

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

SSL SERVICES LLC,
Patent Owner.

Case IPR2015-01754
Patent 6,158,011

Before KEN B. BARRETT, MICHAEL W. KIM, and
DANIEL N. FISHMAN, *Administrative Patent Judges*.

FISHMAN, *Administrative Patent Judge*.

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

I. INTRODUCTION

A. Background

Cisco Systems, Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) for *inter partes* review of claims 1–7 of U.S. Patent No. 6,158,011 (Ex. 1001) (“the ’011 patent”) pursuant to 35 U.S.C. §§ 311–319. SSL Services LLC (“Patent Owner”) filed a Patent Owner’s Preliminary Response (Paper 8, “Prelim. Resp.”). On February 23, 2016, based on the record before us at the time, we instituted an *inter partes* review of all claims (1–7) (Paper 9, “Decision to Institute” or “Dec.”). We instituted the review on the following challenges to the claims:

References	Basis	Claims challenged
Alden ¹ , Takahashi ² , Quinn ³ , and Schneier ⁴	§ 103(a)	1–7

Dec. 25.

After we instituted this review, Patent Owner filed a Patent Owner Response (Paper 28, “PO Resp.”)⁵ and Petitioner filed a Corrected Reply

¹ Alden et al., U.S. Patent No. 6,101,543 (filed Oct. 25, 1996) (Ex. 1006) (“Alden”).

² Yasuhiro Takahashi et al., *Communication Method with Data Compression and Encryption for Mobile Computing Environment*, INET96 Proc. (June 24–28, 1996), http://www.isoc.org/inet96/proceedings/a6/a6_2.htm (Ex. 1007) (“Takahashi”).

³ Bob Quinn & Dave Shute, *Windows™ Sockets Network Programming* (Alan R. Feuer, ed., 4th prtg. 1997) (Ex. 1008) (“Quinn”).

⁴ Bruce Schneier, *Applied Cryptography* (Paul Farrell, ed., 1994) (Ex. 1009) (“Schneier”).

⁵ Paper 28 is filed under seal. A redacted version of PO Resp. is filed as Paper 29.

(Paper 50, “Pet. Reply”).⁶ Petitioner relies on the Declaration of Dr. Michael Caloyannides (Ex. 1004). Patent Owner relies on the Declaration of Dr. John A. Hamilton (Ex. 2011).⁷

Petitioner filed a Motion to Exclude (Paper 47), to which Patent Owner filed an Opposition (Paper 52). Petitioner then filed a Reply to Patent Owner’s Opposition (Paper 54). Patent Owner filed a Motion to Exclude (Paper 48), to which Petitioner filed an Opposition (Paper 51). Patent Owner then filed a Reply to Petitioner’s Opposition (Paper 53). Oral hearing was conducted on November 15, 2016. The record contains a transcript of the hearing (Paper 57, “Tr.”)

We have jurisdiction under 35 U.S.C. § 6(c). The evidentiary standard is a preponderance of the evidence. *See* 35 U.S.C. § 316(e); *see also* 37 C.F.R. § 42.1(d). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

For the reasons expressed below, we conclude that Petitioner has demonstrated by a preponderance of evidence that claims 1–7 are unpatentable.

B. The ’011 patent

The ’011 patent relates to “a system and method for allowing private communications over an open network, and in particular to a virtual private network which provides data encryption and mutual authentication services for both client/server and peer-to-peer applications at the applications,

⁶ Paper 50 is filed under seal. A redacted version of Petitioner’s Corrected Reply is filed as Paper 49.

⁷ Exhibit 2011 is filed under seal. A redacted version of the Exhibit is filed as Exhibit 2012.

transport driver, and network driver levels.” Ex. 1001, 1:10–16. The ’011 patent acknowledges two known approaches for providing encryption for such secured communications — first, a dedicated server that provides encryption and authentication services for clients using a network (i.e., a client/server architecture), and second, private, secured communications between any two cooperating computers on a network (i.e., a peer-to-peer architecture). *Id.* at 1:31–40. According to the ’011 patent, previously known approaches for encrypted peer-to-peer communications over a virtual private network (“VPN”) required modifications to various layers of the communications software, as compared to client/server applications, using a VPN rendering the two architectures mutually exclusive. *Id.* at 1:58–66.

To remedy such problems, the ’011 patent discloses maintaining the general architecture of the known client/server architecture for encrypted communication, and adding one or more “shims” to lower level communications software “in order to accommodate a variety of peer-to-peer communications while utilizing the applications level infrastructure for authentication and session key generation purposes.” *Id.* at 2:13–20.

Specifically, the ’011 patent discloses:

The changes made by the present invention to the conventional client server virtual private network may be thought of as, essentially, the addition of means, most conveniently implemented as shims, which add a secured mutual authentication and session key generation channel between the server and all parties to a communication, at all levels at which a communication can be carried out.

Id. at 2:41–48.

Figure 5 of the '011 patent, reproduced below, shows various embodiments of shims (50, 53, and 55):

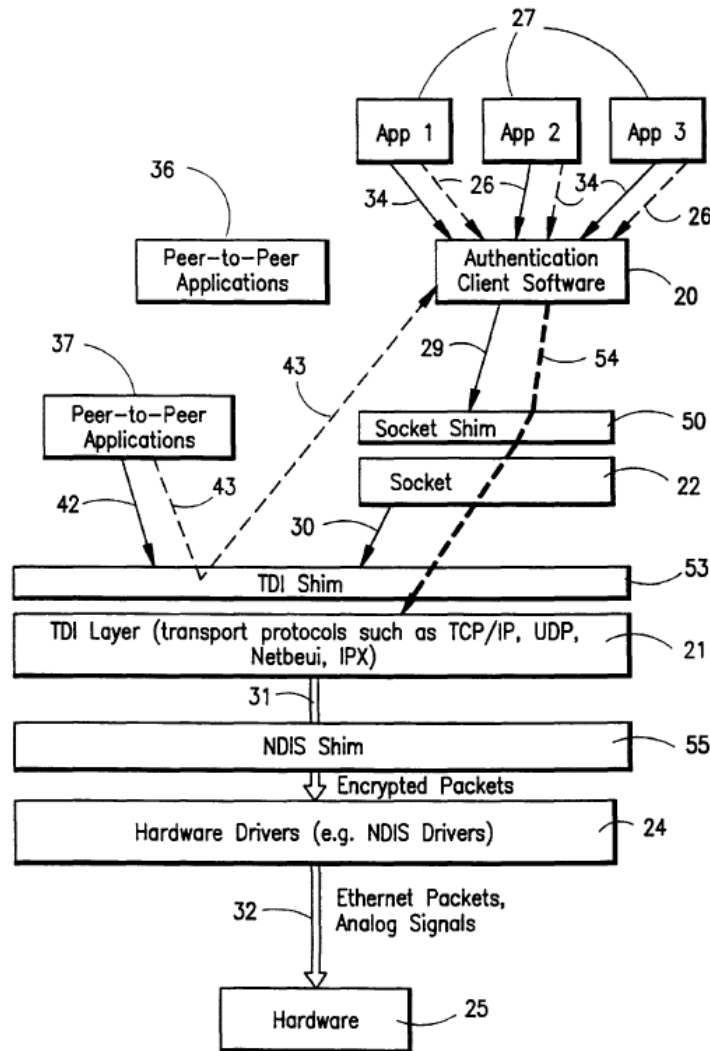


FIG. 5

Figure 5 of the '011 patent, reproduced above, discloses exemplary shims (50, 53, and 55) inserted between layers of the communication software modules to enable support for peer-to-peer secured communications (36, 37) utilizing applications level authentication and encryption (20) with minimal modifications to the various software elements of the system.

The '011 patent discloses that various configurations of one or more of shims 50, 53, and 55 may be implemented to provide various levels of security. *See id.* at 9:46–11:19 (describing functions of shims 50, 53, and 55 in reference to Figures 3–5).

C. *Related Matters*

Both parties identify the following related court proceedings involving the '011 patent: *SSL Servs., LLC v. Cisco Sys., Inc.*, Case No. 2:15-cv-00433 (E.D. Tex.); *SSL Servs., LLC v. Citrix Sys., Inc.*, Case No. 13-1419 (Fed. Cir.); *Juniper Networks, Inc. v. SSL Servs., LLC*, Case No. 4:08-cv-05758 (N.D. Cal.); and *SSL Servs., LLC v. Citrix Sys., Inc.*, Case No. 2:08-cv-00158 (E.D. Tex.). Pet. 1; Paper 5, 2; Paper 35, 2. Patent Owner identifies additional court proceedings involving the '011 patent: *SSL Servs., LLC v. Citrix Sys., Inc.*, Case No. 13-1420 (Fed. Cir.) and *Juniper Networks, Inc. v. SSL Servs., LLC*, Case No. 10-1107 (Fed. Cir.). Paper 5, 2; Paper 35, 2.

Both parties also identify the following related *Ex Parte* Reexamination proceedings involving the '011 patent: Control No. 90/011,242 (“the '242 reexamination”), Control No. 90/020,048 (“the '048 reexamination”), and Control No. 90/013,253 (“the '253 reexamination”). Pet. 1; Paper 5, 2; Paper 35, 2.

D. *Illustrative Claims*

Independent claim 1, reproduced below, is exemplary of the invention:

1. Apparatus for carrying out communications over a multi-tier virtual private network, said network including a

server and a plurality of client computers, the server and client computers each including means for transmitting data to and receiving data from an open network, wherein said means for transmitting data to and receiving data from an open network includes a lower set of communications drivers, said lower set of communications drivers being arranged to receive function calls and requests for service from an applications program in order to transmit and receive said data comprising:

means for intercepting said function calls and requests for service sent by said applications program to said lower level set of communications drivers, said intercepted function calls and requests for service being limited to communications functions with no reference to encryption functions;

means for causing an applications level authentication and encryption program in said one of said client computers to communicate with the server in response to receiving said intercepted function calls and requests for service by generating a session key, using the session key generated by the applications level authentication and encryption program to encrypt file sent by the applications program, and sending function calls and requests for service to the lower level set of communications drivers in order to transmit said encrypted files over said open network.

Ex. 1001, 12:40–67.

II. ANALYSIS

A. *Claim Construction*

In an *inter partes* review, a claim in an unexpired patent shall be given its broadest reasonable construction in light of the specification of the patent in which it appears. 37 C.F.R. § 42.100(b); *see also* *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2142 (2016) (affirming that USPTO has statutory authority to construe claims according to 37 C.F.R. § 42.100(b)).

Under the broadest reasonable construction standard, claim terms are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

Additionally, all challenged claims include one or more “means” elements. Use of the word “means” in a claim gives rise to a rebuttable presumption that 35 U.S.C. § 112, sixth paragraph analysis applies to interpret the claim. *Personalized Media Commc’ns, LLC v. Int’l Trade Comm’n*, 161 F.3d 696, 703–04 (Fed. Cir. 1998). In deciding whether that presumption has been rebutted, “the focus remains on whether the claim as properly construed recites sufficiently definite structure to avoid the ambit of § 112, ¶ 6.” *Id.* at 704.

On the record before us, we determine that most claim terms do not need express interpretation. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (holding that only those terms that are in controversy need to be construed, and only to the extent necessary to resolve the controversy).

1. *Previously Construed Terms*

In our Decision to Institute, we construed the claim terms “means for transmitting data to and receiving data from an open network,” “means for intercepting...,” “means for causing...,” and “shim.” Dec. 10–15. In particular, we construed the means for transmitting and receiving as reciting sufficient structure (including a “lower set of communication drivers”) so as to rebut a presumption that 35 U.S.C. § 112, sixth paragraph interpretation applies. *Id.* at 12. We construed “shim” to mean “software that is added

between two existing layers, which utilizes the same function calls of the existing layers.” *Id.* at 15. Lastly, we construed the “means for intercepting...” and the “means for causing...” under section 112, sixth paragraph to be disclosed in the ’011 patent as the structure of a “shim” and equivalent structures. *Id.* at 12–14.

Although the parties discuss and apply these claim constructions, neither party contests these claim constructions themselves. We see no reason to modify them in light of the record developed at trial. *See SAS Institute, Inc. v. ComplementSoft, LLC.*, 825 F.3d 1341, 1351 (Fed. Cir. 2016) (holding that the Board may not change a claim interpretation from the institution decision where neither party anticipated that “already-interpreted terms were actually moving targets”).

We determine no other terms require construction.

B. Obviousness over Alden, Takahashi, Quinn, and Schneier

Petitioner contends that claims 1–7 are obvious over the combination of Alden, Takahashi, Quinn, and Schneier, and provides analysis of each claim, mapping each feature of each claim (1–7) to disclosures of the combined references. Pet. 10–60. Patent Owner disagrees, arguing, for various reasons, that Alden and Takahashi cannot be combined (PO Resp. 16–48), secondary considerations demonstrate the claims are not obvious (*id.* at 48–50), and, even if the references can be properly combined, the proposed combination fails to render the claims obvious (*id.* at 50–59). Petitioner replies countering each of Patent Owner’s responses. Pet. Reply 2–29.

Obviousness is a question of law based on subsidiary findings of fact relating to “the scope and content of the prior art, differences between the prior art and the claims at issue, the level of ordinary skill in the pertinent art, and any objective indicia of nonobviousness.” *Randall Mfg. v. Rea*, 733 F.3d 1355, 1362 (Fed. Cir. 2013) (citing *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007)). Furthermore, the *KSR* Court guides us that,

“there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness” [H]owever, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ. 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

With these standards in mind, we address the obviousness challenge below.

1. *Level of Ordinary Skill*

Dr. Caloyannides opines that a person of ordinary skill in the relevant art would possess “(i) a Bachelor’s degree in Computer Science, Electrical and/or Computer Engineering, or equivalent training, and (ii) approximately two to three years of virtual private network implementation and engineering experience.” Ex. 1004 ¶ 45. Dr. Caloyannides further clarifies that “[l]ack of work experience can be remedied by additional education, and vice versa.” *Id.* Patent Owner’s expert, Dr. Hamilton, agrees with Dr. Caloyannides’ characterization of the level of ordinary skill in the art. Ex. 2011 ¶ 61. Furthermore, we find the parties’ definition of the level of ordinary skill in the art is commensurate with the level of ordinary skill in the art as reflected in the prior art. See *Okajima v. Bourdeau*, 261 F.3d

1350, 1355 (Fed. Cir. 2001) (“[T]he absence of specific findings on the level of skill in the art does not give rise to reversible error where the prior art itself reflects an appropriate level and a need for testimony is not shown.”) (internal quotations omitted); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995).

a. Petitioner’s Motion to Exclude Expert Testimony

Relating to the level of ordinary skill, Petitioner asks us to exclude the entirety of Dr. Hamilton’s Declaration (Exs. 2011 and 2012) alleging he is not qualified as an expert because he lacks “the requisite ‘scientific, technical, or other specialized knowledge’ to assist the Board with evaluating the obviousness of the ’011 patent claims.” Paper 47, 4. Petitioner argues Dr. Hamilton lacks sufficient expertise based upon his answer to certain questions in a deposition, in which Dr. Hamilton indicated he would have to do a “literature review” to answer the question. *Id.* at 3. Petitioner further argues Dr. Hamilton demonstrated lack of expertise by testifying “that a ‘routing table is not part of the TCP/IP stack.’” *Id.* at 3–4. Petitioner also contends Dr. Hamilton’s Declaration should be excluded because, although he essentially agreed with the description of the background of an ordinarily skilled person provided by Dr. Caloyannides, Dr. Hamilton’s deposition testimony “demonstrated his confusion and lack of familiarity with what the POSITA skill level represents.” *Id.* at 5. Petitioner asserts Dr. Hamilton, in his deposition testimony, “repeatedly referred to his idea of a ‘POSITA’ representing a variety of different individuals with differing skillsets and knowledge levels.” *Id.* at 6. Petitioner argues, “[c]ontrary to Dr. Hamilton’s mistaken beliefs, there is no

room for numerous different ‘POSITAs’ in a properly structured obviousness analysis,” and, therefore, “Dr. Hamilton’s mistaken beliefs infect and render unreliable the entirety of his declaration.” *Id.* at 7.

Patent Owner opposes Petitioner’s Motion, arguing that each of Petitioner’s grounds for excluding Dr. Hamilton’s testimony goes to the weight to be accorded his Declaration, rather than to admissibility of his declaration. Paper 52.

We agree with Patent Owner that each of Petitioner’s bases to exclude Dr. Hamilton’s testimony are properly directed to the weight to be accorded his testimony rather than to admissibility. The Board is fully capable of weighing the reliability of such expert testimony. *See, e.g., Yorkey v. Diab*, 601 F.3d 1279, 1284 (Fed. Cir. 2010) (holding the Board has discretion to give more weight to one item of evidence over another “unless no reasonable trier of fact could have done so”). Therefore, we will consider Dr. Hamilton’s testimony in light of Petitioner’s assertions, and accord it the proper weight.

We agree with Petitioner’s observations in its Motion to Exclude, however, that Dr. Hamilton’s testimony expresses a varying, dynamic interpretation of the skills of an ordinarily skilled artisan, depending on the particular issue. Paper 47, 5–8. Dr. Hamilton’s variable standard of what an ordinarily skilled artisan would understand in the ’011 patent and in the prior art references raises concerns that we address by the weight we accord his testimony in the analysis that follows.

2. Summary of Alden, Takahashi, Quinn, and Schneier

a. Alden (Ex.1006)

Alden discloses a pseudo network adapter for coupling to a virtual private network. Ex. 1006, 3:2–3. The pseudo adapter captures packets from the local protocol stack appearing to the protocol stack as a driver for a network adapter. *Id.* at 3:3–9. The pseudo adapter transmits captured packets to an encryption engine and encapsulates the encrypted packet into a tunnel packet. *Id.* at 3:19–25. Alden Figure 21, reproduced below, depicts an exemplary data flow in an exemplary pseudo adapter embodiment.

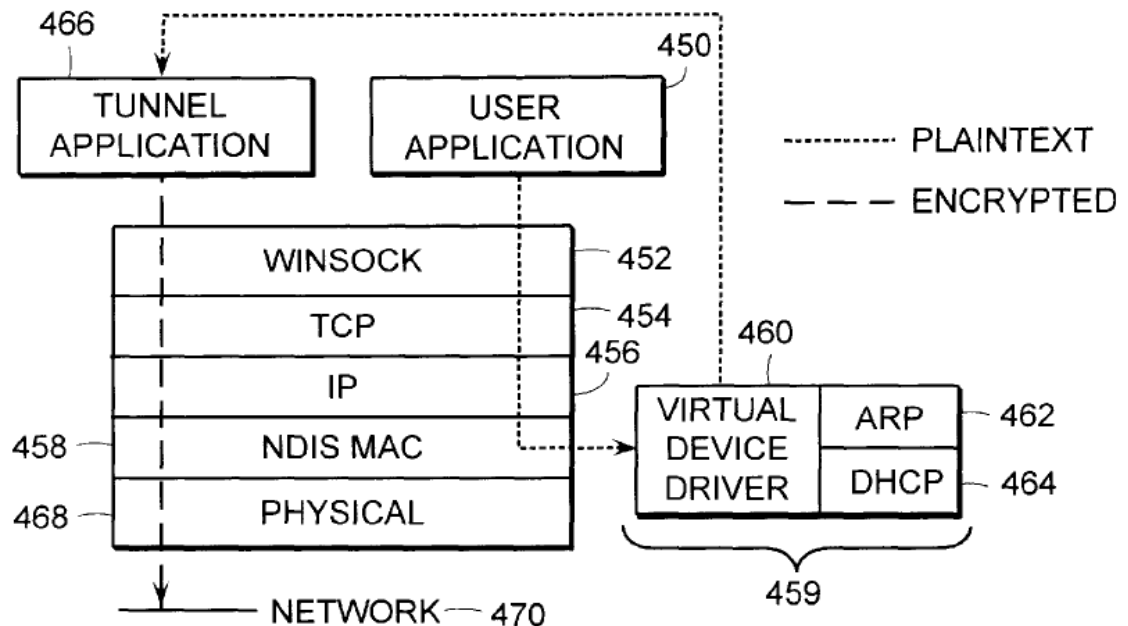
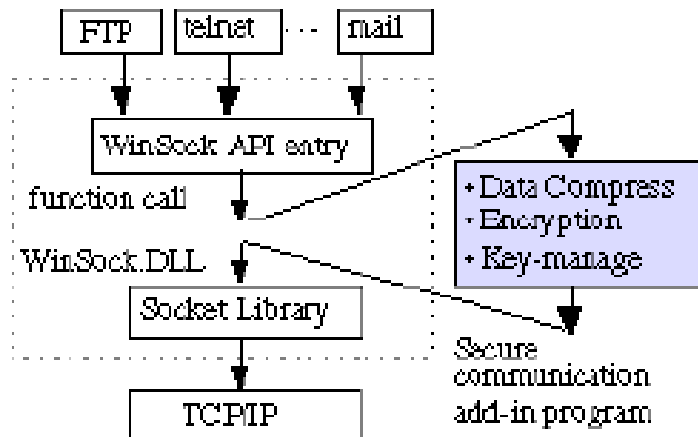


FIG. 21

Alden's Figure 21 shows pseudo adapter 459 that captures plaintext packets from NDIS MAC layer 458 of protocol stack 454–458, and forwards the captured plaintext packets to tunnel application 466 for encryption and encapsulation to create tunnel packets, which are, in turn, transmitted back through the protocol stack to network 470. *See id.* at 18:14–49.

b. Takahashi (Ex. 1007)

Takahashi discloses an “add-in” program that intercepts Winsock⁸ commands to compress and encrypt data of the intercepted commands. Ex. 1007, 1. The compression and encryption is achieved “without changing the TCP/IP and application software by intercepting Winsock commands from Winsock API [(application program interface)] temporarily and adding individual processing.” *Id.* at 2. Figure 2 of Takahashi (reproduced below) depicts exemplary data flow for Takahashi’s solution.



Takahashi Figure 2 shows a secure communication add-in program (highlighted in purple) that performs data compression, encryption, and key management by: intercepting function calls of the Winsock API (invoked by an application such as FTP, telnet, or mail); processing the data of the intercepted command (i.e., to encrypt or compress); and forwarding the Winsock function call to the Winsock DLL with the associated data encrypted and/or compressed.

⁸ Some references identify this layer as “WinSock” and others identify it as “Winsock.” For consistency in this Decision, we refer to this layer as “Winsock.”

c. Quinn (Ex. 1008)

Quinn is an excerpt from a reference book describing details of exemplary functions of the Winsock DLL library. *See* Ex. 1008, 4.

d. Schneier (Ex. 1009)

Schneier is an excerpt from a reference book describing exemplary techniques for encryption key generation and management. *See* Ex. 1009, 4–7.

3. Mapping the Claims to the Combined Teachings

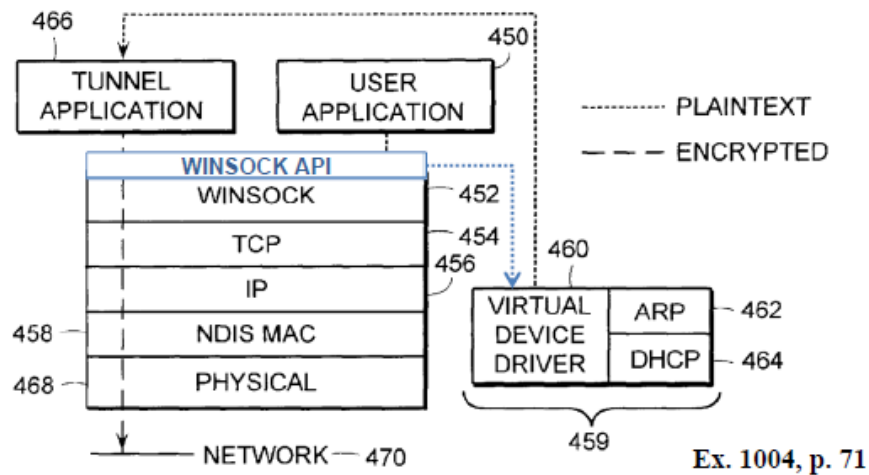
a. Petitioner's Arguments

i. Claim 1

Regarding independent claim 1, Petitioner argues Alden discloses the various recitations of the preamble of claim 1. Pet. 19–34. In particular, Petitioner argues the recited means for transmitting and receiving that includes the “lower set of communications drivers being arranged to receive function calls and requests for service from an applications program in order to transmit and receive said data” is disclosed as the protocol stack depicted in, for example, Alden’s Figure 21, as reproduced above. *Id.* at 22–32. According to Petitioner, Alden discloses use of the Winsock API (*id.* at 32–33), but does not describe details of the Winsock functions for receiving and transmitting data (*id.* at 33). Thus, Petitioner relies on Quinn, in combination with Alden, for disclosing details of Winsock function calls to send and receive data and provides a reason to combine Alden and Quinn. *Id.* at 33–34; *see also id.* at 16–18.

As discussed *supra*, Alden does not disclose a structure that intercepts function calls, but instead discloses pseudo adapter 459 installed at the link layer (NDIS MAC) of the protocol stack, the pseudo adapter operable to receive packets routed thereto and re-direct those packets to tunnel application 466 for applications level encryption and re-transmission through the protocol stack to the destination through the network. *See, e.g.*, Ex. 1006, Fig. 21, 18:14–49. Petitioner maps the recited means for intercepting to the disclosures of Takahashi in combination with Alden and Quinn. Pet. 34–40. Specifically, Petitioner argues Takahashi’s add-in program (i.e., a *shim* as we construe the term) intercepts Winsock function calls from an application program directed to the Winsock layer using the Winsock application program interface (API)—i.e., as a shim (“software that is added between two existing layers, which utilizes the same function calls of the existing layers”). *Id.* at 35–36.

Petitioner provides an annotated version of Alden’s Figure 21 excerpted from Dr. Caloyannides’ expert testimony (Ex. 1004 ¶ 141), modified to reflect the proposed combination with Takahashi’s Winsock interceptor disclosing the means for intercepting as a *shim*. Pet. 38. The annotated Figure 21 is reproduced below:



The above diagram (excerpted from Petitioner’s expert testimony with Dr. Caloyannides’ annotations) shows Alden’s pseudo adapter 459 modified to serve as a *shim* inserted between user application 450 and the Winsock layer 452, as taught by Takahashi’s add-in program—i.e., modified to be software that is added between two existing layers, which utilizes the same function calls of the existing layers. Pet. 35–36, 38; *see also* Ex. 1004 ¶ 140–143; Ex. 1007, 2, Fig. 2.

Petitioner argues the functions of Winsock (as detailed in Quinn) do not address encryption and, thus, the proposed combination of Alden, Takahashi, and Quinn meets the claim limitation that “said intercepted function calls and requests for service are limited to communication functions with no reference to encryption functions.” Pet. 38–40.

Petitioner also contends the recited “means for causing” is disclosed by the combined teachings of Alden and Takahashi, where the proposed modified pseudo adapter 459 (exemplified in the above-reproduced, annotated Figure 21) causes the recited communication in response to the shim intercepting a function call or request. Pet. 40–43. Specifically, in accord with our interpretation of “means for causing” and “shim,” Petitioner

contends the proposed modified pseudo adapter intercepts Winsock functions and utilizes Alden's tunnel application 466 to perform encryption and authentication at the applications level in conjunction with a server. *Id.* at 40–41. Petitioner asserts,

Takahashi's negotiation process is a mutual authentication process, similar to the one disclosed in Alden. Ex. 1007, p. 3; Ex. 1004, [p.] 111. During the negotiation process, the client sends the connection requirement associated with the intercepted `connect()` function to the server. Ex. 1007, pp. 3 & 6. As such, *Alden and Takahashi together teach* that Alden's tunnel application is caused to communicate with the server for initiating the negotiating sequence *in response to receiving the intercepted connect() function* and requests for connection from the modified pseudo network adapter. Ex. 1004, pp. 113–114.

Id. at 41–42 (emphasis added). Petitioner further asserts Alden, in the proposed combination, discloses the recited authentication and encryption functions in the functioning of tunnel application 466. *Id.* at 42.

Petitioner cites Schneier, in combination with Alden, Takahashi, and Quinn, for disclosing details regarding generation and management of session keys in encryption. Pet. 18–19. Specifically, Petitioner argues the combination of Alden, Takahashi, Quinn, and Schneier discloses well-known functions for authentication/encryption server communications, including generating a key (*id.* at 43–44) and using the generated key to encrypt files (*id.* at 44–46).

Lastly, regarding claim 1, Petitioner asserts the proposed combination discloses sending intercepted function calls and requests to lower level drivers to transmit encrypted files as recited by using Alden's protocol stack (454, 456, 458) to send and receive encrypted files via network 470 (i.e.,

using tunnel application 466 for application level encryption/decryption).
Pet. 46–47.

ii. *Claims 2–7*

Independent claim 2 claims a virtual private network comprising a server and a plurality of clients where each of these elements includes a “means for transmitting data to and receiving data from an open network.” The claim further defines the means for transmitting and receiving as generally including applications level encryption software, lower level set of communication drivers, and a shim arranged to intercept function calls from an applications program to cause the applications level encryption program to send encrypted files over the network. Thus, as discussed *supra*, this “means” element recites sufficient structure so as to rebut the presumption that 35 U.S.C. § 112, sixth paragraph analysis applies. Similar to analogous elements of claim 1, Petitioner identifies each of these elements in the proposed combination of references. Pet. 47–50.

Claim 3 depends from claim 2 and recites that the applications program generates packets to be supplied to a network driver layer via a socket interface and where the shim is a “socket shim” that intercepts the requests from the applications program to the socket interface in order to cause the applications level encryption program to encrypt the packets before transmission to the network. Petitioner identifies the elements of claim 3 in the combined references. Pet. 50–53. Takahashi’s Winsock interceptor is a shim specifically to intercept function calls from a socket interface—i.e., a Winsock API socket interface. Thus, Petitioner asserts the combined prior art references disclose the recited “socket shim” of claim 3. *Id.* at 52.

Independent claim 4 claims software that includes applications level encryption and a shim similar to the features recited in claims 1 and 2. Petitioner identifies these features in the combined references similar to analogous features identified for claims 1 and 2. Pet. 53–57.

Claims 5 and 6 depend from claim 4—claim 5 reciting the shim is a socket shim positioned between an applications program and an application socket, and claim 6 reciting that the shim is positioned between the applications program and the driver level. Petitioner identifies these features in the combined references. Pet. 57–59.

Independent claim 7 is a method claim reciting as method steps the functions of the means for intercepting and the means for causing recited in claim 1. Petitioner identifies these method steps in the combined references using the same disclosures as identified in claim 1. Pet. 59–60

b. Patent Owner's Response

Patent Owner argues, even if the references are properly combined, for the reasons discussed below, the combined teachings fail to teach or suggest every element of the claims.

i. Takahashi Is Deficient

Patent Owner contends the combination fails to teach all elements because Takahashi would not have sufficiently informed an ordinarily skilled artisan as to how to create a Winsock interceptor as relied upon by Petitioner. PO Resp. 51. In particular, Patent Owner argues Takahashi discloses its Winsock interceptor alters the “linkage between the application program and the Winsock DLL” (*id.* (citing Ex. 1007, 2)), but asserts

Takahashi “does not explain how to change this linkage to perform the interception, and a POSITA would not have known how to create Takahashi’s interceptor” (*id.* (citing Ex. 2011 ¶ 78⁹)).

Petitioner replies arguing the ’011 patent, *per se*, admits that Winsock interceptors were well-known. Pet. Reply 19 (citing Ex. 1001, 7:1–3 (“[i]n one especially preferred embodiment of the invention, the client software includes a Winsock shim arranged to intercept function calls to the Winsock library on a client”), 10:16–17 (“while it is appreciated that the use of socket shims is well-known”)); *see also* Pet. Reply 15–16. Petitioner further argues the ’011 patent demonstrates Winsock shim technologies were well-known because it refers to a publication by Stardust Technologies that discloses Winsock shim technology (*id.* at 16 (citing Ex. 1001, 5:63–65; Ex. 1002, 154)). Petitioner further contends other patents at the time similarly recognized the well-known use of Winsock shims by referring to products from Stardust Technologies. *Id.* (citing Ex. 1040, 7:58–66 (“to ‘hook’ or intercept datastreams being communicated to and from [an] application program. . . . such as a WINSOCK program”))).

Based on the above, we are not persuaded Takahashi would have failed to inform the ordinarily skilled artisan how to make or use its add-in program (a Winsock shim). The ’011 patent relies on well-known, commercially available, Winsock interceptor technology (i.e., Stardust Technologies) for disclosing a Winsock shim in its “especially preferred embodiment.” Ex. 1001, 7:1–3. This fact alone is sufficient to show that the

⁹ We believe Patent Owner intended to cite paragraph 77 of Exhibit 2011, in which Dr. Hamilton opines “that Cisco’s prior art does not enable one of ordinary skill in the art to implement Takahashi’s Winsock interceptor.”

ordinarily skilled artisan, at the time of the '011 patent, would have known how to make and use a Winsock interceptor (shim) based on the limited disclosure of the '011 patent.

Patent Owner further alleges implementation of a Winsock shim would have been beyond the skill level of the ordinarily skilled artisan at the time of the '011 patent. PO Resp. 51; Ex. 2011 ¶¶ 69, 77. In support of this contention, Patent Owner primarily relies on Dr. Hamilton's Declaration (Ex. 2011) and Exhibits 2014, 2015, and 2016. PO Resp. 17–23, 50–53. Dr. Hamilton's testimony, in support of the assertion that hooking Winsock is difficult and error prone, similarly relies on the same Exhibits. Ex. 2011 ¶¶ 68–77.

We accord little weight to Exhibit 2015 principally because the document bears a date in 2005—eight years after the earliest priority date of the '011 patent. As noted by Petitioner, the Windows[®] operating system, in which Winsock operates, changed versions a number of times during those eight years, potentially requiring developers to design a similar number of versions of a Winsock interceptor to be created and maintained. Pet. Reply 2–5. Thus, the fact that eight years after the '011 patent filing, Cisco engineers determined there were technologically simpler, less error-prone, and commercially viable approaches to the desired goal does not provide sufficiently probative evidence regarding the difficulty to implement a Winsock shim at the time of the '011 patent. As noted by Petitioner, such a task could have been more or less difficult at the time of the '011 patent and could have been more or less commercially desirable at the time of the '011 patent. See Pet. Reply 2–3. For similar reasons, Mr. Parla's testimony (Exhibit 2016) regarding Exhibit 2015 is of little value to our decision

process because the underlying Exhibit 2015 is of little probative value. Thus, we also accord little weight to Exhibit 2016.

Patent Owner further relies on an excerpt of Dr. Caloyannides' deposition testimony suggesting that, even with his extensive expertise, he did not know how to modify Alden to use a Winsock shim such as Takahashi's add-in program. PO Resp. 52 (citing Ex. 2014, 149:14–150:7). This assertion similarly fails to evidence the difficulty in implementing the Winsock shim at the time of the '011 patent filing. Specifically, when asked "what changes do you have to make to the software so that function calls go from Winsock API to box 459," Dr. Caloyannides testified. "I'm not a programmer by profession, . . . [thus] I cannot specify exactly what programming lines do what, if that's what you're asking me." Ex. 2014, 149:17–21. Whether Dr. Caloyannides could create the specific lines of code to implement a Winsock shim is not a relevant measure of the sufficiency of the disclosure of Takahashi. *See Robotic Vision Sys., Inc. v. View Eng'g, Inc.*, 112 F.3d 1163, 1166 (Fed. Cir. 1997), *citing Fonar Corp. v. Gen. Elec. Co.*, 107 F.3d 1543, 1549–50 (Fed. Cir. 1997) (stating that "when disclosure of software is required, it is generally sufficient if the functions of the software are disclosed, it usually being the case that creation of the specific source code is within the skill of the art"). Dr. Caloyannides further testified "I would imagine there are changes that a person who's a programmer at heart and by experience would know by looking at what Alden has and what Takahashi has, and then merging the two." Ex. 2014, 150:4–7. Thus, Patent Owner's reliance on Dr. Caloyannides' deposition testimony similarly fails to shed light on how difficult it would have been for

an ordinarily skilled person to implement Takahashi's Winsock interceptor and, thus, deserves little weight on this issue.

Dr. Hamilton's Declaration also is accorded little weight regarding this issue. As argued in Petitioner's Motion to Exclude discussed *supra*, Dr. Hamilton's deposition testimony on this issue suggests confusion on his part with regard to what knowledge a person of ordinary skill would possess. Paper 47, 5–8. Specifically, Dr. Hamilton testified, “even within the agreed-to definition of a person of ordinary skill in the art, you’re going to have widely varying subsets of knowledge.” Ex. 1034, 59:20–23. Later, Dr. Hamilton testified, “some people of ordinary skill in the art, you know, would be familiar with sockets and would be familiar with hooking function calls. And some, you know – and some wouldn’t.” *Id.* at 79:3–6. Still further, Dr. Hamilton testified, “depending on when the POSITA graduated and became that kind of person, they may or may not even [have] had Winsock on their Windows computer at that time.” *Id.* at 92:1–3. Although we *dismiss* the motion to exclude Dr. Hamilton's testimony, on this issue regarding sufficiency of the prior art disclosure in particular, we accord little weight to his opinion.

Weighing the above considerations, we determine Takahashi sufficiently discloses to the ordinarily skilled artisan how to make and use a Winsock shim in the proposed combination.

ii. *Interception “In Order to Cause...”*

Independent claim 2 includes “a shim arranged to intercept ... in order to cause the applications level authentication and encryption program to communicate with the server, generate said session key, and encrypt files.”

Independent claims 4 and 7 each include a substantially similar recitation. Patent Owner argues the parties agree that Alden, alone, fails to teach this feature, because Alden's pseudo adapter "does not receive communications before any alleged session key is generated, and thus cannot 'intercept function calls and requests for service . . . in order to cause the applications level authentication and encryption program to . . . generate said session key.'" PO Resp. 53–54. Patent Owner acknowledges that the Petition relies on the combination of Alden with Takahashi (and Quinn and Schneier) to disclose this feature, but argues, "even if Alden and Takahashi are combined, Alden will still create the alleged 'session key' during initialization, before the modified pseudo network adapter intercepts any communications" and, thus, the combination fails to disclose this limitation. *Id.* at 54–55. Patent Owner then acknowledges that Petitioner's proposed combination modifies Alden to utilize Takahashi's "negotiation sequence." *Id.* at 55.

Patent Owner's argument improperly attacks the teachings of Alden in isolation from the proposed combination. *See In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986). In Petitioner's proposed combination, Takahashi's negotiation sequence to generate an encryption key is initiated in response to interception of a "connect ()" Winsock function call. Pet. 41–43; Pet. Reply 26. Furthermore, the test of obviousness does not require bodily incorporation of Takahashi with Alden, but rather considers what the combination would have suggested to the ordinary skilled artisan. *See In re Keller*, 642 F.2d 413, 425 (CCPA 1981). Thus, Petitioner's proposed combination teaches or suggests the recited "shim . . . in order to cause . . ." as previously discussed (section II.B.3.a.ii above).

iii. No Shim

Patent Owner argues the Petitioner fails to “explain how the Takahashi add-in program which, according to [Petitioner], operates ‘at the Winsock layer,’ is software that is added ‘between’ two existing layers.” PO Resp. 58. We disagree. The Petitioner sufficiently identifies Alden’s pseudo adapter, as modified by Takahashi, residing between the applications layer and the Winsock layer to intercept the Winsock function calls using the same Winsock functions, thus, concluding the modified pseudo adapter is a “shim,” as we have construed the term. Pet. 41–43. Petitioner further explains this proposed structure implements a Winsock shim in the same manner as the Winsock shim discussed as the preferred embodiment of the ’011 patent, and observes Dr. Hamilton’s concession in this regard. Pet Reply 27 (citing Ex. 1034, 44:23–45:4). We agree with Petitioner that the Petition sufficiently explains how Takahashi’s Winsock interceptor functions as a “shim” in the proposed combination with Alden.

c. Summary Regarding the Combined Teachings

We have reviewed Petitioner’s identification of the features of all claims in the proposed combination of Alden, Takahashi, Quinn, and Schneier. Other than the arguments addressed above, Patent Owner does not present arguments regarding the sufficiency of the teachings in the proposed combination with respect to individual claim limitations. We have reviewed all of Petitioner’s above-referenced mappings of Alden, Takahashi, Quinn, and Schneier, and are persuaded that they are correct. Accordingly, we adopt them as our own. We are persuaded that the combination of Alden,

Takahashi, Quinn, and Schneier teaches or suggests every limitation of claims 1–7.¹⁰

4. *Motivation/Reasons to Make the Proposed Combination*

a. *Positions of the Parties*

Petitioner argues the ordinarily skilled artisan would have combined Takahashi with Alden for three reasons: (1) to reduce the overhead burden of Alden’s “pre-configuration” processing exemplified in Alden’s Figure 23; (2) to avoid the need for Alden to modify the TCP/IP protocol stack in establishing a new secure connection because Takahashi specifically discloses an approach to avoid modifying the TCP/IP protocol stack; and (3) to enhance flexibility using Takahashi’s approach that allows secure access to any compatible device, because Takahashi does not require initialization and configuration processing of Alden to establish a new secure connection. Pet. 12–16.

Petitioner also contends the ordinarily skilled artisan would have added Quinn to the combination to disclose details of Winsock application program interface functions, as in Quinn (Pet. 16–18), and contends the ordinarily skilled artisan would have added Schneier to the combination to disclose details of secure key generation as in Schneier (*id.* at 18–19). In particular, Petitioner contends that the ordinarily skilled artisan would have sought Schneier as a reference for secure key management, because it is identified as such a reference by Alden. Pet. 18; Ex. 1006, 1:55-59.

¹⁰ We address separately below whether Petitioner has provided sufficient evidence and reasoning to support making the proffered modifications.

Patent Owner responds to Petitioner’s reasons to combine, arguing Dr. Caloyannides testified that the alleged “pre-configuration” processing burden of Alden is nothing more than modifying data in the TCP/IP routing table, and questions why it would be considered burdensome. PO Resp. 27–28 (citing Ex. 2014, 112:1–7, 112:15–21, 35:20–36:11).¹¹

Petitioner replies, contending Patent Owner mischaracterizes Dr. Caloyannides’ testimony by selecting only portions thereof. Petitioner argues Dr. Caloyannides testified that the “pre-configuration” processing burden encompasses ten steps of processing, as depicted in Alden’s Figure 23 (culminating in potential updates to the TCP/IP routing table). Pet. Reply 6–7 (citing Ex. 2014, 23:12–25:5, 83:12–21). Petitioner further argues, Dr. Hamilton confirmed that only *after all ten steps of Figure 23 are performed*, can Alden’s devices engage in secure communications. Pet. Reply 7 (citing Ex. 1034, 123:5–9).

b. Analysis of Motivation to Combine

We agree with Petitioner that combining Takahashi’s disclosures with that of Alden would have reduced the “pre-configuration” processing burden of Alden, and the ordinarily skilled artisan would have been motivated to seek such improvement based on Takahashi’s disclosure that its method “can be used without modifying . . . communication control software, or application software.” Ex. 1007, 1; *see also* Ex. 1004 ¶ 114, 140–143. More specifically, we are persuaded that modification of the TCP/IP routing table is a modification of the protocol stack, in that it is data used by the

¹¹ Patent Owner does not respond to Petitioner’s arguments regarding motivation to combine Quinn and Schneier with Alden and Takahashi.

protocol stack to provide its routing capabilities, and the processing of Alden's Figure 23 to determine how the table should be modified may be considered a burden by the ordinarily skilled artisan. Alden requires a modification of the routing table. Takahashi suggests the undesirability of such modifications to the TCP/IP protocol stack (Ex. 1007, 1) and, thus, we are persuaded the proposed combination is expressly suggested by the prior art reference.

Patent Owner argues at Oral Hearing that there is no evidence in the record that Alden's pre-configuration constituted a burden or that the burden, if any, would have been recognized as a problem by the person of ordinary skill in the art. Tr. 21:22–22:5. However, “[u]nder the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.” *KSR*, 550 U.S. at 420; *In re Beattie*, 974 F.2d 1309, 1312 (Fed. Cir. 1992) (“As long as some [reason,] motivation or suggestion to combine the references is provided by the prior art taken as a whole, the law does not require that the reference be combined for the reasons contemplated by the inventor.”); *In re Kemps*, 97 F.3d 1427, 1430 (Fed. Cir. 1996) (“Although the motivation to combine here differs from that of the applicant, the motivation in the prior art to combine the references does not have to be identical to that of the applicant to establish obviousness.”). Here, the art “taken as a whole” clearly contemplates improved performance in addition to the goal of secure communications. In particular, Takahashi specifically observes the problems arising in secure communications as mobile computing environments have increased in performance (Ex. 1001, 1), and the problems in performance of encryption

techniques associated with such secure communications (*id.* at 2). Thus, we are persuaded that the ordinarily skilled person would have recognized the problem of computational burden in any system used for secure communications in a mobile computing environment (such as that of Takahashi, Alden, and the '011 patent).

Although Petitioner does not present evidence quantifying the degree of the burden reduction, a preponderance of the evidence persuades us that the pre-configuration processing burden exemplified by Alden's Figure 23 is reduced by the approach of Takahashi. Alden's approach requires each tunnel client that desires a secure virtual private network connection, to initiate the connection by a request sent to the tunnel server. Ex. 1006, 19:16–18 (“The steps shown in [Fig.] 23 are performed for example in the tunnel client 247 as shown in [Fig.] 14.”); *see also* Pet. 42; Ex. 1004, 104–114. This client request initiates processing within the client's TCP/IP stack to request an IP address for the client's pseudo adapter, and initiates processing within the tunnel server to emulate dynamic host configuration protocol (“DHCP”) processing to provide the needed IP address information. Ex. 1006 19:25–20:27. Included in this processing is modification of the routing table in the tunnel client. *Id.* at 19:60–20:4. By contrast, Takahashi's approach does not require this processing to establish a new, secure connection but, instead, merely intercepts a Winsock “connect ()” function call and exchanges a secure key with the compliant end-point based on the previously configured (as system start up) route to its known IP address. Accordingly, there is no need to modify the TCP/IP routing table for each new, secure connection.

Despite Patent Owner’s contentions to the contrary, Dr. Hamilton’s testimony confirms that Alden requires processing, exemplified in Figure 23, before a secure connection is established, and confirms that that processing includes steps 500 through 518 prior to determine the modification to the routing table in step 520. Ex. 1034, 103–123. In particular, we note Dr. Hamilton confirms that steps 512–518 require processing to emulate a DHCP server and to respond to an address resolution protocol (“ARP”) request in accordance with TCP/IP protocol—these steps are required to establish a route to the virtual address of the secure node to which a new connection is to be established. Ex. 1034, 119:13–123:9, 128:15–129:5 (“We are emulating ARP and emulating DHCP to get the correct address information, [(from the modified routing table)] . . . your network enabled applications are going to take the path that has been defined by the setup of the virtual device driver.”).

Relying on Dr. Hamilton’s testimony, Patent Owner further argues Takahashi and Alden share the same burden of updating the TCP/IP routing table (PO Resp. 28 (citing Ex. 2011 ¶¶ 86–88)), and argues that Alden’s modification of the TCP/IP routing table is not a modification of the TCP/IP protocol stack, but, instead, “Alden merely configures the routing table to have certain addresses, which is not a modification to the TCP/IP protocol stack” (*id.* at 34–35 (citing Ex. 2011 ¶¶ 23, 36, 37, 92)).

We disagree. Dr. Hamilton specifically testifies “most computers that communicate[] using the TCP/IP protocol update[] and populate[] [their] routing table upon system start up.” Ex. 2011 ¶ 87. Dr. Hamilton’s statement reveals a key distinction in that, although every computer using TCP/IP likely has a routing table, that table is populated once, upon *system*

start up (as Dr. Hamilton testified), not updated at each request for a new, secure connection, as required in Alden’s approach.

Dr. Hamilton further testifies that Takahashi discloses a similar burden to Alden’s updating of the routing table, in that “Takahashi imposes an equivalent burden, as the ports for secure communications must be pre-identified so they can be used during the negotiation sequence.” *Id.* ¶ 88. We agree with Petitioner that the secure port numbers assigned in Takahashi are, like a routing table, initialized at system start up and remain constant, not updated/modified with each new, secure connection. Pet. Reply 7–8 (citing Ex. 1034, 223:7–10, 223:23–224:6).

Still further, contrary to Dr. Hamilton’s testimony that Alden does not present a burden of modifying the TCP/IP stack, because the routing table is not part of the TCP/IP, we agree with Petitioner that Alden specifically recites that the routing tables are *within* the TCP/IP stack. Pet. Reply 9–10 (citing Ex. 1006, 19:60–61).

Thus, we are persuaded that the ordinarily skilled artisan would have looked to Takahashi’s approach, in combination with Alden’s virtual private network architecture, to reduce the processing required by Alden to initiate a new secure connection.

Regarding Petitioner’s reasons to combine Quinn and Schneier with Alden and Takahashi, we find Petitioner has articulated reasons based on rational underpinnings—namely, an ordinarily skilled artisan would have looked to the Quinn reference for background details on the Winsock functions (Pet. 16–18), and would have looked to Schneier for background details regarding encryption key generation and management (*id.* at 18–19).

c. Patent Owner's Other Arguments Regarding the Combination

In addition to Patent Owner's direct responses to Petitioner's reasons for the proposed combination, Patent Owner argues there is no motivation for the combination for additional reasons as follows.

i. Cisco's Engineers Rejected the Proposed Combination

Patent Owner argues Exhibit 2015 reveals that Cisco's engineers rejected the concept of "hooking" Winsock to create a Winsock interceptor (shim) for a virtual private network product because such a solution was "tricky, complex, and error prone." PO Resp. 19. Petitioner replies that Exhibit 2015, consisting of notes of Cisco engineers in 2005, does not "relate in any way to the obviousness of the claims in 1997." Pet. Reply 3. Petitioner further argues there are a variety of reasons the Cisco engineers may have rejected the solution of "hooking" Winsock including, for example, business reasons based on the complexity of more Windows[®] operating system versions to support. *Id.* at 3–5.

We agree with Petitioner and, thus, we accord little weight to Exhibit 2015 as evidence of a lack of motivation to combine references at the time of the '011 patent filing.

ii. Takahashi Alone Nullifies Reasons to Combine

Patent Owner argues Petitioner identifies three deficiencies of Alden and proposes all three are alleviated by the combination with Takahashi but asserts, "if Takahashi alone provides the benefits that a POSITA would have allegedly sought, a POSITA would have simply implemented Takahashi—not a combination of Alden and Takahashi." PO Resp. 24. Petitioner

argues, and we agree, the proposed combination improves Alden by incorporating features of Takahashi, and contends Alden provides features not present in Takahashi including applications level encryption—a benefit Dr. Hamilton conceded in testimony. Pet. Reply 14 (citing Ex. 1034, 97:2–98:7). In particular, we observe Alden discloses the underlying virtual private network architecture recited as the contextual environment for all claims of the '011 patent.

iii. The Combination Changes the Principle of Operation of Alden

Patent Owner argues the proposed combination changes the principle of operation of Alden in that Alden encrypts *packets* whereas the proposed combination performs encryption before the data is packetized, thus, not encrypting *packets* themselves. PO Resp. 41. Patent Owner characterizes Alden's principle of operation as a pseudo adapter that encrypts packets as opposed to merely the data within a packet. *Id.* Patent Owner further argues that, based on this interpretation of Alden's principle of operation, Alden achieves numerous benefits that are lost in the proposed combination. *Id.* at 43–44 (citing Ex. 2011 ¶¶ 39–44, 99, 100).

Petitioner replies, *inter alia*, that Patent Owner improperly defines the principle of operation of Alden and, instead, argues Alden and Takahashi share the same basic principle of operation—namely “providing secure communications for users in a mobile environment using encryption.” Pet. Reply 22 (citing Ex. 1006, 1:7–22; Ex. 1007, 1). We agree with Petitioner's broader understanding of the shared principle of operation for Alden and Takahashi and find Patent Owner's characterization unduly narrow. Alden specifically recites its primary purpose as follows:

Thus there is required a new pseudo network adapter providing a virtual private network having a dynamically determined end point to support a user in a mobile computing environment. The new pseudo network adapter should appear to the communications protocol stack of the node as an interface to an actual physical device. The new pseudo network adapter should support guaranteed, in-order delivery of frames over a tunnel to conveniently support cipher block chaining mode or stream cipher encryption over multiple packets.

Ex. 1006, 2:58–67. Alden recites that the requisite guaranteed in-order delivery of packets is achieved by use of the TCP/IP protocol. *Id.* at 5:38–41. Furthermore, the benefits of encrypting packets alleged by Patent Owner are based on unsupported assertions in Dr. Hamilton’s testimony, and are neither disclosed nor claimed in Alden or the ’011 patent.

Thus, we determine the proposed combination of Alden and Takahashi does not alter the principle of operation of Alden, because the combined references are both directed to the same principle of operation—secure mobile communications.

d. Conclusion Regarding Motivation to Combine the References

Having considered the arguments of the parties and supporting evidence, for the above reasons, we are persuaded by a preponderance of the evidence that Petitioner has articulated reasons for the proposed combination based on rational underpinnings.

5. Secondary Considerations

Patent Owner argues “commercial acquiescence via licensing” must be considered as objective evidence of non-obviousness. PO Resp. 49 (citing *Ruiz v. A.B. Chance Co.*, 234 F.3d 654, 663 (Fed. Cir. 2000)). Patent

Owner asserts Citrix, a competitor of Petitioner, obtained a license to the '011 patent after unsuccessfully asserting invalidity of the '011 patent in litigation. *Id.* at 50. Patent Owner further asserts payment for the license “is tied to the merits of the '011 patent” because Citrix attempted, but failed, to invalidate the '011 patent in that litigation and was “undoubtedly aware that the Patent Office upheld the validity of the '011 patent during an *ex parte* reexamination.” *Id.*

Petitioner argues “commercial acquiescence” is found in only one Federal Circuit decision, and in earlier cases is considered equivalent to “industry acceptance” and “widespread adoption.” Pet. Reply 25 (citing *RCA Corp. v. Applied Digital Data Sys., Inc.*, 730 F.2d 1440 (Fed. Cir. 1984)). Petitioner contends “SSL’s single patent license does not indicate ‘industry acceptance’ or ‘widespread adoption,’ but rather merely satisfaction of a judgment.” *Id.*

Assuming, for the sake of argument, that there is a nexus between the Citrix license and the merits of the '011 patent, we find Patent Owner’s evidence of a single license agreement insufficient to demonstrate “commercial acquiescence” supporting non-obviousness. *Cf. RCA*, 730 F.2d at 1448 (“commercial acquiescence of competitors, evidenced by RCA’s *extensive licensing of the invention*”) (emphasis added). We are not persuaded that a single license to Citrix under the articulated circumstances can be considered “extensive licensing.”

For the above reasons, we are not persuaded that Patent Owner’s asserted secondary considerations comes remotely close to outweighing the above objective factors of obviousness.

D. Other Issues

1. Motions to Exclude

For the reasons discussed *supra*, we *deny* Petitioner’s Motion to Exclude Exhibits 2011 and 2012 (Dr. Hamilton’s declaration un-redacted and redacted, respectively). Petitioner’s arguments are properly directed to the weight of these Exhibits rather than to the admissibility thereof.

Patent Owner filed a Motion to Exclude (Paper 48). Patent Owner’s motion requested us to exclude Petitioner’s exhibits 1036–1039 and 1041–1064. We do not rely on any of these exhibits in our decision and, accordingly, Patent Owner’s Motion to Exclude is *dismissed* as moot.

2. “New Arguments”

Pursuant to our Order following a conference call (Paper 40), Patent Owner filed a paper listing arguments in Petitioner’s Reply that Patent Owner considered “new arguments” to be stricken from the record. Paper 41. In response, Petitioner filed a paper identifying where in the record all such alleged “new arguments” were presented. Paper 42. We are persuaded none of the alleged “new arguments” need be stricken from the record because Petitioner has persuasively identified where each such argument was previously presented in the record.

E. Conclusion

Petitioner has demonstrated, by a preponderance of the evidence, that claims 1–7 of the ’011 patent are unpatentable.

III. ORDERS

After due consideration of the record before us, and for the foregoing reasons, it is:

ORDERED that claims 1–7 of the '011 patent are held unpatentable;

FURTHER ORDERED that Patent Owner's Motion to Exclude is *dismissed*;

FURTHER ORDERED that Petitioner's Motion to Exclude is *denied*; and

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

IPR2015-01754
Patent 6,158,011

PETITIONER:

David L. McCombs
Theodore M. Foster
Pranay K. Pattani
Thomas King
HAYNES AND BOONE, LLP
david.mccombs.ipr@haynesboone.com
ipr.theo.foster@haynesboone.com
pranay.pattani.ipr@haynesboone.com
thomas.king@haynesboone.com

PATENT OWNER:

Richard Z. Zhang
David M. Saunders
Desmond Jui
FISCH SIGLER LLP
richard.zhang.ipr@fischllp.com
david.saunders@fischllp.com
desmond.jui@fischllp.com