

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

APPLE INC.,  
Petitioner,

v.

VIRNETX INC.,  
Patent Owner.

---

Case IPR2014-00403<sup>1</sup>  
Patent 7,987,274 B2

---

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

EASTHOM, *Administrative Patent Judge*.

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

---

<sup>1</sup> As discussed below, IPR2014-00483 has been joined with IPR2014-00403.  
This Final Written Decision applies to the joined case.

## I. BACKGROUND

Microsoft Corporation filed a revised Petition (Paper 4) requesting *inter partes* review of claims 1–5, 7, 8, 10, 12, 13, 15, 17, and 18 of U.S. Patent No. 7,987,274 B2 (“the ’274 Patent,” Ex. 1001) pursuant to 35 U.S.C. §§ 311–319. Paper 4. The Board instituted an *inter partes* review of claims 1–5, 7, 8, 10, 12, 13, 15, 17, and 18. Paper 13 (“Inst. Dec.”).

Apple Incorporated (“Petitioner”) also filed a Petition (Paper 2) seeking an *inter partes* review of claims 1–5, 7, 8, 10, 12, 13, 15, 17, and 18 of the ’274 patent pursuant to 35 U.S.C. §§ 311–319 in Case IPR2014-00483 (“’483 IPR”). Noting that Microsoft Corporation’s Petition and Apple Incorporated’s Petition were substantially identical in material aspects, the Board instituted an *inter partes* review of claims 1–5, 7, 8, 10, 12, 13, 15, 17, and 18, and joined IPR2014-00483 with IPR2014-00403 pursuant to 35 U.S.C. § 315(c). *See* ’483IPR, Paper 11, 6–9.<sup>2</sup> Thereafter, pursuant to a settlement agreement, the present proceeding was terminated with respect to Microsoft Corporation only. Paper 38.

Prior to institution, VirnetX Incorporated (“Patent Owner”) filed a Patent Owner Preliminary Response (Paper 9) (“Prelim. Resp.”), and after institution, filed a Patent Owner Response (Paper 26) (“PO Resp.”). Petitioner then filed a Reply (Paper 34) (“Pet. Reply”). An Oral Hearing transpired on April 28, 2015. Paper 41 (“Tr.”).

The Board has jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision issues pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

---

<sup>2</sup> Unless otherwise noted, all citations hereinafter are to filings in IPR2014-00403.

For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–5, 7, 8, 10, 12, 13, 15, 17, and 18 of the '274 patent are unpatentable.

*A. The '274 Patent (Ex. 1001)*

The '274 patent Specification describes secure systems for communicating over the Internet. Ex. 1001, Abstract, 9:38–39. The secure systems use a secure domain name service (SDNS): “SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS 3313 stores a computer network address corresponding to the secure domain name.” *Id.* at 47:15–19. The '274 patent Specification also describes creating a secure communication link in the form of a virtual private network (“VPN”) link. One preferable “VPN communication link can be based on a technique of inserting a source and destination IP address pair into each data packet that is selected according to a pseudo-random sequence.” *Id.* at 46:64–67. The '274 patent Specification refers to this technique and similar techniques as an “address hopping regime” or a “particular information hopping technique.” *Id.* at 47:1, 13–14.

*B. Illustrative Claim*

Claim 1 of the '274 patent, illustrative of the challenged claims, follows:

1. A method of accessing a secure network address, comprising:
  - sending a query message from a first network device to a secure domain service, the query message requesting from the secure domain service a secure network address for a second network device;

receiving at the first network device a response message from the secure domain name service containing the secure network address for the second network device; and  
sending an access request message from the first network device to the secure network address using a virtual private network communication link.

*C. Cited Prior Art*

Provino	US 6,557,037 B1	Apr. 29, 2003	(Ex. 1003)
Xu	US 6,151,628	Nov. 21, 2012	(Ex. 1007)

Dave Kosiur, *Building and Managing Private Networks* (Sept. 1, 1998) (Ex. 1006, “Kosiur”).

*D. Instituted Grounds of Unpatentability*

References	Basis	Claims Challenged
Provino	§ 102	1, 7, 8, 10, 12, 13, 15, and 17
Provino and Kosiur	§ 103	2–5
Provino and Xu	§ 103	18

*E. Claim Construction*

In an *inter partes* review, the Board interprets claim terms in an unexpired patent according to the broadest reasonable construction in light of the specification of the patent in which they appear. *In re Cuozzo Speed Techs., LLC*, No. 2014-1301, 2015 WL 4097949, at \*6 (Fed. Cir. July 8, 2015); 37 C.F.R. § 42.100(b). Under that standard, claims must be construed according to their ordinary and customary meaning, in view of the specification, as would be understood by one of ordinary skill in the art at the time of the invention. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). A “lexicographer” who redefines a claim term to

have an “uncommon meaning[]” or “uncommon definition” must do so with “reasonable clarity, deliberateness, and precision.” *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (citation omitted).

Recently, the Federal Circuit indicated that even for non-expired patents that return to the PTO, prosecution history may be an important component of intrinsic evidence in construing claims (notwithstanding that Patent Owner may amend the claims and a broadest reasonable construction standard applies).<sup>3</sup> See *Tempo Lighting, Inc. v. Tivoli, LLC*, 742 F.3d 973, 977 (Fed. Cir. 2014) (“In claim construction, this court gives primacy to the language of the claims, followed by the specification. Additionally, the prosecution history, while not literally within the patent document, serves as intrinsic evidence for purposes of claim construction. This remains true in construing patent claims before the PTO.”) (citing *In re Morris*, 127 F.3d 1048, 1056 (Fed. Cir. 1997)); *Microsoft Corp. v. Proxyconn, Inc.*, No. 2014-1542, 2015 WL 3747257, at \*3 (Fed. Cir. June 16, 2015) (“The PTO should also consult the patent’s prosecution history in proceedings in which the patent has been brought back to the agency for a second review.”)

---

<sup>3</sup> For district court litigation and for expired patents that return to the PTO, claims cannot be amended. Those claims must be construed using their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art, at the time of the invention, in light of the language of the claims, the specification, and the prosecution history of record. See *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313–17 (Fed. Cir. 2005) (en banc); *In re Rambus*, 694 F.3d 42, 46 (Fed. Cir. 2012) (“[T]he Board’s review of the claims of an expired patent is similar to that of a district court’s review.”); *Cuozzo*, 2015 WL 4097949, at \*6 n.6 (“The claims of an expired patent are the one exception where the broadest reasonable interpretation is not used because the patentee is unable to amend the claims.”) (citing *In re Rambus, Inc.*, 753 F.3d 1253, 1256 (Fed. Cir. 2014)).

(citing *Tempo Lighting*, 742 F.3d at 977); *Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1349 (Fed. Cir. 2004) (“[T]he prosecution history of one patent is relevant to an understanding of the scope of a common term in a second patent stemming from the same parent application.”). On the other hand, in *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.”

Although disclaimers or lexicographic definitions in a specification may be express, they need not be. *Compare In re Bigio*, 381 F.3d 1320, 1325 (Fed. Cir. 2004) (“Absent claim language carrying a narrow meaning, the PTO should only limit the claim based on the specification or prosecution history *when those sources expressly disclaim* the broader definition.”) (emphasis added), *with Bell Atl. Network Servs., Inc. v. Covad Commc’ns Grp., Inc.*, 262 F.3d 1258, 1268 (Fed. Cir. 2001) (“[A] claim term may be clearly redefined without an explicit statement of redefinition. . . . In other words, the specification may define claim terms by implication such that the meaning may be found in or ascertained by a reading of the patent documents.”) (citations and internal quotation marks omitted), *and Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996) (“The specification acts as a dictionary when it expressly defines terms used in the claims or when it defines terms by implication.”).

In any case, prosecution history disclaimers, like uncommon or lexicographic meanings, must be clear and unambiguous: “[W]hile the prosecution history can inform whether the inventor limited the claim scope in the course of prosecution, it often produces ambiguities created by

ongoing negotiations between the inventor and the PTO. Therefore, the doctrine of prosecution disclaimer only applies to unambiguous disavowals.” *Grober v. Mako Prods., Inc.*, 686 F.3d 1335, 1341 (Fed. Cir. 2012) (citing *Abbott Labs. v. Sandoz, Inc.*, 566 F.3d 1282, 1289 (Fed. Cir. 2009)). A “heavy presumption” exists in favor of the ordinary meaning of claim language. *Bell Atl. Network Servs., Inc.*, 262 F.3d at 1268. To overcome this presumption, the patentee must “clearly set forth” and “clearly redefine” a claim term away from its ordinary meaning. *Id.* The disavowal must be “unmistakable” and “unambiguous.” *Dealertrack, Inc. v. Huber*, 674 F.3d 1315, 1322 (Fed. Cir. 2013). This standard is “exacting.” *Thorner v. Sony Computer Entm’t Am. LLC*, 669 F.3d 1362, 1366 (Fed. Cir. 2012).

#### *1. Virtual Private Network (VPN) Communication Link*

We previously construed the claim 1 term “virtual private network communication link” to mean “a transmission path between two devices that restricts access to data, addresses, or other information on the path, generally using obfuscation methods to hide information on the path, including, but not limited to, one or more of authentication, encryption, or address hopping.” Inst. Dec. 8–9.<sup>4</sup> Patent Owner “disagrees with this construction,” contending that the term “must incorporate the ‘direct communication’ and ‘network’ aspects of the VPN that are disclosed in the ’274 patent specification.” PO Resp. 5. However, Patent Owner does not contend that the last two requirements “materially affect[] the parties’ disputes.” *See* PO

---

<sup>4</sup> Our construction is consistent with the broadest, reasonable construction in *Inter Partes* Reexamination Control No. 95/001,792. *See Cisco Systems, Inc. v. VirnetX, Inc.*, Appeal 2014-000491, slip. op. at 4–8 (PTAB Apr. 1, 2014) (Decision on Appeal) (involving a grandparent patent to the ’274 patent, U.S. Patent No. 7,188,180).

Resp. 4. Patent Owner also clarified during the oral hearing that it does not contend that Provino fails to disclose “direct communication.” *See* Tr. 86:8–14.

Therefore, we maintain our construction of the term “virtual private network” or “virtual private network communication link” for purposes of this decision. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (stating that claim terms need only be construed to the extent necessary to resolve the case).

## 2. *Secure Domain Service (SDNS)*

Patent Owner proposes that a “secure domain service” (SDNS), as recited in claim 1, should be construed as “[a] lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer address for a requested secure domain name.” PO Resp. 15.<sup>5</sup> Petitioner proposes that an SDNS should be construed as “[a] service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service [(“DNS”)] cannot resolve addresses.” *See* Pet. 13; PO Resp. 15 (discussing Petitioner’s proposed construction). The distinction between the two proposals centers on what the function of “recognizes . . . requesting a secure domain name” requires.

To support its construction, Patent Owner argues, among other things, that “during the now-completed *inter partes* reexamination” (Reexam.

---

<sup>5</sup> Claim 1 recites a “secure domain service” and a “secure domain name service.” For purposes of this Final Written Decision and because it is not at issue, we do not distinguish the claim term “secure domain service” from a “secure domain name service,” and generally refer to each as an “SDNS.” *See* Pet. 12 (pointing out that claim 1 recites both terms).



Control No. 95/001,270) (“’270 reexamination”) of the grandparent patent to the ’274 patent, U.S. Patent No. 7,188,180 (the “’180 patent,”), “VirnetX . . . disclaimed secure domain services that do not perform this recognition,” and, further, the Eastern District of Texas “later relied on VirnetX’s statements.” PO Resp. 16–17 (citing Ex. 2040, 7 (Response to Office Action, Apr. 19, 2010, ’270 reexamination); Ex. 1018, 2, 17–18 (District Court Memorandum Opinion and Order)). During the ’270 reexamination proceeding, Patent Owner contended that an SDNS, as claimed and disclosed, cannot merely “resolve[] a domain name query that, unbeknownst to the secure domain name service, happens to be associated with a secure domain name.” See PO Resp. 16 (quoting Ex. 1040, 7).

Patent Owner does not contend explicitly that, or explain how, Petitioner’s proposed construction improperly embraces the allegedly disclaimed type of a conventional DNS that “happens” to resolve a domain name query “associated with secure domain name.” See *id.* at 15–17. It also is not clear how that allegedly disclaimed feature relates to the “recognizes” function in Patent Owner’s proposed claim construction.

Claim 1 recites sending a query message to “a secure domain service,” requesting a secure network address, and receiving “a response message from the secure domain name service containing the secure network address.” It does not recite “recogniz[ing] that the query message is requesting a secure computer address.” “[T]he claims themselves provide substantial guidance as to the meaning of particular claim terms” and “the context in which a term is used in the asserted claim can be highly instructive.” *Phillips*, 415 F.3d at 1314. “The construction that stays true to the claim language and most naturally aligns with the patent’s description of

the invention will be, in the end, the correct construction.” *Phillips*, 415 F.3d at 1316.

Based on the context of the claim, the Specification, and the prosecution history, claim 1 does not require “recogniz[ing]” as argued by Patent Owner. As explained in the Background section *supra*, the Specification describes an “SDNS 313” that “contains a cross-reference database of secure domain names and corresponding secure network addresses. That is, for each secure domain name, SDNS 3313 stores a computer network address corresponding to the secure domain name.” Ex. 1001, 47:15–18. This disclosure comes closest to aligning with the claim term, “secure domain service” (i.e., an SDNS as set forth in the disclosure). Patent Owner does not point the panel to a disclosure in the Specification that clearly supports the requirement of an SDNS to “recognize that the query message is requesting a secure computer address.”

Patent Owner also contends that during the ’270 reexamination, Patent Owner proposed various examples of possible “additional functionalities not available with a traditional domain name service.” PO Resp. 17. For example, Patent Owner maintains that it argued during the reexamination that a secure domain name service “may allow an entity to register server secure domain names representing different levels of access to the secure website” and “may also support the establishment of a VPN communication link.” *See* PO Resp. 17 (citing Ex. 1001, 47:38–51; Ex. 2040, 3, 7–8). According to Patent Owner, “[t]hus a secure domain service is distinguished from a conventional domain name service.” *Id.* at 17.

Contrary to Patent Owner’s arguments, even if the prosecution history of claims in the grandfather ’180 patent in the ’270 reexamination

proceeding somehow limits the claims here that Patent Owner otherwise could have moved to amend under a broadest reasonable construction, Patent Owner's arguments were not "unambiguous," and do not "call for the application of prosecution history disclaimer." *See* PO Resp. 17–18. There was no "express disclaimer," *Bigio*, 381 F.3d at 1325, or "unambiguous disavowal[]," *Grober*, 686 F.3d at 1341.

For example, as Petitioner points out, Patent Owner argued, among other things, as follows during the '270 reexamination of the '180 patent:

*To illustrate, the '180 patent explicitly states 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. See, '180 Patent at col. 51, ll. 18–45 (stating "[b]ecause the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown") . . . .*

Ex. 2040, 7 (emphasis added); *see* Pet. Reply 10 (discussing prosecution history); Pet. 10–13 (discussing prosecution history and district court litigation).

Responding to Patent Owner's various arguments during the '270 reexamination of the '180 patent, the examiner reasoned as follows:

Further, Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name" from a domain name that happens to correspond to a secure computer. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name." For example, *the '180 patent explains that a secure domain name is a non-standard domain name and that querying a convention domain name server using a secure domain name will result in a return message indicating that the URL is unknown ( '180 patent, column 51 lines 25–35). Similarly,*

Patent Owner argues that the '180 patent clearly distinguishes the claimed "secure domain name service" from a conventional domain name service that *can resolve domain names of computers that are used to establish secure connections*. Patent Owner's argument is persuasive. The Examiner agrees that the '180 patent distinguishes the claimed "secure domain name service." *For 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* ('180 patent, column 51 lines 25–35).

Ex. 3001, 3 ('270 reexamination of the '180 patent, Right of Appeal Notice (Dec. 30, 2010)) (emphases added, examiner's emphasis omitted).<sup>6</sup>

This exchange between the Patent Owner and the examiner reveals that the central reason for confirmation by the examiner in the '270 reexamination was Patent Owner's argument that the '180 patent makes clear that a conventional DNS *cannot resolve addresses for a secure domain name*, whereas the disclosed SDNS can. *Id.*

Petitioner contends that the declarants for Patent Owner and Petitioner essentially agree to this key distinction. *See* Pet. Reply 7–8 (citing Ex. 1090, 21:14–22:1, 23:16–26:15, 16:9–17:17; Ex. 1011 ¶ 15). Quoting the '274 patent, Dr. Roch Guerin, Petitioner's declarant, testifies that the '274 patent indicates that "SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses." Ex. 1001, 47:15–16. In other words, *the SDNS 3313 differs from a standard name service in that it is configured to resolve secure domain names.*" Ex. 1011 ¶ 15 (emphasis added). After summarizing other pertinent disclosures in the '274 patent Specification (*see* Ex. 1011 ¶¶ 11–23), Dr. Guerin testifies that

---

<sup>6</sup> Page number "3" in Ex. 3001 refers to the original page number supplied by the examiner in the Right of Appeal Notice.

“a broadest reasonable interpretation of ‘secure domain name service’ would be broad enough to cover ‘a service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service cannot resolve addresses.’” Ex. 1011 ¶ 24.

Dr. Fabian Monroe, Patent Owner’s declarant, testified during cross-examination that a “secure domain name service is referred to as a lookup service that recognizes that a query message is requesting a secure computer address and returns a secure computer address for the requested secure domain name.” Ex. 1090, 21:18–22. Arguing that Provino does not disclose an SDNS, Patent Owner relies on Dr. Monroe’s declaration testimony that the disclosed SDNS does more than provide a mere look-up function. *See* PO Resp. 30–32 (citing Ex. 2041 ¶¶ 35–39); *see also* Ex. 1090, 17:18–18:4 (Dr. Monroe’s deposition testimony: “For example, the ability to initiate a virtual private network communication, the ability to have multiple levels of access control, the ability to make decisions based on the -- on the originator, et cetera.”). Similar to this declaration and deposition testimony, Patent Owner lists different “additional functionalities not available with a traditional domain name service. For instance, a secure domain service may allow an entity to register server secure domain names representing different levels of access to the secure website.” *See* PO Resp. 17 (citing Ex. 2040, 3, 7; Ex. 1001, 47:15–37).

Even if these types of “example[s]” describe possible functions of a disclosed SDNS, they do not arise to an unequivocal disclaimer or show that the “recognizes” function must be incorporated into the claimed SDNS. Dr. Monroe and Patent Owner do not offer a clear interpretation of what the “recognizes” function entails and do not point to where that term appears in

the '274 patent Specification. Describing “some examples” of what some of the disclosed “SDNS[] . . . embodiments . . . can perform” fails to link those examples with the proffered “recognizes” function. *See* Ex. 1090, 21:18–22:5. In other words, Dr. Guerin’s testimony and Petitioner’s claim construction tracks more closely to direct support in the '274 patent Specification.

During the oral hearing in this proceeding, when questioned about the specific added functionality the claims may require by disclaimer or otherwise, Patent Owner indicated that the claims do not require a specific functionality: “Because in some instances it could be example A and in some instances it could be example B. But as long as it is recognizing that a query message is requesting a secure . . . computer address . . . it can’t be just a conventional DNS operation. It has to be more than that.” Tr. 67:24–68:4.

Therefore, the clearest thread running through the arguments, prosecution history, evidence, the '274 patent Specification, and the claim language, is that “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* ('180 patent, column 51 lines 25–35).” Ex. 3001, 3 (emphasis added). Simply put, a conventional DNS does not resolve a *secure* address for a *secure* domain name, hence the name, *secure* domain server, and nomenclature, SDNS. *Cf. In re Abbott Diabetes Care Inc.*, 696 F.3d 1142, 1149–50 (Fed. Cir. 2004) (disavowal must “repeatedly, consistently, and exclusively” show the same feature).

In a similar vein, according to Patent Owner, “each of the disclosed embodiments performs more than the conventional DNS functions and supports establishing a secure communication link.” PO Resp. 30–31. Describing what some embodiments may do fails to explain why Petitioner’s construction, “resolv[ing] secure computer network addresses for a secure domain name” does not also “support[] establishing a secure communication link.” The arguments and evidence show that a “secure domain service” (SDNS) requires no functionality beyond Petitioner’s proposed construction.<sup>7</sup>

Further alleging a Specification disclaimer, Patent Owner quotes the ’274 patent as noting that “[t]he *conventional scheme* suffers from certain drawbacks,” and points to “certain aspects of the invention” as setting up a VPN. *See* PO Resp. 30 (quoting Ex. 1001, 39:4–41 (emphasis by Patent Owner), citing Ex. 2041 ¶ 35). In that conventional scheme, the ’274 patent discloses that “[o]ne *conventional scheme* . . . provides the DNS server with public keys of the machines that the DNS server has addresses for.” Ex.

---

<sup>7</sup> Patent Owner also argues that “the Board has rejected arguments that “a ‘secure domain name service’ is a service that can resolve secure computer network addresses that a conventional domain name server cannot resolve.” PO Resp. 35 (citing *Apple Inc. v. VirnetX Inc.*, Case IPR2014-00482, slip. op. at 9 (PTAB Sept. 3, 2014) (Paper 10); *Apple Inc. v. VirnetX Inc.*, Case IPR2014-00481, slip. op. at 9 (PTAB Sept. 3, 2014) (Paper 11)). This argument mischaracterizes and overstates the import of those prior decisions to institute. In both proceedings, we determined that “for purposes of this Decision, a ‘secure domain name service’ is a service that provides a secure computer network address for a requested secure domain name”—if anything, a slightly broader construction than the petitioner’s proposed construction there and Petitioner’s similar construction proposed here. *See, e.g., Apple*, Case IPR2014-00481, Paper 11 at 9. Also, those decisions involved preliminary findings and claim constructions. *See id.*

1001, 39:13–17 (emphasis added). The '274 patent describes “drawbacks” pertaining to that “conventional *scheme*” (i.e., not the DNS itself and not an SDNS): “For example, any user can perform a DNS request. . . . [and] DNS requests resolve to the same value for all users.” Ex. 1001, 39:23–25 (emphasis added). Although it is not clear, this disparaged “scheme” may be the basis upon which Patent Owner relies for its disclaimer argument that an SDNS cannot merely “resolve[] a domain name query” that “happens to be associated with a secure domain name” “unbeknownst to the domain name service.” See PO Resp. 16 (quoting Ex. 2040, 7, but not linking directly the disclosed conventional public key scheme to the prosecution argument). Nevertheless, Patent Owner fails to explain how Petitioner’s construction embraces this disparaged public key scheme. Petitioner proposes that an SDNS “can resolve secure computer network addresses for a *secure domain name*.” *Id.* at 34 (emphasis added). On its face, a “secure domain name” does not “happen” to be “associated with a secure name”; rather, a secure domain name *is* a secure name.

Moreover, the '274 patent describes overcoming the problems associated with the public key “scheme” by doing much more than adding Patent Owner’s proposed “recognizing” functionality to the SDNS as construed by Petitioner: “According to *certain aspects* of the invention, a *specialized* DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communications are defined), *the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user*. The VPN is preferably implemented using the IP address ‘hopping features.’” Ex. 1001, 39:24–34 (emphases added). The claims do not recite



a “specialized DNS,” but even if the claimed SDNS somehow relates to this disclosed “specialized DNS,” Patent Owner does not urge that its proposed SDNS must return a false IP address, automatically set up a VPN, or use hopping features—which the Specification discloses as solving problems associated with the allegedly disparaged conventional DNS/public key scheme.

Patent Owner also does not explain how its proposed “recognizes” functionality would overcome the conventional scheme’s problem of allowing “any user [to] perform a DNS request,” or prevent its proposed SDNS from “resolv[ing] the same value for all users.” *See* Ex. 1001, 39:23–25. There is no dispute on this record that a “secure network address is an address that requires authorization for access.” Ex. 1090, 21:10–13; PO Resp. 24 (agreeing with claim construction of “secure network address” in Institution Decision, *see* Inst. Dec. 9). Assuming that “any user” even has access to a secure domain name, a secure network address that requires authorization naturally prevents “any user” from obtaining it via a resolved secure domain name, thereby overcoming the prior art problems in the DNS conventional scheme, and suggesting that any “recognizes” functionality as a proposed SDNS requirement is superfluous or not required.

Overcoming that prior art scheme’s problems with a list of disclosed features that are not required under Patent Owner’s claim construction fails to support that construction. Criticizing a prior art *scheme* in the disclosure or in arguments does not criticize an SDNS itself. As a specific example, urging construction of a client computer as a user’s computer, Patent Owner refers to a “conventional” “user’s” computer as “another embodiment,” even though the ’274 patent Specification disparages the “conventional

architecture” that employs such a user’s computer (because it is not secure enough). *See* Ex. 1001, 39:4–13; PO Resp. 21. Further, as Petitioner argues, even if a DNS/public key scheme embodiment falls into Petitioner’s construction, “[m]ere criticism of a particular embodiment encompassed in the plain meaning of a claim term is not sufficient to rise to the level of clear disavowal.” Pet. 7 (quoting *Thorner v. Sony Computer Entm’t Am. LLC*, 669 F.3d 1362, 1366 (Fed. Cir. 2012)).

Finally, Patent Owner made the opposite argument to the District Court that it is making here, and argued that the “non-standard” distinction, which underlies the “recognizing” interpretation according to Patent Owner’s arguments here, “is not supported by the specification or the prosecution history.” Ex. 1018, 18 (discussing Patent Owner’s ’180 patent prosecution history arguments in the ’270 reexamination). In other words, *despite* Patent Owner’s arguments to the contrary in the District Court, the District Court found against Patent Owner, and reasoned that Patent Owner had “explained 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.’” *Id.* (quoting argument by Patent Owner). Therefore, the District Court stated that “[a]ccordingly, the non-standard characterization proposed by *Defendants* should be retained.” *Id.* (emphasis added).

The District Court then construed a “secure domain name service” as a “non-standard lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name.” *Id.* at 19. Nevertheless, in arguments and reasons presented on this record and in the District Court,

Patent Owner unequivocally “explained 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.’” *See id.* at 18 (quoting argument by Patent Owner).

Accordingly, and with a record that is distinct from that in the reexamination and the District Court, we adopt Petitioner’s proposed construction, which tracks Patent Owner’s repeated argument and the ’274 patent Specification that all show that an SDNS is “[a] service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service [(“DNS”)] cannot resolve addresses.”

Moreover, unlike in the District Court, Patent Owner here had the opportunity to propose claim amendments that included the “recognizes” functionality urged, but chose not to do so. In addition, Patent Owner did not amend claims to address and clarify an SDNS during the original prosecution history for the ’274 patent, or during the prosecution history of the ’180 patent. These factors weigh against finding prosecution history disclaimer, especially where any disclaimer is equivocal at best. *See Tempo Lighting*, 742 F.3d at 978 (“This 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. However, in this instance, the PTO itself requested Tivoli rewrite the ‘non-photoluminescent’ limitation in positive terms. Tivoli complied, and then supplied clarification about the meaning of the ‘inert to light’ limitation.”).<sup>8</sup>

---

<sup>8</sup> In *Tempo Lighting*, the original prosecution creating the disclaimer that the PTO was “under no obligation to accept” was closed, and the Board

Based on the foregoing discussion and the record, we adopt Petitioner’s proposed construction and do not adopt Patent Owner’s proposed construction of the term “secure domain service.”

### *3. Tunnel Packeting*

Patent Owner argues that one of ordinary skill in the art would have understood the term “tunnel packeting” to mean “forming a packet to be transmitted that contains data structured in one protocol format within the format of another protocol.” PO Resp. 18. As Patent Owner notes, we initially proposed that it means “placing data or information in one protocol format (or packet portion), into another protocol format (or portion) of a packet.” Inst. Dec. 10–11; PO Resp. 18. Petitioner agrees with our construction and argues that Patent Owner’s construction is not consistent with the plain language of the term. *See* Pet. Reply 5 (citing Ex. 1011 ¶ 38).

Citing arguments and citations in the Preliminary Response, we determined that “[i]n context, according to Patent Owner’s apparent position, a first protocol format includes a part of a packet or frame, such as a header (e.g., an address), and a second protocol format includes another part of a packet or frame, such as the payload (e.g., the data).” Inst. Dec. 11 (citing Prelim. Resp. 29 & n. 8). Patent Owner does not dispute this contextual observation, which correlates one protocol format with, for example, the “header portion” (which includes an address portion) of a packet, and a different protocol format with the “payload portion” (data

---

employed that original record as part of the intrinsic record to shed light on the meaning of the claim during an appeal of a subsequent reexamination. 742 F.3d at 978–79.

portion) of a packet. *See* Prelim. Resp. 29 & n.8 (citing Ex. 2026, 4).<sup>9</sup> In originally setting forth its claim construction, Patent Owner stated that “[p]ackets generally contain a header portion and a payload portion.” Prelim. Resp. 29 n.8. Patent Owner’s explanation observes that a payload has “some structure. . . . that holds the message data in contrast to the headers, which are considered overhead.” *Id.* In other words, we gleaned from Patent Owner’s explanation an implication that headers and payloads have different structures, or protocol formats.

Although Patent Owner now contends that our construction “may operate to read out the concept of protocol formats altogether,” Patent Owner fails to explain why a header and payload have different protocol formats. *See* PO Resp. 18–19. Addressing claims 12 and 13, Patent Owner contends, without explanation, that “[s]imply placing the integer Internet address inside the data portion of a packet does not necessitate a change in protocol format from ‘one protocol’ to ‘another protocol.’” PO Resp. 41 (citing Ex. 2041 ¶ 47). Dr. Monroe’s testimony is similarly conclusory, because it does not explain why putting address information inside a payload, as occurs in the ’274 patent Specification (as explained below), does not constitute a change in protocol format. *See* Ex. 2041 ¶¶ 25, 26, 47.

Patent Owner also contends that

[o]bstensibly, the Board adopted its construction to take into account “encapsulating one packet portion or an entire packet inside of another packet.” (Decision at 11.) *VirnetX’s construction, however, allows for either of these possibilities.*

---

<sup>9</sup> Exhibit 2026 includes a trade dictionary definition that defines tunneling as “data structured in one format within the format of another protocol.” Ex. 2026, 7. Patent Owner does not allege that our construction is inconsistent with this definition.

(Ex. 2041 at ¶ 26, Monroe Decl.) Specifically, “forming a packet to be transmitted that contains data structured in one protocol format” embraces a packet that contains either a portion of a packet or an entire packet. (Ex. 2041 at ¶ 26, Monroe Decl.)  
PO Resp. 19 (emphasis added).

In other words, Patent Owner also ambiguously contends that its construction embraces our construction, but that our construction “may operate to read out the concept of protocol formats.” *Id.* Dr. Monroe’s testimony does not clarify Patent Owner’s position, but parrots the language in the Patent Owner Response. *See* Ex. 2041 ¶¶ 25, 26, 47.

The ’274 patent Specification describes “tunnel[ing] the unencrypted, unprotected communication packets through a new protocol, thereby protecting the communications from a denial of service.” Ex. 1001, 49:31–33. It also describes “modify[ing] the payload portion of all message packets by tunneling the data for forming a virtual private connection . . . into the payload portion.” *Id.* at 50:46–49. “Preferably, the data for forming the virtual private connection data contains field hopping data . . . .” *Id.* at 50:29–31.

As the latter two sentences show, the ’274 patent Specification describes placing field hopping data (i.e., an address hopping technique, *see id.* at 46:64–47:11), into a payload portion of a data packet. The Specification does not tie “tunneled” packets into a specific requirement that requires a change in formatting—above and apart from any protocol formatting or structural change that may happen to, or does, occur by placing one type of data field (header) into another type of data field (payload). After discussing the insertion of the field hopping data into the payload portion, the Specification then describes that these “modified

message packets preferably conform to the UDP protocol,” or “[a]lternatively . . . can conform to the TCP/IP protocol or the ICPM protocol.” *Id.* at 50:30–35. In other words, if there is a change in a protocol in these disclosed examples—for example, from one protocol format to a UDP protocol format—any change appears to come in *preferred* embodiments and after the packets have been modified (i.e., tunneled).

Accordingly, based on the foregoing discussion, we modify our construction as set forth in the Institution Decision, such that “tunnel packeting” means “placing data or information from one field, such as a header, into another packet field, such as a payload, wherein the two fields normally have different structures or formats, or placing data structured in one format within the format of another protocol.”

#### *4. Client Computer*

Patent Owner contends that this term is “material to claim 15.” PO Resp. 20. Patent Owner also contends that “the broadest reasonable interpretation of ‘client computer’ is a ‘user’s computer.’” PO Resp. 20. Patent Owner does not contend that Provino fails to disclose a user’s computer, or a client computer as set forth in claim 15.

Therefore, this term does not appear to be material in this proceeding. In any event, to the extent it is material, the ’274 patent Specification employs the term “user’s computer” in a “conventional scheme . . . shown in FIG 25. A user’s computer 2501 includes a client application 2504 (for example a web browser) . . . .” Ex. 1001, 38:61–63. Although Patent Owner refers to this “conventional” computer as “another embodiment,” the ’274 patent Specification disparages the “conventional architecture” that employs a user’s computer, because it is not secure enough. *See* Ex. 1001,

39:4–13; PO Resp. 21. In general, the '274 patent Specification states that “[t]he present invention” involves a “client computer” with a “client application” that “communicates with a server.” *See* Ex. 1001, 7:40–44. This description of “[t]he present invention” does not mention a “user’s computer.”

Therefore, the '274 patent Specification does not repeatedly treat a “client computer” and a “user’s computer” as the same. The broadest reasonable construction of a client computer is a computer associated with a client.

#### *5. Access Request Message*

As Patent Owner explains, the construction of this term “do[es] not appear to be relevant to the parties’ disputes.” PO Resp. 24.

#### *6. Secure Network Address*

As Patent Owner explains, the construction of this term “do[es] not appear to be relevant to the parties’ disputes.” PO Resp. 24.

### III. ANALYSIS

#### *A. Provino*

For at least the reasons discussed below, we find that Petitioner has demonstrated that Provino anticipates claims 1, 7, 8, 10, 12, 15, and 17 under 35 U.S.C. § 102.

#### *1) DNS Server*

Claim 1 recites a “secure domain service,” referred to herein as SDNS. *See supra* note 5. Patent Owner argues that Provino’s VPN Name Server 32 is not an SDNS because “nameserver 32 behaves just like nameserver 17, which Petitioner concedes is a conventional DNS.” PO Resp. 35.



Patent Owner's argument is not persuasive. Patent Owner does not dispute that Provino's SDNS resolves secure domain names into secure network addresses, thereby satisfying the claim construction of a secure domain service, as discussed above and further below. *See* Pet. Reply 8. Further, Provino's VPN nameserver 32 resides behind a firewall, which controls access to secure devices 31(s), indicating it is secure for that additional reason.<sup>10</sup> Ex. 1003, Fig. 1, 9:6–17. The fact that nameservers 17 and 32 perform similar functions simply demonstrates that they are both nameservers.

In addition, Provino's SDNS 32 "is generally similar to . . . nameserver [17], *except* that the integer Internet address will be provided by the nameserver 32 in a message packet directed to the firewall 30, and the firewall 30 will thereafter transmit the message packet over the secure tunnel to the device 12(m)." Ex. 1003, 11:20–25. In other words, even under Patent Owner's narrow claim construction that requires an SDNS to perform an additional function (i.e., in addition to resolving a secure domain name (*see* PO Resp. 16–18)), unlike conventional nameserver 17, secure nameserver 32 directs a message packet to firewall 30, and thereby performs

---

<sup>10</sup> *See VirnetX, Inc. v. Cisco Systems, Inc.*, 767 F.3d 1308, 1317–19 (Fed. Cir. 2014) ("VirnetX provided substantial evidence for the jury to conclude that paths beyond the VPN server may be rendered secure and anonymous by means of 'physical security' present in the private corporate networks connected to by VPN On Demand."). Underlying that finding, the *Cisco* court noted that "VirnetX's expert testified that one of ordinary skill would understand that the path . . . within the private network[] would be secure and anonymous owing to the protection provided by the private network." *Id.* at 1321.

that additional function (i.e., implicitly “recognizing” that the request is for a secure address).

Discussing Provino’s nameserver 32 and relying on Dr. Monroe, Patent Owner argues that “when nameserver 32 receives a human-readable address, it simply checks ‘whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet,’ and, if so, ‘generate[s] a response message packet including the integer Internet address for transmission to the firewall.’” PO Resp. 35–36 (quoting Ex. 1003, 14:39-46; citing Ex. 2041 ¶ 40).

Patent Owner contends that this and other similar operations show that nameserver 17 and secure nameserver 32 behave the same, rendering secure name server 32 a conventional DNS that a proper claim construction does not embrace. *See* PO Resp. 35–36. Setting aside the additional functionality that Provino’s name server 32 provides as discussed above (sending packets to a firewall), Patent Owner’s arguments turn on an overly narrow claim construction, which this Final Written Decision does not adopt. Patent Owner’s response does not dispute that Provino’s secure nameserver 32 operates differently from nameserver 17 in a more critical fashion, as Petitioner argues: “Provino distinguishes nameserver 32 from public nameserver 17, which *cannot* resolve queries for *secure* network addresses because they do not have network addresses for *secure* devices behind firewall 30 of VPN 15.” Pet. Reply 8 (comparing the disclosed invention to Provino’s similar nameservers, citing Ex 1003, 10:45–55, 11:11–14, Ex. 1011 ¶ 14; Ex. 1001, 46:41–44). Despite Patent Owner’s arguments (*see* PO Resp. 31–32), as discussed *supra* in the Claim Construction section (Section I.E), Patent Owner has not disparaged or

disavowed, unequivocally, a “secure domain service,” as set forth in the claims, which resolves a secure domain name. *See* Pet. Reply 8–9.

As Dr. Guerin testifies, Provino’s secure nameserver 32 provides an Internet address for secure server 31(s) that nameserver 17 cannot provide. *See* Ex. 1011 ¶¶ 35–36; Ex. 1003, 11:5–25; 15:21–30. As Petitioner contends, there is no reasonable dispute, if any, on this record about that key difference, which the claim construction of “secure domain service” captures. *See* Pet. Reply 7–8 (citing Ex. 1090, 38:5–40:18; Ex. 1003, 9:56–60, 13:63–14:24); PO Resp. 35. For example, as Provino explains, “[s]ince nameserver 17 is outside of the virtual private network 15 and will not have the information requested by the device 12(m)”—i.e., the integer Internet address associated with secure server 31(s)—“it will send a response so indicating.” Ex. 1003, 11:10–13.

Based on the foregoing discussion and the record, Petitioner shows by a preponderance of evidence, and we find, that Provino discloses a “secure name service” as recited in claim 1.

## *2) Access Request Message*

Patent Owner argues that Provino does not disclose “sending an access request message from the first network device to the secure network address using a virtual private network communication link,” as claim 1 recites, because

Provino does not disclose what the message packets sent from device 12(m) to server 31(s) do, let alone whether the message packets sent to server 31(s) include a signal that “signifies that the [device 12(m)] seeks communication, information, or services, with a [server 31(s)],” as required by the Decision’s construction of “access request message.”  
PO Resp. 37 (discussing Inst. Dec. 8).

Patent Owner argues that the Institution Decision relies on “inherency,” and implies that Provino does not disclose that the message packets “necessarily” request access to servers 31(s). *Id.*

Petitioner responds by noting that it relies on what Provino describes, implicitly or otherwise, to ordinarily skilled artisans. *See* Pet. Reply 11. In general, after obtaining the secure network address for server 31(s) and decrypting it, Provino’s network device 12(m) uses it to communicate with server 31(s) by sending message packets thereto. *See* Ex. 1003, 15:27–30. Petitioner points out that Patent Owner’s declarant agreed during his deposition that “requesting access to whatever information is stored on server 31S . . . could be one reason to connect to 31S.” Pet. Reply. 11 (citing Ex. 1090, 42:12–43:10).

Petitioner also relies on Dr. Guerin, who testifies as follows:

Once the device 12(m) obtains the integer Internet address of server 31(s) from nameserver 32 during the second phase of establishing communications with server 31(s), the device 12(m) may send access requests to server 31(s) using the secure tunnel established with the firewall 30 in the first phase of the communication process. *See* Ex. 1003, 15:21–30. In particular, Provino describes that the server 31(s) may be a “storage server” that provides information that is requested by a client. *See* Ex. 1003, 6:19–50. As a consequence, the requests sent to server 31(s) by device 12(m) may be requests for information stored at the server 31(s). By describing that device 12(m) generates a message packet for transmission to server 31(s) and receives information transferred from server 31(s), Provino describes that device 12(m) leverages the resolved secure computer network address (i.e., integer Internet address) to send access request messages to server 31(s) that contain requests for access to information stored on server 31(s).

Ex. 1011 ¶ 40; *see* Pet. 11–12 (discussing *id.*, citing Ex. 1090 at 42:12–43:10; Ex. 1003, 6:19–28).

Provino corroborates Dr. Guerin. Generally, Provino’s ultimate goal is to “provide[] a system for easing communications” between devices in a secure tunnel through a firewall that defines or corresponds to a VPN. Ex. 1003, 15:59–60. The communicating devices include servers, personal computers, workstations, and other similar devices that operate in a “client-server” relationship, where requesting client device 12(m), for example, can “initiate service,” and server 31(s), or a similar device, can “perform processing operations at the request of the client,” or “provide information to the client.” *Id.* at 6:31–50.

As Dr. Guerin describes, Provino describes one embodiment wherein server 31(s) is a storage server, which provides information requested by first network device 12(m) in a client-server relationship. *See* Ex. 1003, 6:19–50; Ex. 1011 ¶¶ 39–40. “If the server is to provide information to the device, it (that is, the server) may generally be referred to as a storage server.” Ex. 1003, 6:43–45. The devices “communicate by transferring messages over the Internet.” *Id.* at 6:30–31. The message itself identifies “the intended recipient of the message packet” which may be “another device, such as server 31(s).” *Id.* at 10:31–33.

Provino also describes that the “integer Internet address for the server 31(s) can be cached in the *access* control list (“ACL”) in the IP parameter store 25 [of access requesting device 12(m)], along with the association of the human-readable Internet address thereto, an indication that the server 31(s) is *to be accessed* through the firewall 30 of the virtual private network 15.” Ex. 1003, 11:35–41 (emphases added). In other words, in addition to

the above-described showing, Provino also describes that “the server 31(s) is *to be accessed, id.*, using a “message packet” or “message packets.” *See id.* at 11:13–45.

Based on the foregoing discussion and the record, Petitioner shows by a preponderance of evidence, and we find, that Provino discloses a “request message packet” and the other elements recited in claim 1.

### 3) Claims 12 and 13

In addition to its arguments advanced with respect to claim 1, Patent Owner contends that “[t]hough *Provino* uses the term ‘secure tunnel’,” *Provino* does not disclose “using tunneling over the virtual private network communication link,” as claim 12 recites, and does not disclose “using tunnel packeting over the virtual private network communication link,” as claim 13 recites. PO Resp. 41 (citing Ex. 1003, 5:45–48; Ex. 2041 ¶ 45).

Patent Owner does not set forth a distinct argument regarding claim 12, but, rather, relies on arguments for claim 13. *See* PO Resp. 41–42; Pet. Reply 12. As Patent Owner acknowledges, and as the record shows, *Provino* employs a secure tunneling system. Ex. 1003, 5:45–48; 10:13–22, 11:26–29. Accordingly, based on the foregoing discussion and the record, Petitioner shows by a preponderance of evidence, and we find, that *Provino* anticipates claim 12.

Regarding claim 13, Patent Owner contends that “[s]imply placing the integer Internet address inside the data portion of a packet does not necessitate a change in protocol format from ‘one protocol’ to ‘another protocol.’” PO Resp. 42 (citing Ex. 2041 ¶ 47). Although Dr. Monrose repeats this sentence in the declaration testimony at the cited paragraph, Dr. Monrose and Patent Owner’s explanation does not overcome the finding and

claim construction flowing from the '274 patent Specification and Patent Owner's contextual remarks in its Preliminary Response, that putting address data into a data field portion of a packet, in a manner consistent with embodiments disclosed the '274 patent Specification, constitutes tunnel packeting. *See supra* Section I.E.3; Pet. Reply 12–13; Prelim. Resp. 29 & n.8; Ex. 1003, 11:26–29 (“[T]he . . . address in the message packet will be in the data portion of the message packet transferred over the secure tunnel.”) As set forth above in the Claim Construction section (Section I.E.), the '274 patent Specification discloses a similar “tunnel packeting,” and the term as construed embraces Provino's tunneling system and embodiments in the '274 patent Specification. Accordingly, based on the foregoing discussion and the record, Petitioner shows by a preponderance of evidence, and we find, that Provino anticipates claim 13.

#### 4) Claim 17

In addition to arguments advanced for claim 1, Patent Owner argues that Provino does not anticipate dependent claim 17, because Provino fails to disclose that “the secure network address is registered with the secure domain service prior to the step of sending a query message to a secure domain service,” as recited in claim 17. PO Resp. 43 (citing Ex. 2041 ¶¶ 48, 49). Patent Owner contends that “nameserver 32 could request that a network address of server 31(s) be registered after receiving a request for the network address from device 12(m).” *Id.* at 44 (citing Ex. 2041 ¶ 48).

As Petitioner contends, Provino shows implicitly, if not explicitly, that registration occurs in advance of any access request or query for access. For example, Provino discloses that “[i]f the nameserver 32 *has* an integer Internet address *associated* with the human-readable Internet address in the

request message packet provided by the device 12(m), it will provide the integer Internet address.” Pet. Reply 13 (quoting Ex. 1003,11:16–19 (emphasis by Petitioner); citing *id.* at 8:67–9:5, 11:46–53, 14:39–46; Ex 1011 ¶¶ 22, 32–36). As Petitioner also observes, Patent Owner did not challenge Dr. Guerin’s testimony that describes Provino’s operation, wherein nameserver 32 conventionally responds to queries using previously established associations. Pet. 13 (citing Ex. 1011 ¶ 33 (“One of ordinary skill in the art would understand that, by determining whether it has an integer Internet address, the nameserver 32 determines whether the human-readable Internet address has been registered, because this process leverages the registration of an association between a human-readable Internet address and an integer Internet address would have to be recorded at the nameserver 32.”)).

On the other hand, Dr. Monroe simply states, without cited support, that “[t]he Decision has not demonstrated that the nameserver 32 would operate in the manner it describes. For example, nameserver 32 could request that a network address of server 31(s) be registered after receiving a request for the network address from device 12(m).” Ex. 2041 ¶ 48. This testimony contradicts Dr. Monroe’s other testimony that “nameserver 32 operates in precisely the same way as the conventional domain name service” and “*simply checks* ‘whether it has an integer Internet address associated with the human-readable Internet address provided in the request message packet.’” Ex. 2041 ¶ 38 (quoting Ex. 1003, 14:39–46) (emphasis added). Simply checking is not dynamically creating.

In other words, Patent Owner’s argument *supra* in connection with claim 1, and Dr. Monroe’s declaration testimony, that nameserver 32



operates in a conventional manner, undermines Patent Owner’s hypothetical theory here in connection with claim 17 that server 31(s) “could” dynamically create the required address association in response to queries. The evidence shows that skilled artisans would have recognized that Provino’s nameserver 32 conventionally stores its associations ahead of a query for those associations instead of dynamically creating them during a query. *See In re Paulsen*, 30 F.3d at 1480 (“This argument, however, fails to recognize that a prior art reference must be ‘considered together with the knowledge of one of ordinary skill in the pertinent art.’” (quoting *In re Samour*, 571 F.2d 559 , 562 (CCPA 1978))).

Based on the record and for the reasons discussed above, Petitioner shows by a preponderance of evidence, and we find, that Provino anticipates claim 17.

*B. Obviousness, Claims 2–5*

Claims 2–5 depend from claim 1. Claim 2 further requires “supporting a plurality of services over the virtual private network communication link.” Claim 3 depends from claim 2 and further requires that “the plurality of services comprises a plurality of communication protocols, a plurality of application programs, multiple sessions, or any combination thereof.” Claim 4 depends from claim 3 and further requires that “the plurality of application programs comprises video conferencing, e-mail, a word processing program, telephony or any combination thereof.” Claim 5 depends from claim 2 and further requires that “the plurality of services comprises audio, video, or any combination thereof.”

In addition to its arguments with respect to claim 1, Patent Owner argues that Kosiur’s “aspirational disclosures” are insufficient to establish

obviousness of claims 2–5, because they “provide no details” and do not enable use of VPNs for “videoconferencing.” PO Resp. 45–46. As an initial matter, this argument is not commensurate in scope with claims 2, 3, and 5, because these claims do not require videoconferencing. Also, with respect to challenged claims 2–5 generally, “[t]his argument . . . fails to recognize that a prior art reference must be ‘considered together with the knowledge of one of ordinary skill in the pertinent art.’” *See Paulsen*, 30 F.3d at 1480 (quoting *Samour*, 571 F.2d at 562).

As noted, claim 4 recites videoconferencing. Addressing videoconferencing, Petitioner argues that Patent Owner’s “conclusory” allegation about a lack of enablement does not show “*why* the Kosiur scheme could not be adapted to work with Provino’s scheme in view of the abilities of a person of ordinary skill.” Pet. Reply 14. “Under § 103, . . . a reference ***need not be enabled***; it qualifies as a prior art, regardless, for whatever is disclosed therein.” *Id.* (quoting *Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1357 (Fed. Cir. 2003); citing *Geo M. Martin Co. v. Alliance Machine Sys. Int’l LLC*, 618 F.3d 1294, 1302–03 (Fed. Cir. 2010)).

Other cases support Petitioner’s point about individual enabling references and obviousness:

In order to render a claimed apparatus or method obvious, the cited prior art as a whole must enable one skilled in the art to make and use the apparatus or method. *Beckman Instruments, Inc. v. LKB Produkter AB*, 892 F.2d 1547, 1551 (Fed. Cir. 1989). An individual reference, on the other hand, “need not be enabled; it qualifies as a prior art, regardless, for whatever is disclosed therein.” *Amgen, Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1357 (Fed.Cir.2003); *see also*

*Symbol Techs., Inc. v. Opticon, Inc.*, 935 F.2d 1569, 1578 (Fed.Cir.1991); *Beckman Instruments*, 892 F.2d at 1551.  
*Therasense, Inc.v. Beckton, Dickinson and Co.*, 593 F.3d 1289, 1297 (Fed. Cir. 2010); *see also Symbol Techs. Inc. v. Opticon Inc.*, 935 F.2d 1569, 1578 (Fed. Cir. 1991) (“[A] non-enabling reference may qualify as prior art for the purpose of determining obviousness under § 103.”).

Even if enablement of each reference would be relevant to an obviousness analysis (which relies, *inter alia*, on what the references fairly teach to an ordinary artisan), Patent Owner’s unpersuasive arguments do not overcome the presumption that each reference is enabled.<sup>11</sup> As an initial matter, the references and Dr. Guerin’s testimony show, and the parties agree, that the skill level involved here is moderately high. *See* PO Resp. 11–12 (noting agreement); Ex. 1011 ¶ 7 (listing Master’s degree in computer science, computer engineering, and electrical engineering, and about two years of experience in computer networking and some aspects of security).

---

<sup>11</sup> *See In re Antor Media*, 689 F.3d 1282, 1287 (Fed. Cir. 2013) (stating that patents and non-patents are presumptively enabling during prosecution, and noting that in a prior case discussing patents, “[w]e . . . indicated that that presumption applies in the district court as well as the PTO, placing the burden on the patentee to show that unclaimed disclosures in a prior art patent are not enabling”) (citing *Amgen.*, 314 F.3d at 1354-55 & n.22 (Fed.Cir.2003)). In other words, even if enablement of individual references is relevant, a patentee must first come forward with some evidence of non-enablement: “Like the applicant in *ex parte* prosecution, however, the patentee may argue that the relevant claimed or unclaimed disclosures of a prior art patent are not enabled and therefore are not pertinent prior art. If a patentee presents evidence of nonenablement that a trial court finds persuasive, the trial court must then exclude that particular prior art patent in any anticipation inquiry, for then the presumption has been overcome.” *Amgen*, 314 F.3d at 1355.

Petitioner cites record evidence that shows that ordinarily skilled artisans would have recognized that Provino's scheme could have been used to transmit videoconferencing. Pet. Reply 14–15 (citing Ex. 1011 ¶ 42; Ex. 1006, 9, 249, 254; Ex. 1003, 4:35–49, 5:28–35). For example, Petitioner points out that “[a]lthough Provino does not specifically address these [videoconferencing and other claimed applications], it does describe device 12(m) as a system unit having the requisite capabilities, including a video display ‘to display processed data,’ and explains that message packets received ‘contain information such as web pages or the like, . . . to be displayed on the device’s video display unit.’” *Id.* at 15 (quoting Ex. 1003, 4:35–49, 5:28–35).

This record indicates that videoconferencing simply constitutes similar packet data traffic to the traffic that Provino's system implements. Petitioner also points out that “even Patent Owner's expert admitted that ‘[Provino is] generally saying that you can send data, and one such type of data is video;’ and could not identify any reason why sending video data on the Provino system would present insoluble problems.” *Id.* (citing Ex. 1090, 46:12–13, 48:2–7). Dr. Monroe's deposition testimony supports Petitioner's characterization of it. For example, Dr. Monroe states that “he didn't opine on whether or not there's anything in Provino that would explicitly not allow the sending of video data. This is not in my declaration, as far as I recall.” Ex. 1090, 48:2–7. Dr. Monroe also did not “reflect on . . . whether [data packets that represent video] will be processed differently or not, and how that could impact the operations of Provino.” *See id.* at 46:17–47:3 (responding to a question during cross-examination).

Petitioner further points out that Kosiur provides a “background on VPN technologies and products,’ Ex. 1006 at 9, and explain[s] that VPNs can support ‘newer applications, such as interactive multimedia and videoconferencing,’ *id.* at 254, as well as ‘file transfers, Web browsing, and e-mail,’ *id.* at 249.” Pet. Reply 14 (quoting Ex. 1006, citing Ex. 1011 ¶ 42). The record suggests that an ordinarily skilled artisan would have recognized that Provino’s system, which sends packets of data over a VPN, including webpages for viewing on a display, could have been modified in a beneficial and predictable fashion, as Kosiur suggests, to send similar packet data to provide videoconferencing on a similar display. “[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

Nonetheless, Patent Owner characterizes Kosiur as providing “aspirational disclosures that provide no details,” and that given the “lack of disclosure,” a skilled artisan would have no basis for combining it with Provino. PO Resp. 46. Aspirational language itself normally does not lend particular relevance to a patentability determination or point ordinary artisans away from advances that happen to involve a combination of similar teachings and similar techniques. *Cf. Antor*, 689 F.3d at 1289–90 (“the mere use of forward-looking language (such as terms like ‘should’) does not show one way or another whether a person of ordinary skill in the art would have to engage in undue experimentation to perform the claimed invention.”)

Patent Owner and Dr. Monroe also point to Kosiur’s disclosure of bandwidth and quality of signal constraints on “secure videoconferencing

[a]s another application of interest.” *Id.* at 45 (quoting Ex. 1006, 264; Ex. 2041 ¶ 51). Dr. Monroe faults Kosiur’s disclosure for not addressing the constraints. *See* Ex. 2041 ¶ 51. Nevertheless, the record shows that the skill level involved here indicates that combining the two teachings to arrive at VPN videoconferencing would be within an ordinary artisan’s capabilities. If anything, disclosures about higher bandwidth and quality of service constraints suggest a solution to such artisans—increasing the bandwidth to handle the higher data rate and the quality of service constraints, or simply accepting some trade-offs in quality of service. *See* Ex. 1011 ¶¶ 41–44 (Provino’s system does not limit “the services or applications that Provino’s VPN 15 may be configured to support.”); Pet. 46 (citing Ex. 1006, 254; Ex. 1011 ¶ 42).

Petitioner also explains that Kosiur discloses a wide variety of known features for VPNs, including various protocols, videoconferencing, transactional traffic, interactive media, IP telephony, file transfers, Web browsers, multimedia, and e-mail. *See* Pet. 46–49 (citing Ex. 1006, 9, 13, 243–249, 254; Ex. 1011 ¶¶ 41–44). Petitioner cites evidence that indicates videoconferencing or similar video services or applications would have been obvious in Provino’s similar system to “increase the mobility and productivity of the employees operating devices” in Provino. *See* Pet. 47 (citing Ex. 1006, 13, 254; Ex. 1011 ¶¶ 43–44).

Based on further review of the record, and for the reasons discussed above, Petitioner shows by a preponderance of evidence that the combination of Provino and Kosiur renders claims 2–5 obvious.

4) *Claims 7, 8, 10, 12, 13, 15, and 18*

Patent Owner contends that “*Provino* does not anticipate remaining claims 7, 8, 10, 12, 13, and 15, for at least the reasons discussed above for independent claim 1, from which they depend.” PO Resp. 44. Patent Owner also contends that *Provino* combined with *Xu* does not render claim 18 obvious, because “*Xu* . . . does not cure the deficiencies of *Provino* discussed . . . for claim 1.” *Id.* at 47.

Based on further review of the record, and for the additional reasons discussed *supra* in connection with claim 1 and presented in the Petition, Petitioner shows by a preponderance of evidence that *Provino* anticipates claims 7, 8, 10, 12, 13, and 15, and *Provino* combined with *Xu* renders claim 18 obvious. Pet. 23–44, 49–51; ’483IPR Pet. 17–33, 38–40.<sup>12</sup>

5) *Termination*

Patent Owner argues that this proceeding should be terminated because the Board’s reliance on *Provino*’s “tunnel set up for the claimed ‘access request message[]’ . . . applies a rationale different from the only one proposed by Petitioner[],” and, therefore, the Board “exceeded its statutory authority.” PO Resp. 38. Patent Owner does not contend that we relied exclusively on the *Provino*’s “tunnel set up” scenario. *See id.* at 39 (arguing that “adopting an *additional* rationale” exceeds statutory authority) (emphasis added). This Final Written Decision does not rely on that additional rationale, and the Institution Decision and the Final Written Decision rely on the same disclosure in *Provino* that Petitioner relies upon in

---

<sup>12</sup> As noted above in the Introduction, no material difference exists between the two petitions.

its Petition—Provino’s message packets to server 31(s). *See* Inst. Dec. 16–17; PO Resp. 37.

The Board has broad authority in institution decisions. *See Cuozzo*, 2015 WL 4097949, at \*3–4 (“We conclude that § 314(d) prohibits review of the decision to institute IPR even after a final decision.”). Patent Owner has not provided a sufficient showing to terminate the present proceeding.

#### IV. ORDER

Petitioner has demonstrated, by a preponderance of the evidence, that Provino anticipates claims 1, 7, 8, 10, 12, 13, 15, and 17 under 35 U.S.C. § 102; that the combination of Provino and Kosiur renders claims 2–5 obvious under 35 U.S.C. § 103(a); and that the combination of Provino and Xu renders claims 18 obvious under 35 U.S.C. § 103(a).

In consideration of the foregoing, it is hereby

ORDERED that claims 1–5, 7, 8, 10, 12, 13, 15, 17, and 18 of the ’274 patent are unpatentable.

This is a final 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.



IPR2014-00403  
Patent 7,987,274 B2

**PETITIONER:**

Jeffrey P. Kushan  
Joseph A. Micallef  
SIDLEY AUSTIN LLP  
jkushan@sidley.com  
jmicallef@sidley.com

**PATENT OWNER:**

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

Jason E. Stach  
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP  
jason.stach@finnegan.com