction.

Further, a conventional DNS function involves resolving names into addresses. *See* Ex. 1005 ¶¶ 126–27 ("much like a file system"), 304–306 (citing Ex. 1001, 39:1–3 (describing Conventional DNS functionality)). The Specification includes additional discussion of conventional DNS. For example, the '705 patent contemplates returning different addresses for the same domain name based on a user's security levels, identity, and/or subscription level, and combining conventional DNS and proxy functions. Ex. 1001, 40:20–29, 38–40, 51–57, 51:6–27. Rather than not returning a secure domain name from a conventional DNS based on the type of name itself, the Specification states that a "DNS *proxy*" returns a "host-unknown" "if the user had requested lookup of a secure web site *but lacked credentials to create such a connection*." *Id*. at 40:24–27 (emphases added). Thus, we are not persuaded to depart from the plain and ordinary meaning of the term previously discussed.

Next we address Patent Owner's prosecution history disclaimer argument. We consider the prosecution history, if raised, in construing claim terms. *Philips*, 415 F.3d at 1317 ("[T]he prosecution history provides evidence of how the PTO and the inventor understood the patent. . . . Yet because the prosecution history represents an ongoing negotiation between the PTO and the applicant, rather than the final product of that negotiation, it often lacks the clarity of the specification and thus is less useful for claim construction purposes."); *Tempo Lighting*, 742 F.3d at 978 (The "court also observes that the PTO is under no obligation to accept a claim construction

proffered as a prosecution history disclaimer, which generally only binds the patent owner.").

The Specification and claims record do not support the prosecution history arguments discussed above. The plain language of the claims outweighs the arguments made. For example, Patent Owner contends that Patentee disclaimed "a domain name that just happens to be associated with a secure computer or just happens to be associated with an address requiring authorization" during an *inter partes* reexamination of a related patent, and that the Specification supports its construction. *See* PO Resp. 5 (citing Response to Office Action in Control No. 95/001,270 (Apr. 19, 2010), 5 (Ex. 2008)). It is not clear how this argument creates a distinction, or what "just happens to be associated with a secure computer" means, but Patent Owner appears to contend it means "a secure domain name cannot be resolved by a conventional domain name service." *See* PO Resp. 5; Ex. 2008, 6 (arguing "a secure domain name cannot be resolved by a conventional domain name service, for example, but relying on "the inventors . . . acting as their *own lexicographers*" and citing disclosed examples in the '180 patent of non-standard top-level domain names) (emphasis added).

This argument obscures the meaning of the challenged claims when viewed in light of the Specification's disclosure of secure domain names. Contrary to its prosecution history arguments, nothing in the '705 (or '180) patent requires a conventional DNS not to return an address for all of the disclosed secure domain names, let alone, sets forth a *lexicographic* definition for such a preclusion. Rather, as discussed above, the '705 patent discloses using conventional DNS look up functionality (*e.g.*, using internal

tables) to determine whether access to a secure website has been requested, adding other layers of functionality, including employing user priority levels, and/or credentials, etc. *See*, *e.g.*, Ex. 1050, 40:1–6 ("proxy . . . intercepts all DNS look up functions" and determines access "by reference to an internal table"), 38–42 (combining proxy and conventional "functions . . . into a single server"), 51–58 ("using an internally stored list of authorized IP addresses"), 51:10–28 (users can "automatically obtain the secure network address" by "register[ing] a secure domain name" with possible additional use of "the user's identity and the user's subscription level.")[11] Patentee's attempt during prosecution of the '180 patent to act as its "own lexicographer[]" by relying on *examples* in the '180 patent that relate to non-standard *top-level* domain names indicates (Ex. 2008, 6) that the disclaimer argument does not pass muster.

Patent Owner does not argue here that the '705 patent supports a lexicographic definition for all its disclosed secure domain names based on unclaimed examples related to top-level secure domain names. Contrary to

[11] The Examiner's citations and reasoning in the 95/001,270 reexamination proceeding involving the '180 patent track Patent Owner's arguments and do not support the specific disclaimer argued. The Examiner states that "[f]or example, the '180 patent explains that a secure domain name service can resolve addresses for a secure domain name whereas a conventional domain name service cannot resolve addresses for a secure domain name." Ex. 2006, 6 (citing '180 patent, 51:25–53). Citing the same passage, the Examiner also states that "querying a convention[al] domain name server using a secure domain name will result in a return message indicating that the URL is unknown." *Id*. The cited examples do not support a clear disclaimer that distinguishes a "secure domain name" from a secure domain name that happens to correspond to a secure computer. *See id*. These passages describe examples that correspond to a non-standard top-level domain name. *See* '180 patent, 51:25–53.

Patentee's assertion of a lexicographic definition during prosecution, no reasonably clear and precise disclaimer appears in the Specification with respect to secure domain names. *See*, *e.g.*, *Paulsen*, 30 F.3d at 1480 (disclaimer requires "reasonable clarity, deliberateness, and precision"). Patentee did not disclaim conventional look up functionality when employed to look up secure domain names. The arguments obscure what a "non-standard" name means and what "conventional" means in terms of the look up function that rises in context to the arguments.

Patent Owner does not demonstrate that the Specification requires a secure domain name to be "top-level" or "non-standard." And more importantly, setting aside the top-level domain names, which are mere examples that Patent Owner does not rely on as part of its proposed claim construction, Patent Owner fails to explain clearly what the term "non-standard" means or how a "non-standard" domain name differs from a "secure computer network address."

Therefore, Patent Owner's construction and its prosecution history arguments obscure the clear meaning of the claim terms—because they attempt to preclude the ability of "conventional" DNS from resolving a "non-standard" name. As the record shows, the conventional DNS functionality at issue simply involves looking up names (using for an example an internal table). Therefore, if a DNS resolves a non-standard name (whatever that means if not limited to a top-level domain name), the resolution itself would be "conventional," whereas Patent Owner's construction implies that any DNS that resolves a "non-standard" name cannot be "conventional."

Accordingly, we determine that the prosecution history argument is not clear and precise, nor is it supported by the Specification, and it is outweighed by the plain language of the claim. As discussed below, even if we adopted Patent Owner's narrower claim construction, as supported by the prosecution history, our obviousness analysis would remain unchanged. Similarly, in addition to the just-described prosecution history, in the final written decision in the '481 IPR, the Board found that "Patent Owner . . . made the opposite argument to a district court that it is making here, and argued that the 'non-standard' distinction 'is not supported by the specification or the prosecution history.'" IPR2014-00481, Paper 35, 13 (quoting '481 IPR Ex. 1018, 18 (district court findings and rationale)).[12] The record here supports the argument made by Patent Owner in the district court—the Specification and prosecution history do not support the non-standard distinction.

Neither are we persuaded that what the parties agreed to in the district court binds us. First, Petitioner does not agree to that construction in this proceeding. We are unaware of any precedent preventing Petitioner from taking inconsistent positions in different forums and Patent Owner does not cite any either. Further, as has now been confirmed in *Cuozzo*, we apply the broadest reasonable interpretation standard and not the litigation standard in district court. On the other hand, the construction Petitioner now proposes is taken directly from other *inter partes* reviews. These circumstances are

[12] The district court case cited in the '481 IPR involved a finding of a disclaimer of a different but related term: "secure domain name service." *See* '481 IPR, Ex. 1018, 17–18; '481 IPR, Ex. 2003, 91.

adequate justification for a differing construction from that of the district court.

In addition to the preceding reasons, we agree with the analysis made in the construction of "secure domain name" in a prior *inter partes* review proceeding. *See* '481 IPR, Paper 35, 13–14. Thus, we construe "secure domain name" as "a name that corresponds to a secure computer network address."

2. "encrypted communications channel" (claims, 1–2, 4–7, 9, 11–13, 18, 21–22, 26–29)

The Petition did not propose a construction for "encrypted communications channel." Patent Owner proposes that an "encrypted communications channel" should be construed to mean "a direct communications channel that is encrypted." PO Resp. 8–10. Petitioner argues the inclusion of "direct" adds an additional limitation we have previously rejected in the related '481 IPR. Pet. Reply 3 (citing '481, Paper 35, 10). In the '481 IPR we concluded the addition of direct was unnecessary to resolve the dispute. '481 IPR, Paper 34, 4.

Patent Owner argues one embodiment in the Specification describing TARP ("Tunneled Agile Routing Protocol," Ex. 1001, 3:14–17) terminals supports its construction by describing that encrypted communications between a client device and target device are "direct." PO Resp. 9 (citing Ex. 1001, 9:41–50, 33:43–51, 38:6–9 (describing Figure 24 as first and second computers directly connected), Fig. 2). Other embodiments described in the Specification are also argued as supporting the addition of "direct" to the construction of "encrypted communications channel." *Id.* (citing Ex. 1001, 40:7–10, 40:66–41:2, 42:6–10, 42:66–43:3, Figs. 24, 26,

28, 29, 33; Ex. 2016 ¶ 19). The citations to the Specification are examples of different embodiments and do not persuade us that the addition of "direct" is warranted. In the absence of such a special definition or other consideration, "limitations are not to be read into the claims from the specification." *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

Patent Owner next argues that in district court litigation Petitioner argued that traversing a network, including being passed or routed through various networks, is "direct." PO Resp. 10 (citing *Markman* Hearing Transcript, 42:16–21, 44:13–45:12,[13] 44:13–45:12 (Ex. 2003). This argument is not persuasive. First, the record does not show and Patent Owner does not explain the context in which the statements were made or what construction issue was being argued. Second, the attorney argument is by an attorney representing another party and not Petitioner. *See* Ex. 2003, 90:2–3 (representing Cisco). Patent Owner has not presented any reason to accept statements from a co-defendant in the district court as binding on another co-defendant. None of Patent Owner's arguments are persuasive, and we decline to require that "direct" should be included in the construction.

However, the Federal Circuit on appeal "construed the related terms 'secure communication link' and 'virtual private network' to include 'direct' communication." PO Resp. 10 (citing *VirnetX Inc. v. Cisco Sys. Inc.*, 767 F.3d 1308, 1317 n.1, 1319 (Fed. Cir. 2014) ("*Cisco*")). Specifically, the Federal Circuit construed "secure communication link" to mean "a direct communication link that provides data security and anonymity." *Cisco*, 767 F.3d at 1319 (emphasis omitted). Our determination not to limit the claims

[13] Patent Owner cites to pages 2 and 4, which it appears was not intended.

to "direct communication" is not inconsistent with the construction in *Cisco*. In contrast to the broadest reasonable interpretation standard employed by the Board for an unexpired patent, the Federal Circuit employs a narrower claim construction standard when reviewing the construction of a claim applied by the district court. *See In re Rambus, Inc.*, 694 F.3d 42, 46 (Fed. Cir. 2012) (contrasting the Board's review of expired patents, which is "similar to that of a district court's review," with the Board's review of unexpired patents, which involves the broadest reasonable interpretation standard); *Cuozzo,* 136 S. Ct. at 2142. As discussed above the addition of "direct" to the construction is narrower and does not comport with the broadest reasonable interpretation. In addition, a reading of *Cisco* indicates that the parties did not dispute the "direct" requirement in *Cisco.* As indicated above, the '705 patent Specification does not require a channel to be direct. Furthermore, although Patent Owner lists examples that encompass a direct link, Patent Owner fails to explain clearly on this record what "direct" means. *See* PO Resp. 10 ("the '705 patent specification discloses that the communication traverses a network (or networks) through which it is simply passed or routed via network devices such as Internet Service Providers, firewalls, and routers").

The patents at issue in *Cisco* have common descriptions to the '705 patent. The '705 patent is a continuation of U.S. Patent No. 7,921,211 ("'211 patent"), which is a continuation of U.S. Patent No. 7,418,504 ("'504 patent"). Ex. 1001 (63). *Cisco* was an appeal relating to the '504 and '211

patents, among others. *Cisco*, 767 F.3d at 1313.[14] In *Cisco*, the court found that "[b]oth the claims and the specification of the '151 patent make clear that encryption is a narrower, more specific requirement than security." *Id.* at 1323 (citing a passage in the '151 patent at 1:49–50 ("Data security is usually tackled using some form of data encryption.")). This passage, relied upon by the Federal Circuit in its construction, also appears in the '705 patent. *See* Ex. 1001, 1:57–59.

In the '237 IPR final written decision, we relied on the Federal Circuit's construction of "secure communications link" in *Cisco* and construed the term as meaning "a transmission path 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 anonymity, authentication, or encryption." '237 IPR, Paper 41, 8. We recognize that "encrypted communications channel" is different from "secure communications link." However, as previously noted, '"encryption' is a narrower, more specific requirement than security." *Cisco*, 767 F.3d at 1323; Ex. 1001, 1:57–58 ("Data security is *usually* tackled using some form of data encryption."). Thus, encryption is a type of "secure communications."

We turn to the difference between a "communications link" and a "communications channel." Both terms are used in the Specification to describe communication between two computers. *See* Ex. 1001, 1:65–67 ("To hide traffic from a local administrator or ISP, a user can employ a local

[14] The patents in *Cisco* included U.S. Patent Nos. 6,502,135; 7,418,504 ("'504 patent"); 7,490,151 ("'151 patent"); and 7,921,211 ("'211 patent"). *Cisco*, 767 F.3d at 1313.

proxy server in communicating over an *encrypted channel* with an outside proxy.") (emphasis added), 20:53–54 ("Two hardware nodes communicating over a physical *communication channel* . . .") (emphasis added), 6:42–45 ("The advantages of the present invention are provided by a method for establishing a *secure communication link* between a first computer and a second computer over a computer network, such as the Internet.") (emphasis added), 50:53–55 ("In this configuration, secure portal 3310 can only be accessed using a VPN *communication link*.") (emphasis added). The claims here use "communications channel" but other claims based on the same disclosure use "communications link." *See* '237 IPR, Paper 41, 8 (*see* claim 1 of US Patent No. 8,504,697). Both parties cite to the '237 IPR and neither argues any distinction between the two terms and, in our review of the Specification and applying the broadest reasonable interpretation to the term, we do not see a claim construction distinction between "communication channel" and "communication link."

Based on the foregoing discussion, "encryption" is more limited than "secure" and is recited specifically in the term under consideration. We agree with the analysis in the '237 IPR and its construction of "secure communication link." *See* '237 IPR, Paper 41, 5–8. Accordingly, the broadest reasonable construction of an "encrypted communications channel" is "a transmission path that restricts access to data, addresses, or other information on the path, hiding information on the path using encryption."

3. "provisioning information" (claims 1, 2, 9, 21)

In the Institution Decision we construed "provisioning information" to mean "information that is provided to enable or to aid in establishing a secure communications channel." Inst. Dec. 8–9. Petitioner agrees with the

construction, which is similar to what we determined in the '481 IPR. *See* Pet. Reply 4 (citing '481 IPR, Paper 11, 10–11 ("'provisioning information' is information that is provided to enable or to aid in establishing communications to occur in the VPN")). Nevertheless, in that case, the claims at issue recited broader subject matter. *See* IPR '481, Paper 35, 41 ("wherein the response message contains provisioning information for the virtual private network").

Patent Owner proposes we construe the term as "[i]nformation that is used to establish an encrypted communications channel." PO Resp. 10–11. Patent Owner notes that the claims refer to an "*encrypted* communications channel" and not just a "*secure* communications channel." *Id.* at 11. Patent Owner's arguments rely on what the claims at issue recite. Accordingly, we need not construe the term in this case, because the claims define what the provisioning information requires. For example, claim 1 recites "providing provisioning information required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel."

4. "intercept[ing] . . . a request to look up an Internet Protocol (IP) address" (claims 1 and 21)

Independent method claim 1 recites "*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" (the "intercepting limitation"). Independent system claim 21 recites similarly "intercept from

the client device a request to look up an Internet Protocl (IP) address." 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 Final Written Decision in the '237 IPR. '237 IPR, Paper 41, 10–12. In its Reply, Petitioner cites to the '237 IPR Final Written Decision, but does not propose another construction. Pet. Reply 4.

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. 24 n5 (referencing our construction of "intercepting" in the '237 IPR). Patent Owner states in the instant proceeding that "no construction is necessary." PO Resp. 13 (Table). 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, preforming an evaluation on it related to establishing an encrypted communications channel." *Id.* at 13–14.

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. 14 (citing Prelim. Resp. 30–34[15]; Ex. 2016 ¶ 24). 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 claim 1 (and a similar phrase in claim 21), captures the functionality, in particular, the "determination" clause of claim 1. *Id.* More specifically, Patent Owner argues in the determination clause of claims 1 and 21, "a determination is made whether the request to look up the IP address corresponds to a device that accepts an encrypted channel connection with the client device, and that 'in response to' this determination, provisioning information required to initiate the encrypted communications channel is provided." *Id.* We are not persuaded that functionality in another step of claim 1 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. 13; Pet. 10–12. 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 to look up an address for another (downstream) entity

[15] 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.

(i.e., the request pertains to that downstream entity). Pet. 9–10 (citing Ex. 1001, 39:1–3, 40:1–7, 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 '705 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 FWD, the broadest reasonable construction of the intercepting limitation is "receiving a request pertaining to a first entity at another entity."

OBVIOUSNESS-AVENTAIL AND RFC 2401

Petitioner alleges claims 1–3, 6, 14, 16–25, 28, 31, and 33–34 would have been obvious over Aventail and RFC 2401. Pet. 27–51. Petitioner's evidence includes the Declaration of Roberto Tamassia ("Tamassia Declaration," Ex. 1005), which describes Aventail and RFC 2401. Ex. 1005 ¶¶ 160–273, 346–382.

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 ¶ 110; *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. Monrose, 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. 2016 ¶ 13. Dr. Monrose 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 '705 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[16]

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."

[16] We address Patent Owner's motion to exclude certain paragraphs of the Tamassia Declaration, Exhibit 1005, in a separate section, below.

PO Resp. 42. Petitioner responds that Dr. Tamassia has "offered probative testimony on many of the factual inquiries underpinning an obvious analysis" that "can certainly 'assist the trier of fact to understand the evidence or determine a fact in issue.'" Pet. Reply 18 (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 18–19.

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. 43. 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:

> *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. 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. 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 Aventail, RFC 2401, and RFC 2543[17]

Patent Owner asserts that Petitioner has not sufficiently established that Aventail (PO Resp. 47–51) or RFC 2401 and 2543 (discussed together,

[17] We address Patent Owner's motion to exclude exhibits relating to whether Aventail Connect, RFC 2401, and RFC 2543 were publicly available before the critical date in a separate section, below.

PO Resp. 51–60) qualify as printed publications as of their alleged publication dates. 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).

1. Aventail

In its Petition, Petitioner cited to the declarations of Christopher Hopen ("Hopen Declaration," Ex. 1023), Michael Fratto ("Fratto Declaration," Ex. 1043), and James Chester ("Chester Declaration," Ex. 1022)[18] to support its allegation that Aventail "was distributed to the public without restriction no later than January 31, 1999."[19] Pet. 15–17. Patent

[18] Exhibits 1022 and 1023 were originally filed in *inter partes* reexamination 95/001697 requesting reexamination of US Patent 7,490,151. *See* Pet. Attachment B, Exs. 1022, 1023. Exhibit 1043 *inter partes* reexamination 95/001697 was originally filed in *inter partes* reexamination 95/001,682 requesting reexamination of US Patent 6,502,135. *See* Pet. Attachment B, Ex. 1043.

[19] Petitioner alleges the effective filing date is no earlier than February 15, 2000. Pet. 7–8. Patent Owner does not dispute the allegation in this proceeding. Petitioner's supporting evidence includes that the limitation

Owner objected to Exhibits 1022, 1023, and 1043 and filed a motion to exclude, which is discussed below. *See* Papers 11 and 36. Petitioner then served Patent Owner Exhibits 1057–1059 as supplemental evidence. *See* 37 C.F.R. § 42.64(b)(2).[20]

Exhibits 1057–1059 are all related to the Hopen Declaration and are alleged to be probative of whether or not Aventail was publicly available. *See* Paper 17 ("Mot. Supp. Inf.") 2, 5–8. Specifically, Exhibit 1057 is the deposition transcript of Mr. Hopen from a related District Court litigation—*VirnetX, Inc. v. Apple Inc.*, 10-cv-00417 (E.D. Tex.), which Patent Owner submitted to the Office as part of an Information Disclosure Statement ("IDS") in the prosecution of U.S. App. No. 13/339,257. *Id.* at 6 n.3. Exhibit 1058 is a declaration of Mr. Hopen from a reexamination proceeding marked as deposition exhibit P4 at Mr. Hopen's deposition. *Id.* Exhibit 1059 is jury trial transcript of the same District Court case, including excerpts from Mr. Hopen's deposition read into the record. *Id.* at 8; *see* Ex. 1059, 21–32.

"domain name" in claims 1 and 21 is first supported in US Application Ser. No. 09/504,783 (now US Patent 6,502,135), a prior related application filed on February 15, 2000. *Id.* at 7; *see* Ex. 1001 (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 '705 patent is February 15, 2000, and the critical date for prior art is February 15, 1999. *See id.* at 16 (Aventail is prior art under 35 U.S.C. § 102(b)).

[20] Petitioner subsequently filed a Motion to Submit Supplemental Information pursuant to 37 C.F.R. § 42.123(a) asking that Exhibits 1057–1059 be considered as supplemental information. We granted that motion. *See* Paper 21.

Apart from whether they are admissible, which is addressed separately below, Patent Owner argues the Hopen, Chester, and Fratto declarations do not prove Aventail was a printed publication publicly available as of January 31, 1999. PO Resp. 47–51. Further, Patent Owner contends the declarations are uncorroborated. *Id.* at 47–48 (citing *Typeright Keyboard Corp. v. Microsoft Corp.*, 374 F.3d 1151, 1158–60 (Fed. Cir. 2004); *Finnigan Corp. v. ITC*, 180 F.3d 1354, 1366 (Fed. Cir. 1999)).

Patent Owner does not dispute that Mr. Hopen states in his declaration that the AEC v3.0 (Ex. 1011) product was distributed along with a copy of Aventail Connect v3.01/2.51 Administrator's Guide (Ex. 1009) no later than January of 1999. PO Resp. 48; *see* Ex. 1023 ¶¶ 13–15. Although Patent Owner acknowledges the Hopen Declaration testimony states that "'thousands of copies of' Aventail v3.01 were distributed during the first six months of 1999," according to Patent Owner there is "no evidence of how many copies were distributed in *January of 1999*—the date alleged by Petitioner as the latest publication date of *Aventail*." *Id.* at 49 (citing Pet. 16, Ex. 1023 ¶¶ 9, 16). Patent Owner argues the Fratto and Chester Declarations do not corroborate Mr. Hopen's testimony that "thousands of copies" of Aventail were distributed or how much of the distribution occurred in January of 1999, the date alleged by Petitioner as the publication date of Aventail. *Id.* at 49–50 (citing Pet. at 16; Ex. 1023 at ¶¶ 9, 16). Patent Owner also points out that the record lacks corroborating documentation. *Id.* at 49.

We find that the testimony of the three declarations, taken together, qualify as credible evidence that Aventail was publicly available as of January 1999. Mr. Hopen, Fratto, and Chester all have personal knowledge

of Aventail and testified consistently about it being publicly available prior to February 15, 2000. Indeed, that the testimony is similar but not identical contributes to the credibility of the testimony. We summarize the evidence below.

Mr. Fratto is editor of the *Network Computing* magazine and website. Ex. 1043 ¶ 2. Mr. Fratto testifies that between 1997 and 1999 he reviewed and published articles on "Aventail Extranet Center ('AEC'),[21] which included client software called 'Aventail Connect' and server software called 'Aventail Extranet Server.'" *Id.* at ¶¶ 6–14 (citing articles attached to his declaration). Based on further discussion below, this testimony is related to the Aventail prior art: Aventail Connect v3.01/v2.51 Administrator's Guide (Ex. 1009); Aventail Connect v3.01/v2.51 User's Guide (1996-1999)(Exhibit 1010); and Aventail ExtraNet Center v3.0 Administrator's Guide (Exhibit 1011).

We have considered Patent Owner's arguments that Mr. Fratto is biased against patents generally and Patent Owner specifically. PO Resp. 50–51 (citing Exs. 2018–2031).[22] Our review of the cited exhibits confirms that Mr. Fratto is outspoken about patent process and patent litigation. Mr. Fratto's use of coarse language and, in one instance, profanity (edited by Mr. Fratto's insertion of an * for a letter, *see* Ex. 2029) in Tweets is consistent with the type of communication that occurs in much of social media. We are not persuaded that Mr. Fratto's statements in Exhibits 2018–2031 extend to all patents and all cases and the patent system in general. Moreover, Mr.

[21] "Aventail Extranet Center" is also referenced in the testimony as "AEC."
[22] By way of example, Patent Owner states "Mr. Fratto announced that he views his role as including 'patent busting' rather than 'patent consulting.'" PO Resp. 51 (citing Ex. 2028; Ex. 2031, 94:4–11).

Fratto's testimony is limited to facts falling within Mr. Fratto's personal knowledge. We do not see any indication the testimony is false. Even assuming Mr. Fratto is biased against some types of patents generally, we do not see any reason to discount the testimony on this particular issue. *See* Pet. Reply 22, n.4 (alleging the "attacks against Mr. Fratto are irrelevant and unfounded").

Patent Owner's basis for asserting that Mr. Fratto has a specific bias against Patent Owner is based on expert testimony Mr. Fratto has given against Patent Owner's patents and his compensation as an expert witness. *See* PO Resp. 51 (citing Ex. 2031, 49:17–50:9, 92:20–93:14). We are not persuaded that giving expert testimony against Patent Owner's patents is bias that would cause us to diminish the weight given Mr. Fratto's testimony. Indeed, carried to its logical extreme, were that the test, expert testimony would be prohibited because it is always "biased against" the opposing party.

Mr. Chester is CEO of Assured Products Group, a software development and consulting firm. Ex. 1022 ¶ 4. Mr. Chester worked for IBM between March 1992 and August 2002 evaluating network security products. *Id.* ¶ 5. Mr. Chester evaluated Aventail VPN products between 1996 and 2000. *Id.* ¶ 9. Mr. Chester "recall[s] that Aventail Corporation announced its AEC v3.0 product in the fall of 1998, and began distributing this product no later than mid-January 1999." *Id.* ¶ 15. Mr. Chester testifies that the AECv3.0 product included version 3.01/2.51 of the Aventail client software (Ex. 1009) and version 3.0 of the Aventail Extranet Server (Ex. 1011). *Id.* ¶ 16.

Neither Mr. Hopen, Mr. Fratto nor Mr. Chester have been shown to have any relationship or interest in the outcome of this proceeding. There is no evidence or even argument that Aventail Corporation, for whom Mr. Hopen worked, is a competitor to Patent Owner. We note that both Mr. Fratto and Mr. Chester were paid for non-expert testimony. *See* Ex. 1022 ¶ 2; Ex. 1043 ¶ 5. There is no indication that payment is tied to the outcome of the case. It is a reasonable inference from the evidence and testimony that both are typically paid for their time. *See* Ex. 1022 ¶ 4 (Mr. Chester is employed by a consulting firm), Ex. 2031 (Mr. Fratto was deposed as an expert witness).

Although the testimony of the three witnesses is sufficient to establish the Aventail documentation, including Aventail client software, is prior art, Petitioner offers additional evidence of corroboration submitted with the declarations, which Petitioner argues Patent Owner ignores. Pet. Reply 22 (citing Ex. 1023, attached Exhibits A, B, and C). The cited exhibits do not relate directly to the Aventail client software or Aventail manuals, but are evidence that the Aventail Corporation was developing VPN security products in 1997 and late 1998. *See* Ex. 1023, Exhibit B, 1 ("For secure remote-access needs, Aventail Corporation's Mobile VPN 2.0 and AutoSocks 2.1 comprise a virtual private network (VPN) software solution."). This evidence ties into the timeline of Aventail Corporation's VPN products introduced between 1996 and 2000, as testified by Mr. Chester. Ex. 1022 ¶¶ 9–13. Petitioner cites additional evidence, also related to Aventail Corporation products, which we have also considered. Pet. Reply 22 (citing Ex. 1057, 79:25–80:9; *id.* at 83:10–84:16, 91:20–92:2, 100:2–104:7; Ex. 1059, 20–32).

Assuming corroboration of the testimony is required, the testimony at pages 100–104 of Mr. Hopen's deposition (Exhibit 1057) describes Exhibit 9 of his deposition, Aventail Connect version 3.01/2.51 Administrator's Guide (Ex. 1009), and correlates the date it was publicly available with the October 1998 date of the press release for the Extranet Center 3.0 product (Exhibit 6 of his deposition, Exhibit 1011 here). Ex. 1057, 100:2–104:4. The Hopen deposition testimony was taken in the district court litigation and was subject to cross examination by Patent Owner. *See* Ex. 1057, 148:1–227:4 (examination by Patent Owner's attorney Mr. Curry). The fact that the witness was cross examined, and the testimony was consistent with the declaration, adds to the credibility of Mr. Hopen's testimony.

Even if required under these circumstances, corroboration "does not require that every detail of the testimony be independently and conclusively supported by explicit disclosures in the pre-critical date documents or physical exhibits." *Ohio Willow Wood Co. v. Alps S., LLC*, 735 F.3d 1333, 1348 (Fed. Cir. 2013) (internal citations omitted); *see* Pet. Reply 21. *Willow Wood* stated a "rule of reason" test in which "the totality of the evidence …, including circumstantial evidence" is assessed "in order to ascertain whether the testimonial assertions are credible." *Willow Wood*, 735 F.3d at 1348.

Mr. Hopen also testified he was involved in the "design, development and distribution of all of Aventail's network security products." Ex. 1023 ¶ 4. He further testifies that the AEC v3.0 product was distributed along with a copy of Aventail Connect v3.01/2.51 (Ex. 1009) before January 1999. *Id.* ¶ 9, 14–16. Mr. Hopen, a person with direct knowledge of the Aventail AEC v3.0 product, also generally testified that "Aventail included printed manuals with the software packages that it distributed." *Id.* ¶ 8. Mr. Hopen

also testified that Aventail Connect v3.01/2.51 (Ex. 1009) and Aventail Extranet Center v3.01 (Ex. 1011) were distributed "no later than January of 1999," *see id*. ¶¶ 8, 14–16, with thousands of copies distributed "during the first six months of 1999" (*id*. ¶ 16). "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)).

The evidence here supports a finding that both Mr. Fratto and Mr. Chester had access to the Aventail Extranet Center v3.0 by January 1999. In the case of Mr. Fratto, between 1997 and 1999, he reviewed and published articles for his *Network Computing* magazine and website relating to Aventail Corporation products and had knowledge, between 1997 and 1999, of "Aventail Connect" and "Aventail Extranet Center." Ex. 1043 ¶¶ 2, 6. Mr. Fratto testified that Aventail Extranet Center 3.0 (Ex. 1011) was distributed in the fall of 1998 and identified "Intranet Applications: Briefs," *Network World*, 55 (October 19, 1988 (Exhibit I to Ex. 1043) as support. *Id.* ¶ 13. Mr. Fratto identified Exhibit G as a non-confidential copy of Aventail Extranet Center v3.0 he received in October 1998. *Id.* ¶ 14. While at IBM, Mr. Chester recalls the announcement of Aventail Corporation acquired the product for IBM in the fall of 1998. Ex. 1022 ¶ 10 (citing an Aventail Corporation press release, Exhibit D to his declaration).

Having reviewed all the evidence, we determine that testimony of Mr. Hopen, Mr. Fratto, and Mr. Chester is corroborated sufficiently and that

Petitioner has shown by a preponderance of the evidence that Aventail Connect v3.01/2.51 (Ex. 1009) and Aventail Extranet Center v3.0 (Ex. 1011) were sufficiently disseminated to persons of ordinary skill interested in computer networking and security to be deemed "publicly accessible" as of January 1999. Viewing the evidence as a whole we determine that Petitioner has shown the Aventail documentation was publicly available before February 15, 1999. Accordingly, we find that Petitioner has established, by a preponderance of the evidence, that the Aventail documentation, including Aventail Connect v3.01/2.51 (Ex. 1009) and Aventail Extranet Center v 3.0 (Ex. 1011), qualify as prior art printed publications under 35 U.S.C. § 102(b).

2. RFC 2401 and RFC 2453

In our Decision to Institute, 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, both RFC 2401 and RFC 2453, 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

¶ 148. Dr. Tamassia goes on to discuss an RFC that discusses the RFC development and publication process itself—RFC 2026, dated October 1996. *Id.* ¶ 149–155; 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.* ¶ 152. 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. 1005 ¶¶ 148–149; Ex. 1036, 5–6.

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.[23]

We find Dr. Tamassia's testimony as to public accessibility of RFCs in general to be credible, especially given the independent support of Exhibit 1036, which is not objected to by Patent Owner and is evidence of record. As part of routine discovery (37 C.F.R. § 42.51(b)(1)(ii)), Patent Owner had

[23] 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. 54 n.7. Patent Owner, itself, however, directed the Board's attention to this testimony in its Preliminary Response (Paper 6, 4–5), and thus clearly has had adequate notice of its contents such that it may respond with no issues of prejudice.

the opportunity to cross-examine Dr. Tamassia and did so, taking the Tamassia Deposition and making it of record. *See* Ex. 2015. 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.

The Tamassia Deposition also references RFC 2543. *See* Ex. 1005 ¶¶ 148–157, ¶¶ 158–159 (specific to RFC 2543). On its face, RFC 2543 gives a date in the upper right hand corner of the first page of March 1999. The reasons given in connection with RFC 2401 apply equally to RFC 2543. Patent Owner does not raise any issue for our consideration specific to RFC 2543 and we are therefore given no reason to make a different determination.

We find that Petitioner has established, by a preponderance of the evidence, that RFC 2401(dated November 1998) and RFC 2543 (dated March 1999) were sufficiently disseminated to persons of ordinary skill interested in computer networking and security to be deemed "publicly accessible" at the relevant time. See *SRI Int'l,* 511 F.3d at 1194. Therefore, on this record, we determine RFC 2401 and RFC 2543 qualify as prior art printed publications under 35 U.S.C. § 102(b).

E. Overview of Aventail

Petitioner alleges each of Exhibits 1009–1011 are documentation for a software product and that the three documents were distributed together.

Pet. 15–17 (citing Exs. 1022, 1023, 1043). Both Petitioner and Patent Owner primarily refer to their respective expert declarations, which describe the Aventail documentation in the context of the Aventail Administrator Guide (Ex. 1009) and its description of "Aventail Connect," the client component of the Aventail ExtraNet Center, when analyzing this ground. *See* Pet. 15–24, PO Resp. 15–17. For example, Dr. Tamassia relies primarily on Exhibit 1009, but also states that "[t]he [three Aventail exhibits] cross-reference each other, which is logical as they are describing two components of a single system that are designed to work together (i.e., the Aventail Connect client running on the client computer, and the Aventail Extranet Server running on a server computer)." Ex. 1005 ¶ 145. Dr. Monrose focuses on Aventail Connect (Ex. 1009) in his description of the product functionality. Ex. 2016 ¶¶ 25–28. Accordingly, we cite to Exhibit 1009 for its description of Aventail Connect.

Aventail Connect is the client component of the Aventail ExtraNet Center. *See* Ex. 1009, 7. The Aventail Connect component can be used in a network as a simple proxy client for managed outbound access, and for secure inbound access. *Id.* It is an application between WinSock and the underlying TCP/IP stack. *Id.* at 9. Aventail Connect can compress or encrypt data before routing to the network. *Id.* The routing is determined by rules described in the configuration file. *Id.* When Aventail Connect receives a connection request, it determines whether or not the connection needs to be redirected to an Aventail ExtraNet Server and whether the connection should be encrypted. *Id.* at 10. This process is described using several steps. *Id.* at 11–13.

In the first step, Aventail Connect does a DNS lookup to convert the hostname to an IP address. Ex. 1009, 11. If the application knows the domain is one to which traffic is being proxied (i.e., the destination hostname matches a redirection rule domain name from the configuration file), a false DNS is created that later can be recognized during a connection request. *Id.* Similarly, if a DNS proxy option is enabled, but the domain cannot be looked up directly, the application again creates a false DNS entry that it can recognize later, and returns this to the calling application. *Id.* at 12. The false entry tells Aventail Connect that the DNS lookup must be proxied (forwarded to and resolved by an extranet server) in the next step of the process. *Id.* Otherwise (if Aventail Connect already knows the IP address of the hostname, the hostname matches a local domain string, or the hostname does not match a redirection rule, and no proxy option is enabled), the DNS lookup proceeds as if Aventail Connect were not running. *Id.*

In the second step, Aventail Connect requests a connection to the remote host. Ex. 1009, 12. The request is first checked to see if it contains a false DNS entry, as may be assigned set in the first step. *Id.* If a false DNS entry is present, the request is proxied—sent to an extranet server ("SOCKS"[24]) for hostname resolution using the authentication method specified in the configuration file. *Id.*

[24] SOCKS is an acronym for "Socket Secure." *See* Ex. 1005 ¶ 162 (SOCKS "enables a client within an internal network protected by a firewall (e.g., a corporate local area network) to establish a connection to a server on the network external to the firewall (e.g., the internet)."; Network Working Group, Request for Comments, SOCKS Protocol Version 5, 5–6, IETF RFC 1928 (Ex. 1018).

Once the connection is complete, in the third step, Aventail Connect transmits and receives data. *Id.* at 12. This data may be encrypted for transmission and decrypted on receipt if "an encryption module is enabled and selected by the SOCKS server." *Id.*

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 21

Although claim 1 recites "a method of transparently creating an encrypted communications channel" and claim 21 recites "a system for transparently creating an encrypted communications channel," the two claims encompass substantially the same subject matter. Both Petitioner and Patent Owner argue claims 1 and 21 together. Pet. 28–43; PO Resp. 15–34; Pet. Reply 2–14. We, therefore, analyze independent claim 1, with the understanding the analysis applies equally to claim 21.

1. Petitioner's Assertions

The preamble of claim 1[25], recites, in pertinent part, "creating an encrypted communications channel between a client device and a target device." Petitioner argues that Aventail discloses a "scheme for creating private communication and data channels over the Internet" between "client computers ('*client devices*') and remote hosts ('*target device[s]*')." Pet. 29 (citing Ex. 1009, 12, 91–92). Petitioner also alleges Aventail discloses that "Aventail is designed to run transparently. . . ." *Id.* (citing Ex 1009, 7; Ex. 1005 ¶ 171).[26]

Petitioner contends that Aventail discloses routing communications through an encrypted channel. *See* Pet. 29–30 (citing Ex. 1009, 1, 11–12, 72–73). Petitioner further argues Aventail discloses "functionality for intercepting connection requests from the client computer to a remote host, and creating an encrypted channel between the client computer and the remote host." *Id.* (citing Ex. 1009, 9–12, 73; Ex. 1005 ¶¶ 171–172, 214–216). Although Petitioner contends that Aventail alone discloses the "encrypted communications channel" of claims 1 and 21, Petitioner also asserts that encryption would have been obvious based on the combination

[25] Petitioner proceeds on the basis that the preamble is limiting. Patent Owner does not make a contrary argument. The preamble recites, in part, "an encrypted communications channel between a client device and a target device," which provides antecedent basis for those terms recited later in the claim. We agree the preamble is limiting. *See* Pet. 29.

[26] The "*system including a memory storage instructions*" and "*a server configuration*" specific to system claim 21 are alleged to be present in the RAM and Extranet server of Aventail Connect. Pet. 30–31 (citing Ex. 1009, 11–13).

of Aventail and RFC 2401, which specifically discloses encryption. *Id.* at 30, 39–42.

Petitioner also argues that Aventail discloses step (1) of claim 1, "intercept[ing] . . . a request to look up an [] IP address corresponding to a domain name associated with the target . . . ." Pet. 31–33. Petitioner cites Aventail's disclosure that a "client computer running Aventail will transparently intercept each connection request made on the client." *Id.* at 31 (citing Ex. 1009, 7–9, 72–73; Ex. 1005 ¶¶ 171–172, 209–216). Petitioner cites to Aventail's disclosure that to connect to a "Remote Host," i.e., the recited "*target device*," a Domain Name System (DNS) lookup converts the hostname into an Internet Protocol (IP) address. *Id.* (citing Ex. 1009, 8, 11, 91–92; Ex. 1005 ¶ 210). In addition, Petitioner cites to Aventail's disclosure that all connection requests to the Aventail Extranet Server contain either the IP address or the domain name of the destination computer, which are used for handling and resolution. *Id.* at 32 (citing Ex. 1009, 12, 61; Ex. 1005 ¶¶ 225–28). Petitioner concludes that "[a] person of ordinary skill would recognize from the teachings in Aventail that, in this configuration, the Aventail Extranet Server will necessarily perform a name resolution of the connection request if the request specifies a host name, rather than an IP address of the target device." *Id.* (citing Ex. 1005 ¶ 228).

Step (2) of claim 1 recites "determining whether the request to look up the IP address transmitted in step (1) corresponds to a device that accepts an encrypted channel connection with the client device." Petitioner contends that Aventail "determines whether or not the connection needs to be . . . encrypted." Pet. 33 (citing Ex. 1009, 10). Petitioner quotes from page 10 of Aventail that when a connection request is received "it

determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) **and/or encrypted** (in SSL)." *Id.* at 33–34. Specifically, Petitioner argues that if the Aventail system is configured to encrypt all communications, and the DNS request is proxied to an Aventail Extranet Server for handling, encryption of all communications occurs. *Id.* at 34 (citing Ex. 1009, 73).

Step (3) of claim 1 recites, in pertinent part, in response to step (2), "providing provisioning information required to initiate . . . [an] encrypted communications channel." Petitioner argues that Aventail discloses that encryption according to a known encryption standard, Secure Sockets Layer (SSL). Pet. 35–36 (citing Ex. 1009, 12, 73, 110; Ex. 1005 ¶¶ 247–250). The Extranet server, according to Petitioner, can be configured to send a digital certificate to the client, which verifies the Extranet server. *Id.* at 36 (citing Ex. 1009, 47–51); *see also* Ex. 1009, 47–51. Petitioner argues the certificate and selection of the encryption method are each "provisioning information" as claimed because they are provided for use in establishing the encrypted link. *Id.* at 36. Petitioner cites to other disclosures of Aventail to further support its contention that step (3) is taught by Aventail. *Id.* at 36–38.

Petitioner argues separately that the last portion of step (3), "the client device being a device at which a user accesses the encrypted communications channel," is also taught by Aventail. Pet. 38–39. Specifically, Petitioner argues that Aventail "is designed to run on remote workstations" and the "users of these workstation access

remote hosts using the encrypted connection" described. *Id.* (citing Ex. 1009, 65).

Petitioner acknowledges that "Aventail does not, however, expressly describe systems in which encrypted data sent by a client computer remains encrypted until it is received by the ultimate destination of that communication (so-called 'end-to-end' encryption)." Pet. 39. Petitioner cites to RFC 2401 in its "Case 4" example, as teaching a configuration for sending encrypted network traffic through proxy or firewall computers, such as the Aventail Extranet Server, without being decrypted, and then being decrypted by a remote computer. *Id*. at 40 (citing Ex. 1005 ¶ 364)(*see* Ex. 1008, 25–26 (Case 4)).

Petitioner argues that one of ordinary skill in the art would combine RFC 2401 with Aventail because Aventail shows encryption over at least part of the connection path while RFC 2401 shows encryption over the entire connection path. Pet. 41 (citing Ex. 1005 ¶¶ 365–382). For the encryption limitation of claims 1 and 21, Patent Owner cites to the testimony of Dr. Monrose but does not specifically argue why the combination would not have been made by the person of ordinary skill in the art, instead arguing the path between the client device and the target device is not "direct." *See* PO Resp. 23–25 (citing Ex. 2016 ¶ 39). Dr. Monrose acknowledges that Aventail discloses encryption over part of the path between the client device and the target device. *See* Ex. 2016 ¶¶ 34–35, 38. While acknowledging that the combination alleged includes RFC 2401, Dr.

Monrose does not clearly articulate any reason why the person of ordinary skill would not have combined Aventail with RFC 2401. *Id.* ¶ 39.

The record supports Petitioner's showing as summarized above, and we expressly adopt Petitioner's reasons for combining Aventail and RFC 2401. On the record before us, we are persuaded that Petitioner has provided sufficiently an articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

2. Patent Owner's Assertions

Patent Owner makes the following arguments in connection with claim 1, which also apply to claim 21. First, Patent Owner alleges Aventail does not disclose step (2) of claim 1, which recites "determining whether the request to look up an IP address intercepted[27] in step 1 corresponds to a device that accepts an encrypted channel connection with the client device." PO Resp. 18–23. Second, Patent Owner argues Aventail does not disclose the recited "*encrypted communications channel* between the client device and the target device." *Id.* at 23–25. Third, Patent Owner argues Aventail does not disclose ""in response to determining, in step (2), that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing *provisioning information* required to

[27] As indicated above (note 6), we proceed on the basis that the claim reads "intercepted" instead of "transmitted."

initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices, the client device being a device at which a user accesses the encrypted communications channel." PO Resp. 25–34. Patent Owner's second and third arguments focus on the italicized words, which we construed in Sections II.A.2. and 3 above.

Patent Owner does not dispute every allegation made in the Petition relating to the steps of claim 1 or the limitations of claim 21. As detailed above, we have reviewed the evidence and argument of the allegations not disputed by Patent Owner and find that Petitioner has shown by a preponderance of the evidence that those steps of claim 1 and limitations of claim 21 are disclosed by Aventail in combination with RFC 2401. Each of Patent Owner's arguments will be addressed below.

a. Determining Step

Claim 1 recites, in pertinent part, "determining whether the request to look up an IP address intercepted in step 1 corresponds to a device that accepts an encrypted channel connection with the client device." Patent Owner argues the "determining" of step (2) is not shown in the cited portions of Aventail. PO Resp. 17–23 (citing Pet. 32). Patent Owner argues the Petition alleges the determining of step (2) is shown because:

> Aventail discloses determining whether a domain name specified in a connection request (alleged 'intercepted DNS request,' *see* Pet at 32) matches a domain name of a remote host

> in Aventail Connect's table of redirection rules. (Pet at. 33–35, citing Ex. 1009 at 8–9, 11–12, 40.)

Id. at 17. Patent Owner argues "a domain name is never specified **in the connection request**." *Id.* at 18–19 (citing Ex. 2016 ¶¶ 29–30).

Patent Owner's argument appears to be that the Petition relied on Aventail disclosing a "*domain name*" to show the "determining" step when the claim language under consideration is "determining whether the request to look up the *IP address*" corresponds to a device that accepts an encryption connection. *See* PO Resp. 17–23 (emphasis added). Based on the preceding, Patent Owner argues the Petition is defective. Patent Owner confirmed this position at the final oral hearing, where counsel for Patent Owner stated "[o]ur argument was Apple's mapping. Apple's mapping was that there is a *domain name* in the connection request." Tr. 53:9–17 (emphasis added). Patent Owner's argument is flawed for the following reasons.

Patent Owner overlooks the showing made by Petitioner in step (1) of claim 1, "intercept[ing] . . . a request to look up an [] IP address corresponding to a domain name associated with the target . . . ." The "determining" step, step (2), specifically refers to "step (1)." Petitioner cites the following as showing step (1):

> Aventail discloses that *to connect* to a "Remote Host" ("target device"), an application on the client device "executes a Domain Name System (DNS) lookup to *convert the hostname into an Internet Protocol (IP) address*.

Pet. 31 (citing Ex. 1009, 8; *see* Ex. 1009, 11; Ex. 1005 ¶¶ 210; *see also* Ex. 1009, 91–92 (accessing remote hosts using Secure Extranet

Explorer)) (emphasis added). Petitioner notes that the Petition identifies a second "interception," i.e., Aventail discloses a "technique of proxying that same 'request' to the Aventail Extranet Server, which receives the request and resolves the hostname into an IP address." Pet. Reply 7 (citing Pet 32; Ex. 1009, 12, 61). We determine the Petition shows the recited "IP address" of step (1) as specifically recited in step (2), the "determining" step.

Patent Owner relies on testimony from Dr. Monrose to support its position. PO Resp. 18–19. We have reviewed the cited portions of the Monrose Declaration, paragraphs 29 and 30. Paragraph 29 summarizes the Petition's showing on the determination step. Paragraph 30 is an analysis of Dr. Tamassia's deposition testimony made to support the original premise of Patent Owner's argument that "a domain name is never specified in the connection request." For reasons set forth above, we understand the Petition to rely on the analysis for step (1) of the claim in the portion of step (2) that explicitly refers to that step.

Moreover, we credit Dr. Tamassia's testimony regarding the disclosure of Aventail. Ex. 1005 ¶¶ 142–145, 160–273. Dr. Monrose's testimony does not persuade us otherwise because, as Petitioner points out, Dr. Monrose:

> never considered the Petition's actual analysis, and explained that he had not "look[ed] at all the other claimed analysis" and "didn't go through all the pages" of testimony to see if Dr. Tamassia or Petitioner had "pointed to something else as" fulfilling the claimed "request," instead focusing exclusively on a presumed

> change in position discerned from only two lines in Dr. Tamassia's deposition.

Pet. Reply 7–8 (citing Ex. 1066, 14:5–8, 16:22–17:2, 20:14–21:7). For these reasons, we are not persuaded by Patent Owner's argument that the Petition does not "map" Aventail to the "determining" step, step (2).

Patent Owner also argues that Aventail's "proxy request" is part of the SOCKS negotiation described in Aventail. PO Resp. 19. Patent Owner contends the SOCKS negotiation occurs *after* the connection request is received in step 2.[28] *Id.* (citing Ex. 2013 (steps 2, 2a); Ex. 2016 ¶ 31). Relying on Exhibits 2013 and 2014[29] and testimony of Dr. Monrose, Patent Owner contends Dr. Tamassia agrees. *Id.* Patent Owner concludes "*Aventail* thus shows that the proxy request, which is sent after the connection is completed, is never matched against a redirection rules table because the matching occurs earlier in step 1b of *Aventail* and the proxy request is not even sent until step 2b(3)." *Id.* (citing Ex. 1009, 11–12; Ex. 2013; Ex. 2016 ¶ 32).

We do not agree with Patent Owner's characterization of Aventail's disclosure. Specifically, we disagree with Patent Owner's assertion that step 1 of Aventail is separate and distinct from step 2. Each applies under different circumstances and Patent Owner's dissection of one from the other

[28] This relates to "steps" described at the cited pages 11 and 12 in Aventail (Ex. 1009) and not the steps of claim 1.
[29] Exhibit 2014 contains a flow chart from the Tamassia Declaration (Ex. 1005 ¶ 218) which was marked as an exhibit in the Tamassia Deposition along with Exhibit 2013, Dr. Tamassia's markup of pages 11 and 12 of Aventail. Ex. 1068 (also identified as Ex. 2015), 247:6–248:23.

fails to take into account what a person of ordinary skill in the art would understand from the disclosure.

We credit Dr. Tamassia's testimony as being a factually detailed discussion of Aventail and drawing reasonable conclusions based on what Aventail discloses. *See* Ex. 1005 ¶¶ 142–145, 160–273. For example, Dr. Tamassia opines that:

> As part of the redirection rule, Aventail provides three options for handling requests, as illustrated in the figure below: all traffic to a particular destination can be blocked (denied); all traffic could be routed to a specified Aventail ExtraNet Server; or traffic can be routed directly to specified destination, bypassing the Extranet Server in its entirety. Ex. 1009 (ACAG) at 40. These options are mutually exclusive. Ex. 1009 (ACAG) at 40 ("Under 'Proxy Redirection,' select one of three redirection options.").

Ex. 1005 ¶ 236. Additionally, Dr. Tamassia testifies:

> if Aventail Connect determines that the hostname in the intercepted DNS request matches one of the destinations for which a redirection rule has been defined, then Aventail Connect will evaluate the redirection rule to determine if the target host is one for which proxy redirection (and an encrypted communication) through the Aventail Extranet Server is required.

Ex. 1005 ¶ 237 (citing Ex. 1009, 11). The Petition specifically relies on the preceding testimony and cites to the Tamassia Declaration for support regarding the "determining" step. *See* Pet. 33–35 (citing Ex. 1005 ¶¶ 229–237).

We have also reviewed the Tamassia Deposition testimony relied on by Patent Owner for its timing argument and do not agree with Patent

Owner's characterization of the testimony. PO Resp. 19 (citing Ex. 2015, 226:1–10, 194:23–195:5). Aventail at page 12, step 2b (*see* Ex. 2013) reads "[w]hen the connection is completed, Aventail Connect begins the SOCKS negotiation." Ex. 1009, 12. That Dr. Tamassia agrees with what is written adds nothing.[30] Dr. Monrose's testimony, which simply repeats what is in the Response, is also unavailing. Ex. 2016 ¶ 32 ("One of ordinary skill in the art would have understood that . . . the proxy request, which is sent after the connection is completed, is never matched against a redirection rules table because the matching occurs earlier in Step 1b of Aventail."). As set out in part above, Dr. Tamassia's testimony is not as limited as Patent Owner argues.

Patent Owner fails to persuade us that its timing argument is relevant to the showing in the Petition. The sequence of steps identified by Patent Owner are not relevant because they are not what Petitioner relies on to show the determining step and were not argued by Petitioner. Neither does the argument persuade us that Aventail does not disclose the determining step.

Patent Owner argues that Aventail does not show that the remote host will "accept" an encrypted connection as per claim 1's determining step (2). PO Resp. 21. Patent Owner acknowledges that "Aventail Connect 'determines whether . . . the connection needs to be . . . encrypted (in SSL).'" PO Resp. 21 (citing Ex. 1009, 10).

[30] "So that's what it says. As I mentioned before, I have given somewhat broader interpretation, given the context." Ex. 1068 (also identified as Ex. 2015), 194:23–25.

Petitioner alleges "[i]nclusion of the remote host in the redirection rule table therefore enables the Aventail Connect client to determine if the remote host will accept an encrypted connection (*"corresponds to a device that accepts an encrypted channel connection with the client device"*) by checking to see if the remote host is listed in the redirection rule table." Pet. 34 (citing Ex. 1009, 8–9, 11–12, 40; *see also* Ex. 1003 ¶ 237[31]). Patent Owner does not respond to the showing of Petitioner other than denying that Aventail's redirection table says anything about whether the remote host accepts encrypted communication. PO Resp. 21–22; Tr. 55:7–10.

Dr. Monrose's cited testimony does not change our determination. Dr. Monrose opines that a person of ordinary skill, even in view of his acknowledgement that Aventail teaches "determin[ing] whether . . . the connection needs to be . . . encrypted (in SSL)." Ex. 2016 ¶ 35. The opinion addresses neither its predicate, the connection needs to be encrypted, nor Petitioner's showing. As such, the opinion lacks sufficient underlying facts or data. 37 C.F.R. § 42.65(a).

Patent Owner also agrees that Aventail teaches the remote connection may result in the connection being proxied. PO Resp. 22 (citing Ex. 2016 ¶ 36). Nonetheless, Patent Owner argues a proxied connection alone "does not disclose or suggest that the remote host is one that accepts an encrypted connection." *Id.*

We disagree. Aventail teaches that:

> Aventail Connect can change data (compressing it or *encrypting* it, for example) before routing it to the TCP/IP stack for transport over the network. The routing is determined by the rules described in the configuration file.

[31] Exhibit 1003, US Patent No. 8,850,009, has no paragraph 237.

Ex. 1009, 9 (emphasis added). Step 3 of Aventail also states that "Aventail Connect encrypts the data on its way to the server." *Id.* at 12. Petitioner cites to the preceding pages of Aventail in its showing that Aventail shows the "accepts an encrypted channel connection with the client device" of step (2) of claim 1. *See* Pet. 34.

b. Encrypted Communications Channel

Patent Owner contends Aventail does not disclose "an encrypted communications channel between the client device and the target device," as recited in the preamble. PO Resp. 23–25. Patent Owner's argument is premised on its proposed construction of "encrypted communications channel," which requires a "direct" communications channel. *Id.* at 23 (citing Section II.B. of the Response).

We interpret "encrypted communications channel" to mean "a transmission path that restricts access to data, addresses, or other information on the path, hiding information on the path using encryption." *See supra* Section II.A.2. In our analysis, we reject specifically Patent Owner's proposed construction which includes "direct."

Even were "direct" communication part of the construction of "encrypted communication channel," Patent Owner's argument fails. We agree with Petitioner that:

> neither Patent Owner nor its expert have attempted to explain what is required by "direct[ness]." Resp. at 8–10, 23–24. To the extent the term itself is informative, Aventail describes the "network connections" that are proxied between client computers and those on the private network as "direct network connections." Ex. 1009 at 72 ("[N]o ***direct network connections*** between the public LAN and the private LAN can

> be created ***without being securely proxied*** through the Aventail ExtraNet Server.").

Pet. Reply 11. Accordingly, we are not persuaded by Patent Owner's argument that Aventail does not disclose an "encrypted communications channel."

c. Provisioning Information

Claim 1 recites, in pertinent part, "that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device, providing *provisioning information* required to initiate the creation of the encrypted communications channel between the client device and the target device such that the encrypted communications channel supports secure data communications transmitted between the two devices." Ex. 1001, 55:43–67 (emphasis added).

Patent Owner argues, citing language from claim 1, that "provisioning information" includes two requirements. First, according to Patent Owner, provisioning information "must be *required to initiate the creation of the encrypted communications channel* between the client device and the target device." PO Resp. 25–26 (citing Ex. 2016 ¶ 41). Second, Patent Owner contends that provisioning information must be provided in response to determining that the request to look up the IP address in step (2) corresponds to a device that accepts an encrypted communications channel connection with the client device." *Id.* Patent Owner contends the Petition identifies four separate instances of "provisioning information" disclosed in Aventail, none of which meet both requirements. *Id.* at 26.

We address each of these sections of the Petition below.

(1) HOSTENT

The Petition alleges HOSTENT is "*required* to identify subsequent communications so that the communications can be sent over the encrypted connection once the connection was initiated." Pet. 36 (citing Ex. 1009, 8–9, 11–12; Ex. 1005 ¶ 237) (emphasis added). Patent Owner argues that "*Aventail* discloses at least one scenario in which an encrypted connection can be created between the client device and the SOCKS server where *Aventail* Connect does not provide HOSTENT to the client application." PO Resp. 27 (citing Ex. 2016 ¶ 44).[32] Thus, Patent Owner concludes Petitioner's analysis is "incorrect" because "HOSTENT is *not required* to initiate the creation of the encryption connection." *Id.* at 29 (citing Ex. 2016 ¶ 46) (emphasis added).

We reject Patent Owner's argument because any alleged discrepancy between the Petition and "one scenario" which is not "required" to initiate the "encrypted communication channel" is not fatal to the Petition. Further, the Petition explains that all hostnames requiring redirection to an Aventail Extranet Server may require encryption of all communications. Pet. 34 (citing Ex. 1009, 73). Thus, the HOSTENT returned by Aventail Connect is "required," i.e., "initiate[s] the creation of" an encrypted communication and "enable[s] or aid[s] in establishing a secure communications channel." *Id.*; *see also* Pet. Reply 12.

Patent Owner also argues the Petition fails to show any relationship between an "encrypted connection" and HOSTENT. PO Resp. 29 (citing

[32] None of the citations to the Monrose Declaration add anything to the Response. The Response and the Monrose Declaration are essentially identical.

Pet. 36; Ex. 2016 ¶ 47). Neither claim 1 nor the claim term "provisioning information" requires any relationship. We are not persuaded by Patent Owner's arguments.

(2) TCP Sequence Numbers

The Petition alleges that TCP sequence numbers are exchanged during a TCP handshake between the client device and the SOCKS server and that TCP numbers are "provisioning information." Pet. 36 (citing Ex. 1009, 12; Ex. 1005 ¶¶ 117–119, 210, 238; DARPA Internet Program, Protocol Specification, *Transmission Control Protocol*, 27 (Ex. 1014)). Patent Owner again argues the Petition did not show a "relationship" between the TCP sequence numbers and an encrypted connection. PO Resp. 30–31. Claim 1 does not require the specific relationship Patent Owner alleges is necessary for "provisioning information."

Patent Owner also argues that the TCP connection is with the SOCKS server and not the remote host in Aventail. PO Resp. 30–31. "Direct" connection is not required under our construction, only a path. Even were it ultimately decided that a "direct" connection is required, the ground alleged is the combination of Aventail and RFC 2401. RFC 2401 "shows an encrypted connection to the remote host." *See* Pet. Reply 13.

We are not persuaded by Patent Owner's arguments.

(3) Selection of Encryption Method and Certificate Exchange

The Petition alleges Aventail can perform a certificate exchange with the SOCKS server and also receives a selection of an encryption method from the server. Pet. 35–36 (citing Ex. 1009, 47–51). We expressly find that the certificate and selection of the encryption method are each '*provisioning information*' because they are provided for use in establishing

the encrypted link." *Id.* at 36. Patent Owner argues "no encrypted connection exists to the remote host in *Aventail*" and the certificate exchange and selection of encryption method "cannot be required to 'initiate the creation of the encrypted communications channel *between the client device and the target device.*'" PO Resp. 31–32 (citing Ex. 2016 ¶ 53).

"Direct" connection is not required under our construction, only a path. Even were it ultimately decided that a "direct" connection is required the ground alleged is the combination of Aventail and RFC 2401. RFC 2401 "shows an encrypted connection to the remote host." *See* Pet. Reply 13.

We are not persuaded by Patent Owner's argument.

(4) SOCKS Exchanges

The Petition alleges "SOCKS negotiation" or SOCKS exchanges performed by Aventail qualify as "provisioning information." Pet. 37–38 (citing Ex. 1009, 12; Ex. 1005 ¶¶ 241–243). In addition, the Petition alleges:

> a person of ordinary skill in the art would also have understood that the SOCKS 5 standard specifies this SOCKS negotiation, and according to standard, if the client computer is allowed access to the requested remote host, the Extranet server will send a "succeeded" response to the client that provides the BIND network address and BIND network port to which the client computer should send its encrypted communications.

Id. at 37 (citing Network Working Group, Request for Comments, *SOCKS Protocol Version 5*, 5–6, IETF RFC 1928 (Ex. 1018); Ex. 1005 ¶ 243).

Patent Owner again argues the SOCKS negotiations "do not initiate the creation of the encrypted communications." PO Resp. 32 (citing Ex. 2016 ¶¶ 54–55). In other words, claim 1 requires the "provisioning information" "to initiate the creation of the encrypted communications channel between the client device and the target device." *See* Pet. Reply 14.

The above passage shows that the relied-upon information does serve to initiate the creation of the encrypted channel, because without it, no such channel would be created.

Patent Owner then argues a "particular message" must be identified as the "provisioning information." PO Resp. 32. Patent Owner contends the SOCKS exchange cannot be "provisioning information" because "the claimed provisioning information must have some relationship to and be *required* for the 'encrypted connection,' which Petitioner fails to demonstrate exists." *Id*. at 33 (citing Ex. 2016 ¶¶ 56, 57).

Claim 1 does not require a specific message. Regardless, Petitioner argues persuasively that "the Petition identified specific messages exchanged during the SOCKS negotiation, including 'a 'succeeded' response to the client that provides the network address and network port of the server to which the client computer should send its encrypted communications.'" Pet. Reply 14 (citing Pet. 37, Ex. 1009, 12; Ex. 1018, 5–6; Ex. 1005 ¶¶ 241–243).

We are not persuaded by Patent Owner's arguments.

3. Conclusion

We expressly agree with Petitioner's reasons for combining Aventail and RFC 2401 and determine that Petitioner has shown by a preponderance of the evidence that claims 1 and 21 would have been obvious over Aventail combined with RFC 2401.

H. Claims 2, 16, and 33

Claim 2 depends from claim 1 and recites, in pertinent part, "a determination that the target device is a device with which an encrypted communications channel can be established." Claim 16 depends from claim

1 and claim 33 depends from claim 21. Similar to claim 2, claims 16 and 33 recite a determination "whether the target device accepts an encrypted channel connection."

For claim 2, Petitioner cites Aventail's description that "SSL parameters, HOSTENT, SOCKS parameters, and TCP sequence numbers are provided only if it is determined that the domain name lookup corresponds to a remote host for which an encrypted connection is required." Pet. 43–44 (citing Ex. 1009, 11–12; Ex. 1018, 5–6); Pet. 35–38 (allegations for "provisioning information" step (3) of claim 1). Petitioner concludes "Aventail in view of RFC 2401 therefore would have rendered claim 2 obvious." *Id.* at 44.

Regarding claims 16 and 33, Petitioner argues the reason "Aventail and the Aventail Extranet server intercept requests to look up IP addresses is to determine whether the request corresponds to a remote host ('*target device*') for which an encrypted link needs to be created." Pet. 48 (citing Ex. 1009, 11–12, 72–73). Petitioner concludes "as explained above, the [sic] Aventail in view of RFC 2401 teaches a scheme in which link are encrypted end-to-end." *Id.* (citing Pet. 33–35 (regarding step (2), the "determining" step)), 39–43 (regarding combining Aventail with RFC 2401)).

Patent Owner references its argument above that Aventail does not disclose the "determining" step: "while inclusion of a remote host within a redirection table may indicate that communication to the remote must be proxied, it does not suggest that the remote host (alleged "target device") accepts an encrypted connection." PO Resp. 35. As detailed above, we do not agree with Patent Owner on this issue. Patent Owner also contends Petitioner does not cite the encryption reference, RFC 2401. *Id*. (citing Ex.

2016 ¶¶ 58–60). However, Petitioner does rely on the combination of Aventail and RFC 2401 as discussed in this section. Pet. 39–43, 48.

We agree with Petitioner's reasons for combining Aventail and RFC 2401 and determine that Petitioner has shown by a preponderance of the evidence that claims 2, 16, and 33 would have been obvious over Aventail combined with RFC 2401.

I. Claims 3 and 25

Dependent claim 3 depends from claim 1. Claim 25 depends from claim 21. Claims 3 and 25 each recite that the "domain name" recited in claims 1 and 21 is a "secure domain name." Above we construe "secure domain name" as "a name that corresponds to a secure computer network address." Petitioner argues "Aventail shows private domain name servers that are accessible only by way of a secure connection that is both authenticated and encrypted." Pet. 44 (citing Ex. 1009, 73 (encryption and authentication requirements), 74 (depicting a DNS server on the private network); Ex. 1005 ¶¶ 224, 243).

Patent Owner argues that Aventail does not disclose that the domain name submitted to the SOCKS server for resolution is resolved by the private DNS. PO Resp. 36–37. Patent Owner also argues, based on its proposed construction, that the "secure domain name" must be "non-standard." *Id.* at 37.

We do not agree with Patent Owner's first argument because Aventail describes that "the SOCKS server performs the hostname resolution" and shows a private DNS server to allow for hostname resolution on the private network. Ex. 1009, 12, 72.

We also do not agree with Patent Owner's second argument. As discussed above, our construction of "secure domain name" reject Patent Owner's argument that a secure domain name is a "non-standard domain name." Patent Owner does not argue that claims 3, 10, and 25 would not have been obvious under our construction of "secure domain name."

Even were we to adopt Patent Owner's proposed construction, Aventail discloses "non-standard" domain names. For example, Aventail explains that "[i]f the DNS proxy option is enabled and *the domain cannot be looked up directly*, Aventail Connect *creates a fake DNS entry* that it can recognize later, and returns this to the calling application." Ex. 1009, 12 (emphasis added). The "fake DNS entry" is not standard because it is an artifice for a domain name that cannot be looked up.

We expressly agree with Petitioner's reasons for combining Aventail and RFC 2401 and determine that Petitioner has shown by a preponderance of the evidence that claims 3 and 25 would have been obvious over Aventail combined with RFC 2401.

J. Claims 17 and 34

Dependent claims 17 and 34 depend from claims 1 and 21 respectively. Each recites that the "intercept[ion]"occurs within another device that is separate from the client device." Aventail "intercept[s]" the request to look up an IP address in two distinct ways: (1) on the client via Aventail Connect, and (2) on the Aventail Extranet Server. *See* Pet. 31–32; Ex. 1009, 11-12; Ex. 1005 ¶¶ 209–256. In this second case, the "intercept[ion]" occurs within a device "separate from the client device." Pet. 48; Ex. 1009, 72.

Patent Owner argues that the "determining" step of claims 1 and 21 must necessarily occur after the "intercepting" step. *See* Resp. 39-40. There is no basis for this requirement in the plain language of the claims. "Unless the steps of a method [claim] actually recite an order, the steps are not ordinarily construed to require one." *Interactive Gift Express, Inc. v. Compuserve Inc.*, 256 F.3d 1323, 1342 (Fed. Cir. 2001). The claimed "intercepting" (step 1) and "determining" (step 2) refer to the same transmitted "request," but the claims require no specific order, and Patent Owner cannot dispute that the "domain name" transmitted in the request before the "determinat[ion]" in Aventail is the same "domain name" received and resolved by the Aventail Extranet Server. Ex. 2015, 193:18–22. Moreover, the reference to "the request to look up the IP address transmitted in step (1)" serves to indicate the antecedent basis for the request, not introduce some temporal relationship between the steps.

We agree with Petitioner's reasons for combining Aventail and RFC 2401 and determine that Petitioner has shown by a preponderance of the evidence that claims 17 and 34 would have been obvious over Aventail combined with RFC 2401.

K. Claims 6, 14, 16, 18–20, 22–24, 28, and 31

Petitioner asserts that the combination of Aventail and RFC 2401 teaches each of the limitations of claims 6, 16, 18–20, 22–24, 28, and 31. We have reviewed Petitioner's evidence regarding these claims. *See* Pet. 46–51. According to Petitioner, Aventail in conjunction with RFC 2401 or the knowledge of a person of ordinary skill in the art would have rendered obvious the limitations added to independent claims 1 and 21 by the challenged dependent claims 6, 16, 18–20, 22–24, 28, and 31. *See*, e.g., Pet.

47, regarding claims 6 and 28 (citing Ex. 1005 at ¶¶ 79, 190; MICROSOFT COMPUTER DICTIONARY, 294 (4th ed. 1999) (Ex. 1019) ("When transmitting, modems impose (modulate) a computer's digital signals onto a continuous carrier frequency on the telephone line. When receiving, modems sift out (demodulate) the information from the carrier and transfer it in digital form to the computer.")).

Patent Owner does not separately challenge claims 6, 16, 18–20, 22–24, 28, and 31. PO Resp. 40. Patent Owner does not separately argue claim 14. The limitation in claim 14 is the same as in claim 31, which was not separately argued. *Id.* We agree with Petitioner's reasons for combining Aventail and RFC 2401 and determine that Petitioner has shown by a preponderance of the evidence that claims 6, 14, 16, 18–20, 22–24, 28, and 31 would have been obvious over Aventail combined with RFC 2401.

OBVIOUSNESS-AVENTAIL, RFC 2401, AND RFC 2543

L. Overview of RFC 2543

RFC 2543 describes a network-based secure video telephony architecture that supports both audio and video conferences. Ex. 1013, 1. These sessions include Internet multimedia conferences, Internet telephone calls, and multimedia distribution. *Id.* RFC 2543 discloses that these multimedia telephony sessions may be encrypted. *Id.* 54.

M. Claims 8–10, 12, 15, 30, and 32

Petitioner asserts that the combination of Aventail, RFC 2401, and RFC 2543 teaches each of the limitations of claims 8–10, 12, 15, 30, and 32. We have reviewed Petitioner's evidence regarding these claims. *See* Pet. 51–55. According to Petitioner, Aventail in combination with RFC 2401, RFC 2543, or the knowledge of a person of ordinary skill in the art would

have rendered obvious the limitations added to independent claims 1 and 21 by the challenged dependent claims 8–10, 12, 15, 30, and 32. *See*, e.g., Pet. 51–54, regarding claims 8, 15, 20, and 32 (where the client device or the target device is a phone):

> A person of ordinary skill in the art would have further considered the teachings of RFC 543 [2543] in implementing Aventail in the end-to-end encryption configuration suggested by RFC 2401. RFC 2543 shows a network-based secure video telephony architecture that supports both audio and video conferences.

We are persuaded that RFC 2543 would have been combined with Aventail because persons of ordinary skill in the art would have "recognized the telephony functionality taught by RFC 2543 would have been one of the protocols that could be utilized with the protocol-independent multipurpose scheme taught by Aventail." Pet. 53 (citing Ex. 1005 ¶ 422). Moreover, "including network-based telephony services on a single, common communications architecture was both desirable and a conventional design technique." *Id.* Finally, we agree that a person of ordinary skill would have found it obvious to make this combination because "it would enable the organization to consistently implement and regulate security and access control measures." *Id.*

Patent Owner does not separately challenge claims 8–10, 12, 15, 30, and 32, raising only arguments we previously found not persuasive. PO Resp. 40–41. For example, claim 9 is argued as patentable for the same reasons we rejected in connection with claim 2. *Id.* at 41. We agree with Petitioner's reasons for combining Aventail, RFC 2401, and RFC 2543 and determine that Petitioner has shown by a preponderance of the evidence that

claims 8–10, 12, 15, 30, and 32 would have been obvious over Aventail, RFC 2401, and RFC 2543.

OBVIOUSNESS-AVENTAIL, RFC 2401, AND BRAND

N. Overview of Brand

Brand discloses that networks can be categorized into two basic networks based on the type of bandwidth used in the network: "broadband systems and baseband systems." Ex. 1012, 1:26–29; Ex. 1005 ¶¶ 406–408. Brand also discloses that baseband networks are "unmodulated." Ex. 1012, 1:31–33.

O. Claims 4, 5, 7, 26, 27, and 29

Petitioner asserts that the combination of Aventail, RFC 2401, and Brand teaches each of the limitations of claims 4, 5, 7, 26, 27, and 29. We have reviewed Petitioner's evidence regarding these claims. *See* Pet. 55–58. According to Petitioner, Aventail in combination with RFC 2401, and Brand, including the knowledge of a person of ordinary skill in the art, would have rendered obvious the limitations added to independent claims 1 and 21 by the challenged dependent claims 4, 5, 7, 26, 27, and 29. *See*, e.g., Pet. 55–56, regarding claims 4 and 26 ("wherein the encrypted communication channel is a broadband connection") (citing Ex. 1005 ¶ 412; Ex. 1015,[33] 1:26–29 ("It would have been obvious for a person of ordinary skill in the art to choose to use a broadband network to implement Aventail's public network connection because a broadband network is one of the two basic types of networks.")). Based on the preceding, there are two basic types of networks, and that implementing Aventail on a broadband network would be a routine design choice because of the "finite set of predictable

[33] US Patent No. 6,430,176 to S. Christie IV, issued August 6, 2002.

alternatives," we are persuaded that Brand would have been combined with Aventail. *See* Pet. 56.

Patent Owner does not separately challenge claims 4, 5, 7, 26, 27, and 29. PO Resp. 41. We agree with Petitioner's reasons for combining Aventail, RFC 2401, and Brand and determine that Petitioner has shown by a preponderance of the evidence that claims 4, 5, 7, 26, 27, and 29 would have been obvious over Aventail, RFC 2401, and Brand.

OBVIOUSNESS-AVENTAIL, RFC 2401, RFC 2543, AND BRAND

P. Claims 11 and 13

Petitioner asserts that the combination of Aventail, RFC 2401, RFC 2543, and Brand teaches each of the limitations of claims 11 and 13, both of which depend from claim 8. We have reviewed Petitioner's evidence regarding these claims. *See* Pet. 58–59. According to Petitioner, Aventail in combination with RFC 2401, RFC 2543, Brand, or the knowledge of a person of ordinary skill in the art would have rendered obvious the limitations added to independent claims 1 and 21 by the challenged dependent claims 11 and 13. *See*, e.g., Pet. 58, regarding claim 11 (citing to the showing on claims 5 and 27 which include the same limitation). Petitioner has shown that Aventail would have been combined by the person of ordinary skill in the art with RFC 2401, RFC 2543, and Brand.

Patent Owner does not separately challenge claims 11 and 13. PO Resp. 42. We agree with Petitioner's reasons for combining Aventail, RFC 2401, RFC 2453, and Brand and determine that Petitioner has shown by a preponderance of the evidence that claims 11 and 13 would have been obvious over Aventail, RFC 2401, RFC 2453, and Brand.

Q. Patent Owner's Motion to Exclude

Patent Owner seeks to exclude Exhibits 1003, 1004, 1007, 1015–1017, 1024–1035, 1037–1041, 1043–1048, 1057–1060, 1063–1065, and 1067–1069, and Portions of Exhibit 1005. Paper 36, 1. 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 *denied*.

1. Exhibits 1022, 1023, 1043, and 1057–1059

Patent Owner seeks to exclude Exhibits 1022, 1023, 1043, and 1057–1059 (collectively, the "Aventail declaration testimony") as inadmissible hearsay. Paper 36, 2. As detailed above, Exhibit 1023 is the Hopen Declaration, Exhibit 1043 is the Fratto Declaration, and Exhibit 1022 is the Chester Declaration. The preceding were relied on in the Petition to establish that Aventail is prior art. *See* Pet. 15–16. Also discussed above are Exhibits 1057–1059, which Petitioner served in response to Patent Owner's objections and submitted as supplemental evidence. *See* Paper 21. Exhibit 1057 is the deposition transcript of Mr. Hopen from a district court proceeding, and Exhibit 1058 is a second declaration of Mr. Hopen from a reexamination proceeding. Exhibit 1059 is a portion of deposition testimony read into evidence in the above-mentioned district court trial. The exhibits are relevant to whether or not Aventail is prior art, as detailed in Section II.D.1 above.

Although the Aventail declaration testimony was originally filed in other proceedings and not specifically created for this proceeding, the main distinction between it and the expert declaration testimony of Dr. Tamassia and Dr. Monrose is the caption. That difference is artificial because all of

the declarations were filed in this proceeding, as if they were prepared for this matter. Indeed, Patent Owner chose not to seek the opportunity to cross examine the declaration testimony. *See* 37 C.F.R. § 42.51(b)(ii); Opposition to Motion to Exclude 3 ("Opp. to Mot. to Exclude," Paper 38); Tr. 63:14–65:22, 68:21–69:16.

Even if considered hearsay, Federal Rule of Evidence 807 provides a "residual exception" to the hearsay rule, which may apply even if no specific exception of Federal Rule of Evidence 803 applies. We determine that the exception applies here. To fall under this exception, the statement must: 1) have equivalent circumstantial guarantees of trustworthiness; 2) be offered as evidence of a material fact; 3) be more probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts; and 4) be in the interests of justice to admit. Fed. R. Evid. 807. The residual exception to the hearsay rule is to be reserved for "exceptional cases," and is not "a broad license on trial judges to admit hearsay statements that do not fall within one of the other exceptions." *Conoco Inc. v. Dep't of Energy*, 99 F.3d 387, 392 (Fed. Cir. 1996), as amended on rehearing in part (Jan. 2, 1997) (internal quotations omitted). Trial courts are accorded wide discretion in applying the residual hearsay exception. *Doe v. United States*, 976 F.2d 1071, 1076–77 (7th Cir. 1992), *cert. denied* 510 U.S. 812 (1993); *United States v. North*, 910 F.2d 843, 909 (D.C. Cir. 1990) *cert. denied* 500 U.S. 941 (1991).

Petitioner has responded to the objections by relying on Federal Rule of Evidence 807. Opp. to Mot. to Exclude 2–8. Each factor is analyzed in detail. *Id.* We agree with Petitioner's analysis. For example, we agree with Petitioner that the Aventail declaration testimony has the same

circumstantial guarantees of trustworthiness as those declarations actually created for this proceeding. *See* Opp. to Mot. to Exclude 3–7. The vast majority of testimony in *inter partes* reviews is admitted in paper form, as a declaration, instead of as live witness testimony. Thus, whether or not testimony is specifically created for a specific IPR or is created for another proceeding, if the declaration is sworn testimony and the witness is available for cross-examination, the testimony bears the same guarantees of trustworthiness. *See also* Fed. R. Evid. 804(b)(1) (exception against the rule against hearsay for former testimony that "was given as a witness at a trial, hearing, or lawful deposition" and "is now offered against a party who an opportunity and similar motive to develop it by direct, cross-, or redirect examination").

Patent Owner argues the exception should be used sparingly in exceptional cases, citing a district court case refusing to admit a declaration because of lack of showing that the case was exceptional. Paper 39, 2 (citing *Pozen Inc. v. Par Pharm., Inc.*, 696 F.3d 1151, 1161 n.6 (Fed. Cir. 2012)). Patent Owner then criticizes the testimony of each witness. *Id.* at 2–4. For example, Patent Owner argues the declarations were prepared long after the event testified about, the January 1999 distribution of Aventail. *Id.* at 2. We noted above in section II.D.1. that the testimony included documentation which corroborates the witnesses memory of the sequence of events. We are not persuaded by Patent Owner's remaining arguments.

Petitioner's showing is persuasive. We adopt the showing by Petitioner, and for those reasons, we deny Patent Owner's Motion to Exclude Exhibits 1022, 1023, 1043, and 1057–1059.

2. Exhibits 1060 and 1063–65

Patent Owner seeks to exclude Exhibits 1060 and 1063–65 as inadmissible hearsay. Paper 36, 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 36, 2 (quoting Paper 17, 5–6). Exhibits 1064 and 1065 are both magazine articles dated 1999 that relate to the same issue. Paper 17, 5–7. 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.

3. Exhibits 1003, 1004, 1007,1015–1017, 1024–1035, 1037–1041, 1044–1048, and 1067–1069

Patent Owner seeks to exclude the above listed Exhibits as lacking relevance. Paper 36, 5. Because we do not rely on the above listed Exhibits, we dismiss this request as moot.

4. 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 other proceedings, *i.e*. IPR2015-00810, 812, and 813. Paper 36, 5–6. Because we do not rely on the cited paragraphs of Exhibit 1005, we dismiss this request as moot.

ORDER

For the reasons given, it is:

ORDERED that claims 1–34 of U.S. Patent No. 8,868,705 B2 have been shown by a preponderance of the evidence to be unpatentable;

FURTHER ORDERED that Patent Owner's Motion to Exclude (Paper 36) is *dismissed* as *moot* in part and is *denied* in part; 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.

PETITIONER:

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

PATENT OWNER:

Joseph E. Palys
Naveen Modi
Daniel Zeilberger
Chestan Bansal
Jason Stach
PAUL HASTING LLP
josephpalys@paulhastings.com
naveenmodi@paulhastings.com
danielzeilberger@paulhastings.com
chetanbansal@paulhastings.com
jason.stach@finnegan.com

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