

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

LIONRA TECHNOLOGIES LTD.,
Patent Owner.

IPR2024-00734
Patent 7,623,518 B2

Before ANNETTE R. REIMERS, STEVEN M. AMUNDSON, and
RUSSELL E. CASS, *Administrative Patent Judges*.

AMUNDSON, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

Cisco Systems, Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1, 3, 15, 17, and 19–21 in U.S. Patent No. 7,623,518 B2 (“the ’518 patent”) (Exhibit 1001) under 35 U.S.C. §§ 311–319. Paper 2 (“Pet.”). Lionra Technologies Ltd. (“Patent Owner”) did not file a Preliminary Response.

In the Institution Decision, we instituted review based on all challenged claims and all challenges included in the Petition. Paper 6 (“Inst. Dec.”).

We have jurisdiction under 35 U.S.C. § 6. We issue this Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons explained below, Petitioner has shown by a preponderance of the evidence that claims 1, 3, 15, 17, and 19–21 in the ’518 patent are unpatentable. *See* 35 U.S.C. § 316(e) (2024).

II. BACKGROUND

A. Procedural History

After we instituted review, Patent Owner filed a Response to the Petition. Paper 9 (“Resp.”). Petitioner filed a Reply to Patent Owner’s Response. Paper 13 (“Reply”). Patent Owner filed a Sur-reply to Petitioner’s Reply. Paper 18 (“Sur-reply”).

In July 2025, we held an oral hearing. The record includes the hearing transcript. Paper 24 (“Tr.”).

B. Real Parties in Interest

Petitioner identifies itself as the sole real party in interest. Pet. 88. Patent Owner identifies itself as the sole real party in interest. Paper 5, 2. The parties do not raise any issue about real parties in interest.

C. Related Matters

Petitioner and Patent Owner identify the following civil actions as related matters involving the '518 patent:

- *Lionra Technologies Ltd. v. Fortinet, Inc.*, No. 2:23-cv-00206 (E.D. Tex. filed May 9, 2023);
- *Lionra Technologies Ltd. v. Cisco Systems, Inc.*, No. 2:23-cv-00207 (E.D. Tex. filed May 9, 2023) (the “Texas case”);
- *Lionra Technologies Ltd. v. Palo Alto Networks, Inc.*, No. 2:23-cv-00214 (E.D. Tex. filed May 11, 2023);
- *Lionra Technologies Ltd. v. CrowdStrike Holdings, Inc. et al.*, No. 1:23-cv-00928 (W.D. Tex. filed Aug. 7, 2023); and
- *Lionra Technologies Ltd. v. VMware, Inc.*, No. 1:23-cv-00929 (W.D. Tex. filed Aug. 7, 2023).

Pet. 88; Paper 5, 2.

D. The '518 Patent (Exhibit 1001)

The '518 patent, titled “Dynamic Access Control Lists,” issued on November 24, 2009, from an application filed on April 8, 2004. Ex. 1001, codes (22), (45), (54). The patent explains that in “an Ethernet local area network (LAN), computers or hosts are attached to the network and each host is uniquely identified by a physical address which is designated a media access control (MAC) address in an Ethernet network.” *Id.* at 1:5–8. The patent also explains that domain name system (DNS) servers “contained in the Internet convert the domain name into a corresponding IP address which

allows a host to communicate with a desired host corresponding to that IP address.”¹ *Id.* at 2:61–64.

The ’518 patent identifies “a need for access control lists that allows [sic] access of hosts in a computer network such as an Ethernet network to be restricted or controlled based upon user names, MAC addresses, domain names, and DNS names instead of merely IP address information.”

Ex. 1001, 3:12–16. The patent endeavors to address that need by providing a method for controlling a user’s access to a network that includes:

- (1) storing in a network switch “an enhanced access control list containing data related to at least one of user names, DNS names, domain names, and physical addresses”; and
- (2) generating a dynamic access control list from “the enhanced access control list, with the dynamic access control list containing a plurality of IP addresses that restrict access of the user to the network.”

Id. at 3:20–30, code (57).

¹ The acronym “IP” stands for “Internet Protocol.” *See, e.g.*, Ex. 1001, 1:30; Ex. 1013, 2:45.

The '518 patent's Figure 1 (reproduced below) depicts an Ethernet network with an Ethernet switch:

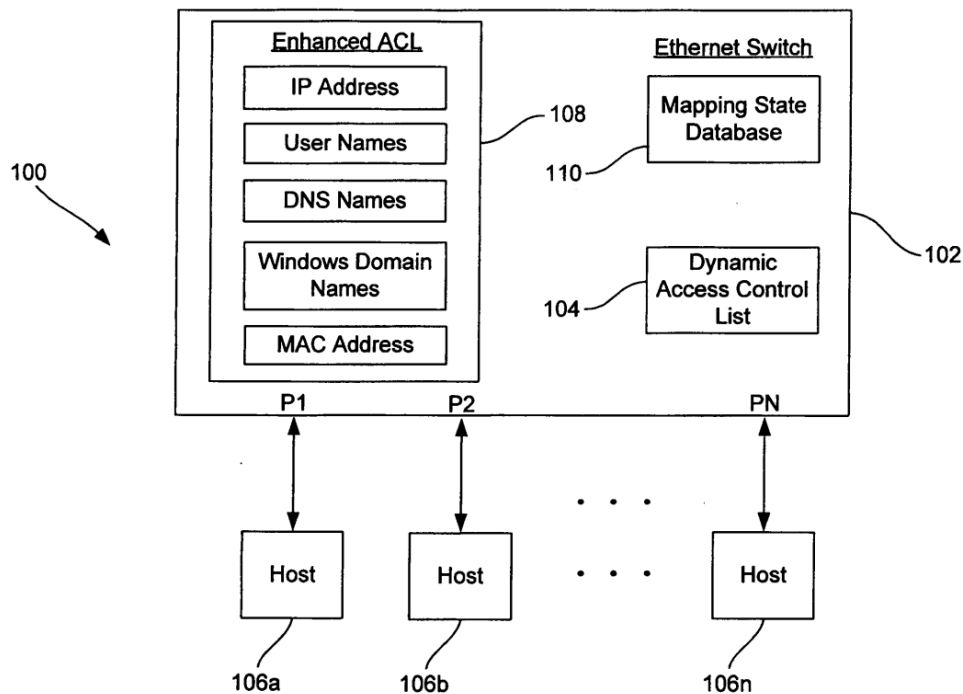


FIG. 1

Figure 1 illustrates Ethernet network 100 with Ethernet switch 102 connected through ports P1–PN to hosts 106a–106n. Ex. 1001, 3:49–53, 4:44–46, Fig. 1.

As Figure 1 shows, Ethernet switch 102 includes the following:

- (1) dynamic access control list 104 “containing IP addresses currently being utilized by various users of the network 100”;
- (2) enhanced access control list 108 “containing IP address, user name, DNS name, Windows domain name, and MAC address information” for the users and hosts 106a–106n of the network 100; and
- (3) mapping state database 110 storing records that associate “the user name with the MAC address of” the specific host 106a–106n that “the user is currently using to access the network 100.”

Ex. 1001, 3:53–55, 3:57–62, 4:61–5:3, Fig. 1.

Ethernet switch 102 “detects all dynamic host configuration protocol (DHCP) packets sent by any of the hosts” to a DHCP server. Ex. 1001, 5:4–6. A DHCP packet includes the source MAC address of the host sending the packet to the DHCP server and, therefore, identifies the host requesting the IP address from the DHCP server. *Id.* at 5:9–12. Ethernet switch 102 “then monitors the return DHCP packets from the DHCP server sent in response to the DHCP packets, and from these return DHCP packets determines the IP address assigned to” the host requesting the IP address from the DHCP server. *Id.* at 5:12–16. “At this point, the switch knows the IP address assigned to a particular MAC address.” *Id.* at 5:16–17.

The ’518 patent’s Figure 2 (reproduced below) is a functional flow diagram depicting the process executed by Ethernet switch 102 in generating a dynamic access control list:

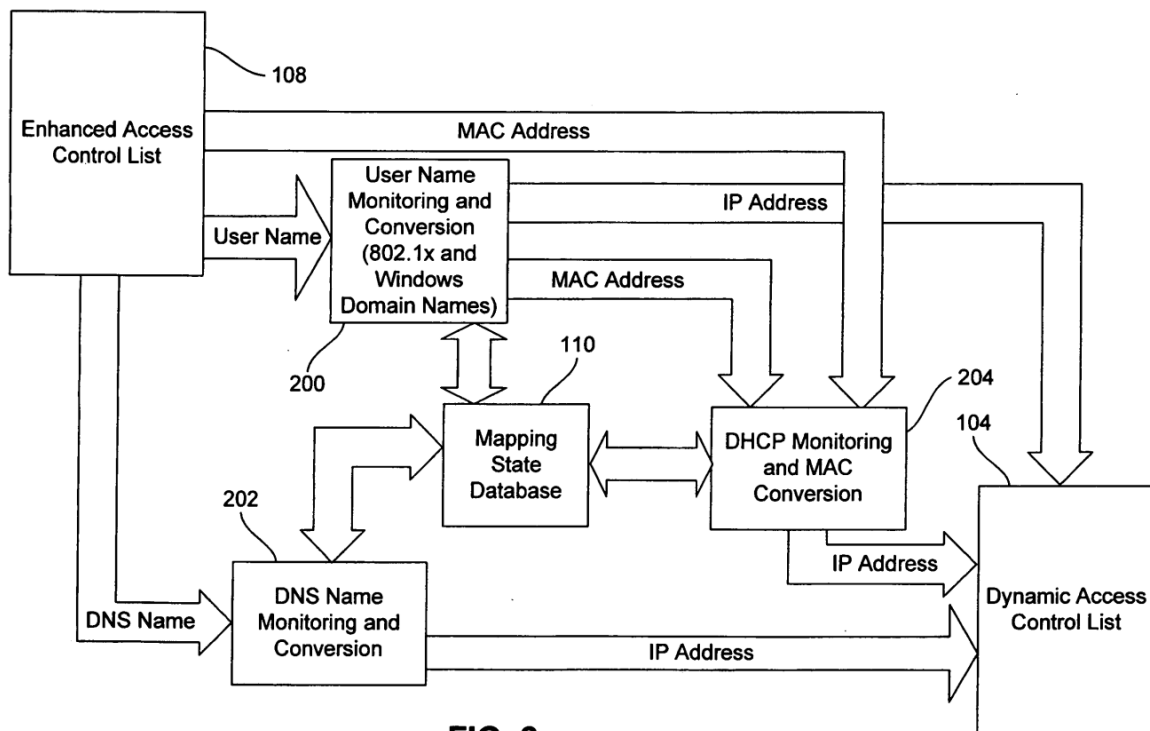


FIG. 2

Figure 2 illustrates dynamic access control list 104, enhanced access control list 108, and mapping state database 110 along with three subprocesses as follows:

- (1) “a user name monitoring and conversion subprocess 200”;
- (2) “a DNS name monitoring and conversion subprocess 202”; and
- (3) “a DHCP monitoring and MAC conversion subprocess 204.”

Ex. 1001, 5:56–66, Fig. 2. These “subprocesses operate in combination to apply the rules contained in the enhanced access control list 108 to generate” dynamic access control list 104 and mapping state database 110. *Id.* at 5:67–6:3.

Subprocess 200 “converts user names into either MAC or IP addresses depending upon the manner in which a user is attempting to log into the network 100.” Ex. 1001, 6:4–7. Subprocess 202 “detects all Ethernet packets being communicated through the switch 102 (FIG. 1) having a source IP address which does not yet exist in the mapping state database 110.” *Id.* at 7:10–13. When subprocess 202 “detects an unknown source IP address, the subprocess generates a reverse DNS lookup query containing the source IP address, and sends this query to a DNS server.” *Id.* at 7:24–27. Subprocess 204 “monitors DHCP return packets from a DHCP server, which corresponds to one of the hosts 106 (FIG. 1), and from these return packets determines the IP address assigned by the DHCP server to a given MAC address.” *Id.* at 7:54–58.

The '518 patent's Figure 3 (reproduced below) depicts Ethernet switch 102 in more detail:

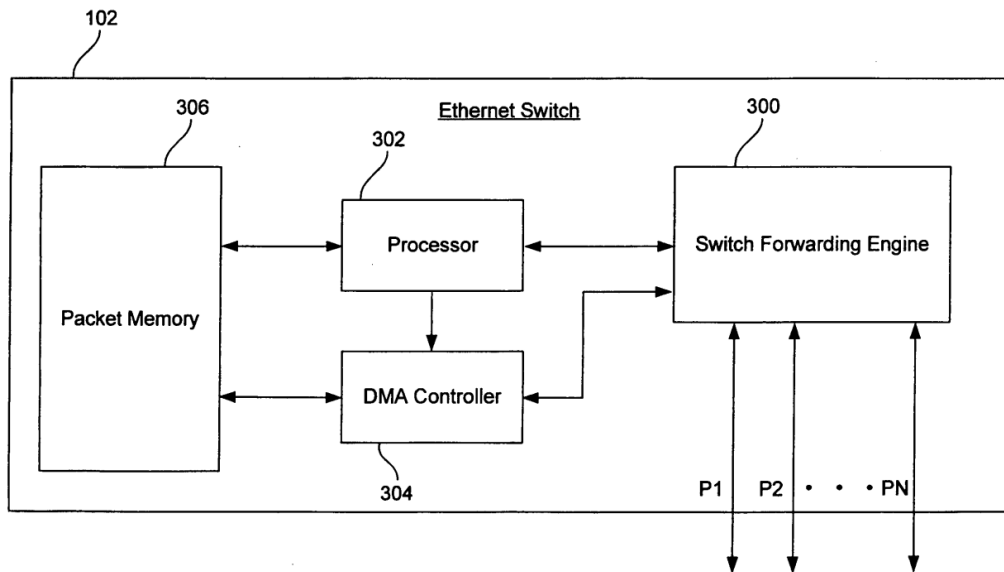


FIG. 3

Figure 3 illustrates Ethernet switch 102 including the following components:

- (1) switch forwarding engine 300 that “examines Ethernet packets received on one of a plurality of ports P1–PN from a host (not shown) coupled to each port and forwards each received Ethernet packet to the proper host through the corresponding port”;
- (2) processor 302 that “programs the switch forwarding engine 300 to execute a desired set of rules to provide selected Ethernet packets received by the forwarding engine to the processor”; and
- (3) direct memory access (DMA) controller 304 that
 - (i) “transfers the packets selected by the switch forwarding engine 300 to a packet memory 306” and
 - (ii) reads “packets from the packet memory 306” so that “the switch forwarding engine 300” may forward “the packets to the required destination host.”

Ex. 1001, 9:9–19, 9:28–30, 9:51–55, Fig. 3.

E. The Challenged Claims

The '518 patent includes 22 claims. Ex. 1001, 10:12–12:61.

Petitioner challenges the following claims:

- independent claim 1 for a “method of developing an access control list”;
- claim 3 that depends directly from claim 1;
- independent claim 15 for a “network switching circuit”;
- claim 17 that depends directly from claim 15;
- independent claim 19 for a “computer network”; and
- claims 20 and 21 that depend directly from claim 19.

Pet. 9–85.

Claims 1, 15, and 19 exemplify the challenged claims and read as follows (with formatting added for clarity and with bracketed numbers added for reference purposes):²

1. [1.0] A method of developing an access control list, comprising:

[1.1] developing an enhanced access control list including data related to at least one of user names, DNS names, Windows domain names, and physical addresses;

[1.2.1] converting, in a network switch, at least one of:

[1.2.2] user names into corresponding IP and physical addresses according to data in the enhanced access control list, wherein converting user names into corresponding IP and physical addresses according to data in the enhanced access control list includes:

detecting login packets being communicated over the network;

² We use the same reference numbers that Petitioner uses to identify the claim language. *See* Pet. 22–42, 48–83.

determining a MAC address from the login packets;

detecting server message block login packets being communicated over the network;

determining an IP address from the server message block login packets; and

developing records in the access control list using the obtained IP address for the respective user name;

[1.2.3] DNS names into corresponding IP addresses according to data in the enhanced access control list; and

[1.2.4] physical addresses into IP addresses according to data in the enhanced access control list; and

[1.3] developing, in the network switch, the access control list from each of the operations of converting.

15. [15.0] A network switching circuit, comprising:

[15.1.1] a forwarding circuit operable to detect specific received packets and [15.1.2] to provide the specific packets on a processor port, and [15.1.3] further operable to receive packets on one of a plurality of ports including the processor port and [15.1.4] to forward each received packet to a port corresponding to a destination address contained in the packet [15.1.5] subject to access restrictions contained in a dynamic access control list;

[15.2.1] a memory circuit coupled to the forwarding circuit,

[15.2.2] the memory circuit operable to store packets and [15.2.3] operable to store an enhanced access control list and [15.2.4] a dynamic access control list; and

[15.3.1] a processor coupled to the forwarding circuit and to the memory circuit,

[15.3.2] the processor operable to define the specific packets detected by the forwarding circuit and

[15.3.3] operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and [15.3.4] store the dynamic access control list in the memory circuit, and [15.3.5] further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets.

19. [19.0] A computer network, comprising:

[19.1.1] a network switch, including,

[19.1.2] a forwarding circuit operable to detect specific received packets and [19.1.3] to provide the specific packets on a processor port, and [19.1.4] further operable to receive packets on one of a plurality of ports including the processor port and [19.1.5] to forward each received packet to a port corresponding to a destination address contained in the packet [19.1.6] subject to access restrictions contained in a dynamic access control list;

[19.2.1] a memory circuit coupled to the forwarding circuit,

[19.2.2] the memory circuit operable to store packets and [19.2.3] operable to store an enhanced access control list and [19.2.4] a dynamic access control list; and

[19.3.1] a processor coupled to the forwarding circuit and to the memory circuit,

[19.3.2] the processor operable to define the specific packets detected by the forwarding circuit and [19.3.3] operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and [19.3.4] store the dynamic access control list in the memory circuit, and [19.3.5] further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets; and

[19.4] a plurality of hosts, each host coupled to a respective port of the network switch.

Ex. 1001, 10:12–37, 11:57–12:17, 12:27–52.

F. The Asserted References

For its challenges, Petitioner relies on the following references:

Name	Reference	Exhibit
Gai	US 6,651,096 B1, issued November 18, 2003 (based on an application filed April 20, 1999)	1006
Kwan	US 7,523,485 B1, issued April 21, 2009 (based on an application filed July 31, 2003)	1007
Georgiou	US 7,003,597 B2, issued February 21, 2006 (based on an application filed July 9, 2003)	1008
Yip	US 8,751,647 B1, issued June 10, 2014 (based on an application filed June 30, 2001)	1013

Pet. 9–85.

Petitioner asserts that Gai, Kwan, Georgiou, and Yip qualify as prior art “under Pre-AIA 35 U.S.C. §§ 102(a) and 102(e).” Pet. 9–10; *see* 35 U.S.C. § 102(a), (e) (2006).³ Patent Owner does not dispute that Gai, Kwan, Georgiou, and Yip qualify as prior art. *See* Resp. 6–33; Sur-reply 2–19.

G. The Asserted Challenges to Patentability

Petitioner asserts the following challenges to patentability:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 3	103(a)	Gai, Yip, Kwan

³ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. § 102 and § 103 effective March 16, 2013. Because the effective filing date of the challenged claims predates the AIA’s amendments to § 102 and § 103, this decision refers to the pre-AIA versions of § 102 and § 103.

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
15, 17, 19–21	103(a)	Gai, Yip, Kwan, Georgiou

Pet. 9–85.

H. Testimonial Evidence

To support its challenges, Petitioner relies on (1) the Declaration of Dr. Mark E. Crovella (Exhibit 1003) submitted with the Petition and (2) the Second Declaration of Mark E. Crovella, Ph.D. (Exhibit 1023) submitted with the Reply. Dr. Crovella states that he has been “asked to provide [his] opinions regarding whether the subject matter of claims 1, 3, 15, 17, and 19–21” in the ’518 patent “would have been obvious to a person having ordinary skill in the art” at “the time of the alleged invention, in light of the prior art.” Ex. 1003 ¶ 3. Dr. Crovella also states that he (1) “earned an undergraduate degree in Biology from Cornell University” in 1982, (2) “received a master’s degree in Computer Science from the University of Buffalo in 1989,” and (3) “received a Ph.D. in Computer Science from the University of Rochester in 1994.” *Id.* ¶ 8.

To support its positions, Patent Owner relies on the Declaration of Dr. Eric Cole (Exhibit 2001) submitted with the Response. Dr. Cole states that Patent Owner “has retained [him] as an independent expert in connection with IPR2024-00734 to provide testimony regarding the technology involved in” the ’518 patent. Ex. 2001 ¶ 1. Dr. Cole also states that his “academic credentials include a master’s degree in computer science and a doctorate in information security” and that he has “worked in the cyber and technical information security industry for over twenty-five years.” *Id.* ¶ 4.

Additionally, Petitioner submits Dr. Cole’s deposition testimony. *See* Ex. 1021 (Apr. 3, 2025, Cole Dep. Tr.).

I. Burden

In an *inter partes* review, a petitioner bears the burden of persuasion to prove “unpatentability by a preponderance of the evidence.” *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (quoting 35 U.S.C. § 316(e)); *see* 37 C.F.R. § 42.1(d) (2025).

III. PATENTABILITY ANALYSIS

A. Legal Principles: Obviousness

A patent may not be obtained “if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” 35 U.S.C. § 103(a) (2006). An obviousness analysis involves underlying factual inquiries including (1) the scope and content of the prior art; (2) differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) where in evidence, objective indicia of nonobviousness, such as commercial success, long-felt but unsolved needs, and failure of others. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18, 35–36 (1966); *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1047–48 (Fed. Cir. 2016) (en banc). When evaluating a combination of references, an obviousness analysis should address “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007).

We analyze the obviousness issues according to these principles.

B. Level of Ordinary Skill in the Art

Factors pertinent to determining the level of ordinary skill in the art include (1) the educational level of the inventor; (2) the type of problems encountered in the art; (3) prior-art solutions to those problems; (4) the rapidity with which innovations are made; (5) the sophistication of the technology; and (6) the educational level of workers active in the field. *Envtl. Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696–97 (Fed. Cir. 1983). Not all factors may exist in every case, and one or more of these or other factors may predominate in a particular case. *Id.* These factors are not exhaustive, but merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007). Moreover, the prior art itself may reflect an appropriate skill level. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Petitioner asserts that a person of ordinary skill in the art at the time of the alleged invention “would have been someone”:

- (1) “knowledgeable with the computer networking techniques available at the time”; and
- (2) “who had a bachelor’s degree in computer science, computer engineering, electrical engineering, or an equivalent, and two years of experience working with computer networks, including network security.”

Pet. 7. Petitioner also asserts that “[l]ack of work experience can be remedied by additional education, and vice versa.” *Id.* Dr. Crovella’s testimony supports Petitioner’s assertions. *See* Ex. 1003 ¶¶ 15–16.

Patent Owner asserts that a person of ordinary skill in the art would have had “a Bachelor’s degree in computer science, computer engineering, electrical engineering or equivalent and at least two years of experience in

computer networking and network system security.” Resp. 5–6. Patent Owner also asserts that “[a]dditional education in the field could be substituted for industry experience, and vice versa.” *Id.* at 6. Dr. Cole’s testimony supports Patent Owner’s assertions. *See* Ex. 2001 ¶¶ 28–29.

Regarding an ordinarily skilled artisan’s education, the parties agree on the level of education (“bachelor’s degree”) and the field of study (“computer science, computer engineering, electrical engineering, or an equivalent”). Pet. 7; Resp. 5–6. Regarding an ordinarily skilled artisan’s experience, the parties generally agree on the area of experience, but Patent Owner’s description allows for more experience (“**at least** two years”) than Petitioner’s description (“two years”). Pet. 7; Resp. 5–6.

We adopt Petitioner’s description of an ordinarily skilled artisan because it comports with the technology and claims in the ’518 patent as well as the asserted references. *See, e.g.*, Ex. 1001, 1:5–3:30, 10:12–12:61; *infra* §§ III.D.1–III.D.3, III.E.1. We note that our analysis would not change if we adopted Patent Owner’s description of an ordinarily skilled artisan, which allows for more experience (“**at least** two years”) than Petitioner’s description (“two years”). *See* Pet. 7; Resp. 5–6. Someone with a higher skill level will understand the technology at least as well as someone with a lower skill level. *See Innovention Toys, LLC v. MGA Ent., Inc.*, 637 F.3d 1314, 1323 (Fed. Cir. 2011); *Tokai Corp. v. Easton Enters., Inc.*, 632 F.3d 1358, 1369 (Fed. Cir. 2011). Hence, “it is generally easier to establish obviousness under a higher level of ordinary skill.” *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1366 (Fed. Cir. 2012).

C. Claim Construction

1. GENERAL PRINCIPLES

We construe claim terms “using the same claim construction standard” that district courts use to construe claim terms in civil actions for patent infringement. *See* 37 C.F.R. § 42.100(b). Under that standard, claim terms “are given their ordinary and customary meaning, which is the meaning the term would have to a person of ordinary skill in the art at the time of the invention.” *Power Integrations, Inc. v. Fairchild Semiconductor Int’l, Inc.*, 904 F.3d 965, 971 (Fed. Cir. 2018) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc)). The meaning of claim terms may be determined by “look[ing] principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

2. PETITIONER’S PROPOSED CONSTRUCTION OF THE PHRASE “AT LEAST ONE OF” IN CLAIM 1

For the phrase “at least one of” in limitations 1.1 and 1.2.1, Petitioner contends that in the Texas case Patent Owner interpreted that phrase as requiring “only one of the listed items,” e.g., “only one” of “user names, DNS names, Windows domain names, and physical addresses” as recited in limitation 1.1. Pet. 8; *see* Ex. 1001, 10:14–16. Here, Petitioner “applies Patent Owner’s apparent district court interpretation of the claim term ‘at least one of’” in claim 1. Pet. 8; *see id.* at 25, 33–34, 39. Further, because the phrase “each of” in limitation 1.2.1 “relates back to the ‘at least one of’ converting operations” in limitation 1.1, Petitioner “applies Patent Owner’s

apparent district court interpretation to mean developing from the at least one of the listed items of converting.” *Id.* at 8 (emphasis omitted); *see id.* at 39.

Petitioner does not propose an explicit construction for any other claim term or phrase. *See, e.g.*, Pet. 7–85; Reply 5–26.

3. PATENT OWNER’S POSITION

Patent Owner does not propose an explicit construction for any claim term or phrase. *See, e.g.*, Resp. 5–26; Sur-reply 2–19.

4. DISCUSSION

“[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.” *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999); *see Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). We determine that no term or phrase in a challenged claim requires an explicit construction to decide whether Petitioner has shown by a preponderance of the evidence that the challenged claims are unpatentable under § 103(a).

In the patentability analysis below, however, we address a claim-construction issue raised with respect to limitations 15.2.1 and 19.2.1 reciting “a memory circuit coupled to the forwarding circuit,” i.e., whether the language “a memory circuit” encompasses multiple components. *See infra* § III.E.3(c)(iii). We address this issue in the patentability analysis below to provide better context to explain the issue and our resolution of the issue.

D. Alleged Obviousness over Gai, Yip, and Kwan: Claims 1 and 3

Petitioner contends that claims 1 and 3 are unpatentable under § 103(a) because the claims would have been obvious over Gai, Yip, and Kwan. *See* Pet. 10–42; Reply 5–19. Patent Owner disputes Petitioner’s contentions. *See* Resp. 6–20; Sur-reply 2–13.

Below, we provide overviews of Gai, Yip, and Kwan. Then, we consider the obviousness issues. For the reasons explained below, we agree with Petitioner that claims 1 and 3 are unpatentable under § 103(a) because the claims would have been obvious over Gai, Yip, and Kwan.

1. OVERVIEW OF GAI (EXHIBIT 1006)

Gai is a U.S. patent titled “Method and Apparatus for Organizing, Storing and Evaluating Access Control Lists,” filed on April 20, 1999, and issued on November 18, 2003. Ex. 1006, codes (12), (22), (45), (54). Gai states that the invention “relates generally to computer networks, and more specifically, to a method and apparatus for manipulating access control lists in order to optimize their evaluation by computer network devices.” *Id.* at 1:15–18; *see id.* at code (57).

Gai explains that certain devices on a network employ access control lists (ACLs) to provide security by determining whether “messages should be forwarded or filtered (i.e., dropped) based on certain predefined criteria,” such as “IP source address, IP destination address, or upper-layer application based on TCP/UDP port numbers.”⁴ Ex. 1006, 2:46–51, 3:17. “Access

⁴ The acronym “TCP” stands for “Transmission Control Protocol.” *See, e.g.*, Ex. 1006, 21:24–25; Ex. 1011, 20:63–64; Ex. 1022, 11. The acronym “UDP” stands for “User Datagram Protocol.” *See, e.g.*, Ex. 1006, 21:24–25; Ex. 1022, 11.

control lists may be established for both inbound and outbound traffic and are most commonly configured at border devices (i.e., gateways or firewalls) to provide security to the network.” *Id.* at 2:53–57.

Gai identifies a need to “optimize the creation and evaluation of multiple access control lists so as to maintain, if not improve, packet processing speeds.” Ex. 1006, 3:34–36. Gai endeavors to address that need by providing “a method and apparatus for efficiently organizing, storing and evaluating access control lists” for “use by an intermediate network device of a computer network.” *Id.* at 3:55–57, code (57).

Gai describes “intermediate network devices” as including the following:

- (1) bridges “used to provide a ‘bridging’ function between two or more LANs”;
- (2) switches “utilized to provide a ‘switching’ function for transferring information, such as data frames or packets, among entities of a computer network” that “may operate at layer 2 which, in the OSI Reference Model, is called the data link layer and includes the Logical Link Control (LLC) and Media Access Control (MAC) sub-layers”;⁵ and
- (3) routers “often used to interconnect dissimilar subnetworks” that (a) “may operate at higher communication layers, such as layer 3, which in TCP/IP networks corresponds to the Internet Protocol (IP) layer,” and (b) “may also examine the transport layer headers of received messages to identify the corresponding TCP or UDP port numbers being utilized by the corresponding network entities.”

⁵ The acronym “OSI” stands for “Open Systems Interconnection.” *See, e.g.*, Ex. 1006, 1:31–32; Ex. 2001 ¶ 51.

Ex. 1006, 1:59–2:22; *see id.* at 5:35–44.

Gai explains that an “intermediate network device includes an ACL converter which, in turn, includes a boolean transformation engine that is operatively coupled to a boolean manipulation engine.” Ex. 1006, code (57). The “boolean transformation engine is configured to access the ACLs in [a] first format and to translate them into a first boolean representation, such as binary decision diagram (BDD) format.” *Id.* The “boolean manipulation engine is configured to perform one or more operations on the ACLs specified for a given interface, including a merge operation, so as to generate a single, unified ACL for the given interface.” *Id.*

With “a single, unified ACL defined per interface per direction” stored in a content addressable memory (CAM), the “intermediate network device is able to rapidly evaluate network messages.” Ex. 1006, 4:26–29. In particular, “upon receipt of a packet at a first interface, a forwarding entity at the intermediate network device tests the packet against the single, unified ACL stored in the corresponding portion of the CAM.” *Id.* at 4:29–32. “When a match is obtained, the corresponding decision is returned to the forwarding entity, which then takes the appropriate action (e.g., forward, discard, log and forward, transfer to CPU for additional processing, etc.).” *Id.* at 4:32–36; *see id.* at 17:26–48.

Gai's Figure 3 (reproduced below) depicts a computer network:

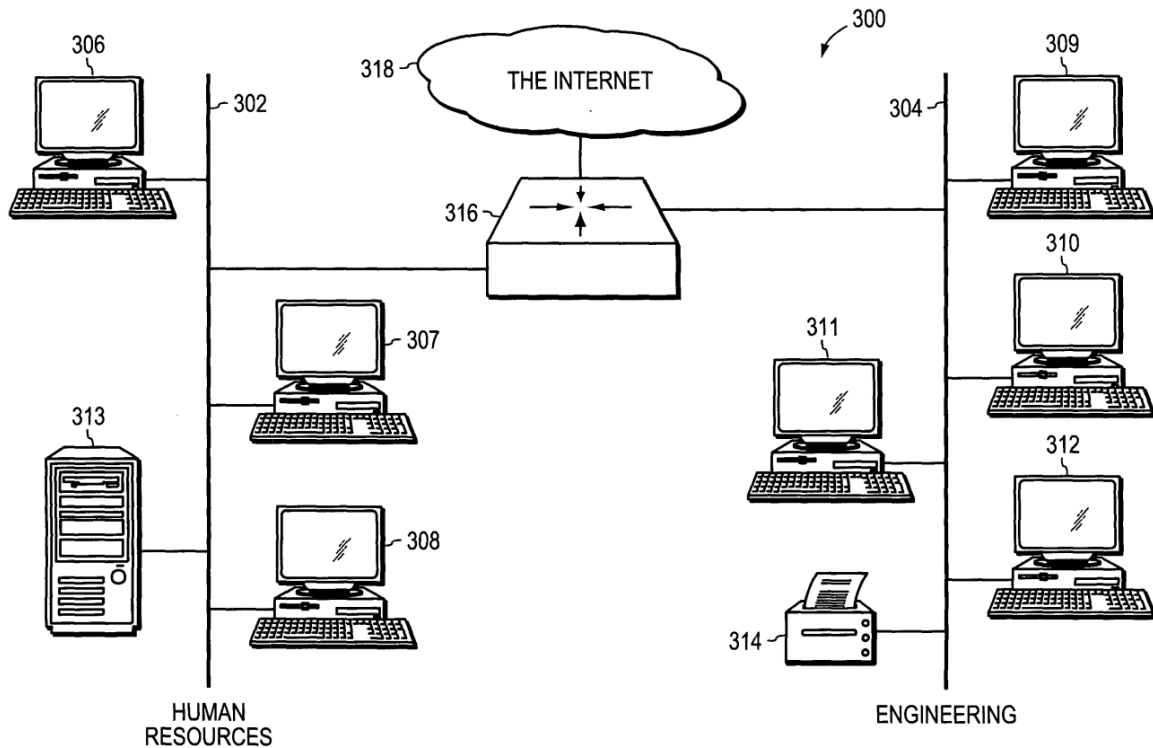


FIG. 3

Figure 3 illustrates computer network 300 including LAN 302, LAN 304, end stations 306–312, server 313, server 314, and intermediate network device 316 connected via the Internet 318. Ex. 1006, 5:3–14, Fig. 3.

Network device 316 may include “transmitting and receiving circuitry and components” and “may also implement network services such as route processing, path determination and path switching functions.” *Id.* at 5:27–32.

Gai's Figure 4 (reproduced below) depicts intermediate network device 316 in more detail:

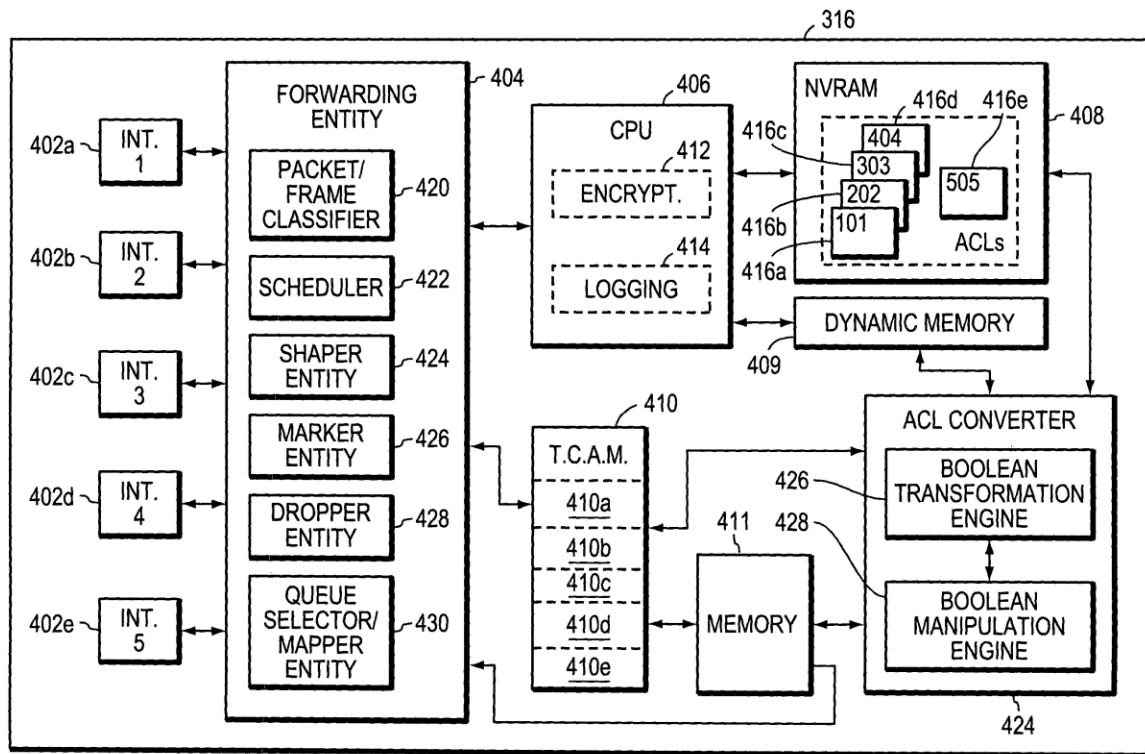


FIG. 4

Figure 4 illustrates intermediate network device 316 including the following components:

- a plurality of interfaces 402a–402e “associated with one or more physical ports (not shown)”;
- forwarding entity 404;
- central processing unit (CPU) 406;
- non-volatile random access memory (NVRAM) 408, e.g., for storing text-based ACLs 416a–416e;
- dynamic memory 409;
- content addressable memory 410, preferably “a ternary content addressable memory (TCAM),” apportioned into segments 410a–410e where each of segments 410a–410e corresponds to a particular interface 402a–402e;

- memory 411 coupled to TCAM 410, preferably including “a plurality of spaces or locations, such that each entry or row of the TCAM 410 has a corresponding location or space in memory 411”; and
- ACL converter 424 with boolean transformation engine 426 and boolean manipulation engine 428 “arranged in communicating relationship by communications means.”

Ex. 1006, 4:52–54, 5:60–6:18, 6:36–51, Fig. 4.

ACL converter 424 “transforms the text-based ACLs” into corresponding BDD representations and “then merges all of the ACLs assigned to each interface into a single, unified ACL.” Ex. 1006, 9:25–29. ACL converter 424 “stores these single, unified ACLs in the TCAM 410 for subsequent use by the forwarding entity 404.” *Id.* at 9:29–31. “The final or merged actions to be implemented by a given forwarding entity may include permit, deny, forward to CPU for additional processing (e.g., encryption, logging, etc.), forward to an alternative forwarding entity, etc.” *Id.* at 13:41–45; *see id.* at 17:44–48.

“ACL converter 424, including boolean transformation engine 426 and boolean manipulation engine 428, may run on or otherwise be executed by CPU 406 or some other processing element (not shown).” Ex. 1006, 6:52–55.

Gai explains that “[p]referably, intermediate network device 316 is a layer 3 intermediate device and thus operates up to the network layer of the communication protocol stack implemented within the network 300.” Ex. 1006, 5:22–25. But Gai further explains that “the present invention may also be utilized in whole or in part with other intermediate network devices, such as switches and/or layer 2 intermediate devices, which are also

intended to broadly cover any intermediate device operating primarily at the data link layer.” *Id.* at 5:44–49.

According to Gai, a “suitable platform for intermediate network device 316 are the Catalyst 8500® series of switch routers and/or the Catalyst® 6000 family of multi layer [sic] switches both from Cisco Systems, Inc.” Ex. 1006, 6:62–65.

2. OVERVIEW OF YIP (EXHIBIT 1013)

Yip is a U.S. patent titled “Method and Apparatus for Network Login Authorization,” filed on June 30, 2001, and issued on June 10, 2014. Ex. 1013, codes (12), (22), (45), (54). Yip states that the invention “relates to the field of network security.” *Id.* at 1:6–7; *see id.* at code (57).

Yip explains that previous “network security techniques have been implemented at a connection point (i.e. at the LAN switch level) to prevent intruder and hacker attacks.” Ex. 1013, 2:33–35. For instance, techniques “have been designed and implemented in LAN switches to prohibit cyber-attacks, such as access control lists (ACLs).” *Id.* at 2:35–38. Yip also explains that ACLs “were developed to combat cyber-attacks on the LAN switch by providing an administrator-controlled list of Internet Protocol (IP) addresses or media access control (MAC) addresses that were authorized to access the network.” *Id.* at 2:43–47; *see id.* at 6:23–27.

Yip endeavors to improve network security by providing a method to “control the admission of a user to a network by preventing a port through which the user connects to the network from forwarding data packets until the user is authorized.” Ex. 1013, 3:39–43, code (57). According to that method, a “network login controller operates in conjunction with”:

- (1) “a user interface to receive a user identification data from the port user”; and
- (2) “an authorization server to authenticate the user by sending a user authentication request containing the user identification data to the authentication server.”

Id. at 3:43–48, code (57).

Based on “the user authentication response from the authentication server,” the “network login controller grants or denies permission to the user to access the network.” Ex. 1013, 3:48–51, code (57). “If permission is granted, then the network login controller unblocks the port through which the user is connected to place it in packet-forwarding mode.” *Id.* at 3:51–54, code (57). “If permission is denied, then the port remains in packet non-forwarding mode (i.e. it remains blocked).” *Id.* at 3:54–56, code (57).

In a preferred embodiment, a packet-forwarding device includes a user interface, e.g., a web browser, and a network login controller, e.g., a web server. Ex. 1013, 5:51–56, Fig. 1. The user interface accepts user identification data from a user and then sends the user identification data to the network login controller. *Id.* at 5:54–56. Next, the network login controller transmits a user authentication request containing the user identification data to a user authentication server. *Id.* at 7:19–24. After receiving the user authentication request, the user authentication server retrieves user authentication data from a user authentication database. *Id.* at 7:24–26. Then, the user authentication server compares the user authentication data from the user authentication database to the user identification data provided in the user authentication request to determine whether to place the port in packet-forwarding mode. *Id.* at 7:24–37.

3. OVERVIEW OF KWAN (EXHIBIT 1007)

Kwan is a U.S. patent titled “System and Method for Source IP Anti-Spoofing Security,” filed on July 31, 2003, and issued on April 21, 2009. Ex. 1007, codes (12), (22), (45), (54). Kwan states that the invention relates to “a method of providing for enhanced security on a computer network to reduce the risk created by the spoofing of IP addresses.” *Id.* at 1:15–17; *see id.* at code (57). Kwan explains that “source IP Address spoofing is a common technique used in denial of service attacks (DoS)” and that other types of “source IP address spoofing attacks are widely known, and include attacks such as distributed denial of service attacks (DDoS), Worm attacks, and Man In the Middle attacks.” *Id.* at 1:21–26.

Kwan explains that “MAC addresses are used to identify the devices” connected to a network because “a MAC address is a unique address” corresponding to “a device connected to a network.” Ex. 1007, 1:38–41. A data packet transmitted over the network includes “the MAC address for the device to which the data packet is to be sent (the destination MAC address) and the MAC address for the host which is sending the packet (the source MAC address).” *Id.* at 1:55–61; *see id.* at 3:63–66.

Additionally, each host device, such as an end-user computer or a server, “will be assigned an IP address” used “to determine routing for data packets” transmitted over the network. Ex. 1007, 1:61–66; *see id.* at 3:66–67. “The IP address is often assigned using the Dynamic Host Configuration Protocol (DHCP).” *Id.* at 1:66–2:1. A data packet includes “a source IP address and a destination IP address” as well as the source MAC address and the destination MAC address. *Id.* at 2:2–7.

Kwan explains that source IP address spoofing “occurs when an attacker host uses a source IP address, which does not correspond, or is not assigned, to its MAC address, in a transmitted data packet.” Ex. 1007, 2:8–10. To thwart source IP address spoofing, Kwan provides a system and method for (1) “analyzing MAC addresses and source IP addresses at the datalink (layer 2) level” and (2) using “the information derived from such analysis to block access through a port where a host device is using a false, or spoofed, source IP address in transmitted data packets.” *Id.* at code (57).

Kwan’s Figure 2 (reproduced below) depicts a network device providing layer 2 switching functions:

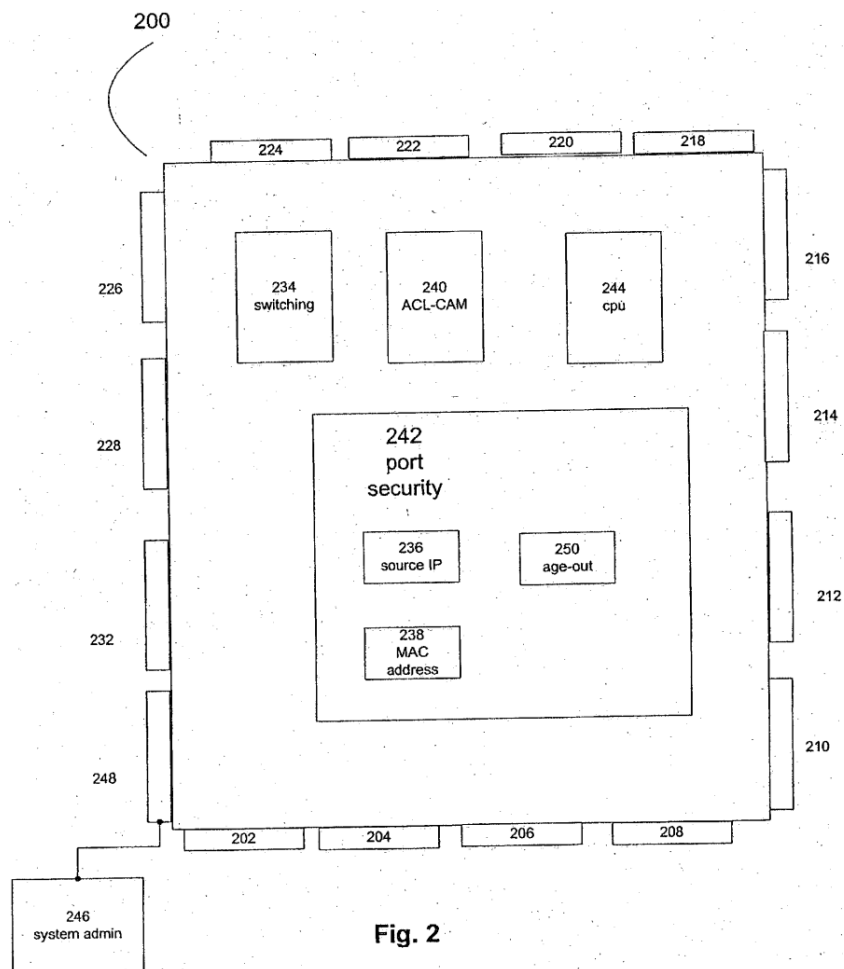


Fig. 2

Figure 2 illustrates network device 200 including the following components:

- a plurality of ports 202–232;
- network device switching 234;
- content addressable memory 240 containing a table that stores IP address-MAC address pairs “embodied as an access control list, which are data fields,” and shown as ACL-CAM 240;
- port security processor 242 with source IP address detector 236, MAC address detector 238, and source IP age-out timer 250;
- central processing unit (CPU) 244; and
- secure port 248 for receiving information from and sending information to “a system administrator’s computer 246.”

Ex. 1007, 3:43–46, 3:53–55, 4:19–29, 4:34–39, 4:56–58, 4:63–5:1, 7:35–36, Fig. 2.

MAC address detector 238 “detects when a new host has been coupled to one of the ports 202–232” of network device 200. Ex. 1007, 4:19–22. After detecting when a new host has been coupled to a port, network device 200 stores the “MAC address for the new host” in a table that “correlates the MAC address for the new host with the port to which it is coupled,” e.g., a table stored in ACL-CAM 240. *Id.* at 4:22–26.

Source IP address detector 236 “automatically learns the source IP address for each MAC address entering a port” of network device 200. Ex. 1007, 4:56–58; *see id.* at 5:23–26. To “determine if the data packets received at a port contain a new source IP address that has not been learned, the ACL-CAM compares the source IP address and the MAC address in a received data packet” with the table of IP address-MAC address pairs. *Id.* at 5:26–30. After learning a new IP address-MAC address pair, “ACL-

CAM 240 is programmed with the information.” *Id.* at 5:35–36; *see id.* at 7:61–66, 8:43–48. After storing a new IP address-MAC pair in ACL-CAM 240, “blocking procedures are applied to the port.” *Id.* at 6:28–30.

Source IP address detector 236 can “learn the source IP address for a host in a number of different ways.” Ex. 1007, 5:38–39. As an example, “the source IP address can be learned by using a reverse address resolution protocol (RARP) which provides for sending out the MAC address on the subnet, and in response the host having the MAC address responds with its IP address.” *Id.* at 5:39–43. As another example, source IP address detector 236 can “learn the IP address for a host by listening to the DHCP response packet being returned to the host” because that response packet contains the source IP address for the host. *Id.* at 5:44–47. When “a DHCP packet is detected, the entry in the table for the MAC address receiving the DHCP packet with a source IP address is cleared and the source IP address provided in the DHCP packet is loaded into the table.” *Id.* at 5:47–50.

Further, to reduce “the risk of possibly learning the wrong IP address,” a system administrator may “seed the IP learning process with the IP address properties that are consistent with the subnet to which the host is coupled.” Ex. 1007, 6:14–18. For instance, “if the IP Subnet is 10.32.1.0/24, then this information can be used to seed” the “learning process and only match a MAC address” with an IP address “consistent with the subnet 10.32.1.0/24 addresses.” *Id.* at 6:18–22. Seeding the IP learning process advantageously “eliminate[s] false learning” of certain default IP addresses assigned “when a DHCP server is not initially located.” *Id.* at 6:22–25.

Network device 200 provides for “dynamically adjusting inbound source IP address anti-spoofing blocking criteria for each port” to permit the “blocking of data packets at the port of the network device based on the source IP address contained in the data packet.” Ex. 1007, 4:58–61, 6:66–7:1. Hence, “a system administrator can specify how many devices or IP addresses to permit per port of the network device 200.” *Id.* at 4:61–63.

4. WHETHER AN ORDINARILY SKILLED ARTISAN WOULD
HAVE BEEN MOTIVATED TO COMBINE THE TEACHINGS OF
THE REFERENCES WITH A REASONABLE EXPECTATION OF SUCCESS

(a) Petitioner’s Contentions

(i) Motivation to Combine: Gai and Yip

Petitioner contends that an ordinarily skilled artisan would have been motivated to combine Yip’s teachings with Gai’s teachings to achieve advantageous results, such as improved network security. *See* Pet. 15–16; Reply 6–15. Specifically, Petitioner asserts that Gai’s intermediate network device 316 uses text-based access control lists (ACLs) with “various criteria initially set up by an administrator for processing packets.” Pet. 15 (citing Ex. 1003 ¶¶ 53–54; Ex. 1006, 2:46–57, 3:26–30, 5:3–21, 6:13–17, 7:16–29, 21:1–7, Figs. 3, 5A–5E). Petitioner asserts that Yip discloses “an administrator including MAC addresses in ACLs.” *Id.* (citing Ex. 1003 ¶¶ 55–56; Ex. 1013, 2:43–47).

As support, Petitioner quotes Yip’s disclosure that ACLs “were developed to combat cyberattacks on the LAN Switch by providing an administrator-controlled list of Internet Protocol (IP) addresses or media access control (MAC) addresses that were authorized to access the network.” Reply 11–12 (quoting Ex. 1013, 2:43–47). Petitioner also quotes Yip’s disclosure that in “an alternate embodiment” to an embodiment using “a

temporary layer-3 address,” “a static layer-2 address, such as the user’s end station MAC address may be adequate for purposes of obtaining access.” *Id.* at 12 (quoting Ex. 1013, 6:23–27).

Petitioner asserts that including MAC addresses in ACLs “was known in the art.” Pet. 15 (citing Ex. 1014, 6:30–32, 8:27–47, 11:57–62; Ex. 1017, 55; Ex. 1018, 13); Reply 13–14 (citing Ex. 1014, 6:30–32, 8:27–47, 11:57–62; Ex. 1017, 55; Ex. 1018, 13; Ex. 1021, 50:22–51:6); *see* Pet. 16–17. According to Petitioner, Dr. Cole conceded that including MAC addresses in ACLs “was known in the art.” Reply 14 (citing Ex. 1021, 50:22–51:6). Petitioner also asserts that an ordinarily skilled artisan would have understood that including MAC addresses in ACLs would “improve security by allowing only devices with known addresses to communicate on the network.” Pet. 15.

Further, Petitioner asserts that an ordinarily skilled artisan would have been motivated to include MAC addresses in Gai’s text-based ACLs to “beneficially allow for dynamically generating TCAM ACLs with MAC addresses to thereby restrict or permit access based on MAC address.” Pet. 15–16; *see id.* at 27 (citing Ex. 1003 ¶¶ 91–92). Petitioner explains that including MAC addresses in Gai’s text-based ACLs would (1) “improve security because only specific MAC addresses would be permitted to communicate packets over the network” and (2) advance “Gai’s goal of providing security and implementing additional features with its ACLs.” *Id.* at 16 (citing Ex. 1003 ¶ 57; Ex. 1006, 8:3–6); *see id.* at 27 (citing Ex. 1003 ¶¶ 91–92).

Additionally, Petitioner contends that the proposed combination:

- (a) “merely represents a combination of prior art elements (MAC addresses, per Yip, with Gai’s ACL) according to known methods to yield predictable results (facilitate filtering of packets based on MAC addresses)”; and
- (b) “is also the use of a known technique (including MAC addresses in an ACL, per Yip) to improve a similar system (Gai’s system) in the same way (provide additional security by only permitting known MAC addresses to communicate on the network).”

Pet. 16 (citing Ex. 1003 ¶ 58); Reply 12.

Petitioner contends that while Gai describes a layer 3 intermediate network device as a preferred embodiment, Gai’s teachings also apply to layer 2 intermediate network devices. Reply 6. As support, Petitioner quotes Gai’s explanation that “the present invention may also be utilized in whole or in part with other intermediate network devices, such as switches and/or layer 2 intermediate devices, which are also intended to broadly cover any intermediate device operating primarily at the data link layer.” *Id.* (quoting Ex. 1006, 5:44–49) (emphasis omitted). According to Petitioner, Dr. Cole conceded that Gai’s teachings apply to layer 2 intermediate network devices. *Id.* at 6–7 (citing Ex. 1021, 109:10–13).

Also, Petitioner cites Gai’s disclosure that a “suitable platform for intermediate network device 316” includes “the Catalyst® 6000 family of multi layer [sic] switches” from Cisco Systems, Inc. Reply 8 (citing Ex. 1006, 6:62–65). Petitioner asserts that “Cisco’s Catalyst® 6000 multilayer switch” could operate at multiple layers, including layer 2 and layer 3. *Id.* at 10 (citing Ex. 1023 ¶ 9); *see id.* at 14–15, 17.

As support, Petitioner provides the following figure identified as Figure 7.5 that depicts a Catalyst® 6000 multilayer switch (Reply 10):

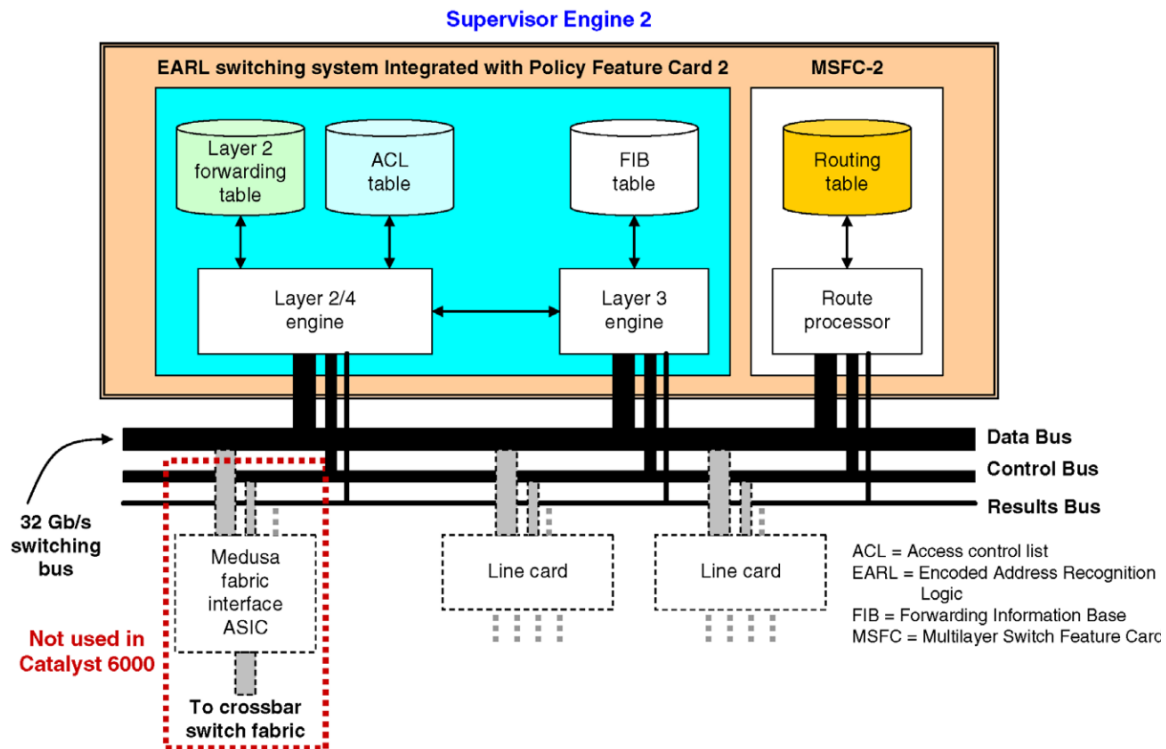


FIGURE 7.5 Catalyst 6000 with Supervisor Engine 2 with Policy Feature Card 2 (PFC2) and Multilayer Switch Feature Card 2 (MSFC2).

Figure 7.5 illustrates a Catalyst® 6000 multilayer switch described as having a “Supervisor Engine 2 with Policy Feature Card 2 (PFC2) and Multilayer Switch Feature Card 2 (MSFC2).” Ex. 1022, 141;⁶ *see* Ex. 1023 ¶ 9. As shown in Figure 7.5, the Catalyst® 6000 multilayer switch includes the following:

- (1) a Layer 2/4 engine connected to a Layer 3 engine;

⁶ For Exhibit 1022 (Chapter 7 titled “Architectures with Bus-Based Switch Fabrics: Case Study—Cisco Catalyst 6000 Series Switches”), we cite to the page numbers that appear in the publication instead of the page numbers that Petitioner applied to the exhibit.

- (2) the Layer 2/4 engine connected to a Layer 2 forwarding table and an ACL table; and
- (3) the Layer 3 engine connected to a Forwarding Information Base (FIB) table.

Ex. 1022, 141; *see* Ex. 1023 ¶¶ 9–10.

Further, Petitioner asserts that the Catalyst® 6000 multilayer switch could perform ACL filtering at layer 2 and layer 3. Reply 10–11 (citing Ex. 1021, 111:18–19; Ex. 1022, 142; Ex. 1023 ¶ 10).

(ii) Reasonable Expectation of Success: Gai and Yip

Petitioner asserts that an ordinarily skilled artisan would have had a reasonable expectation of success in combining Yip’s teachings with Gai’s teachings because (1) “both Gai and Yip disclose similar network devices that use ACLs” and (2) “[a]ny modification needed to implement Gai’s ACLs to include MAC address would have been ‘conventional’ and well within the level of skill in the art.” Pet. 16 (citing Ex. 1006, 2:58–60). Petitioner further asserts that the “expectation of success is also shown by other implementations of ACLs with MAC addresses.” *Id.* at 16–17 (citing Ex. 1003 ¶¶ 59–61; Ex. 1014, 6:30–32, 8:27–47, 11:57–62; Ex. 1017, 55; Ex. 1018, 13); *see* Reply 22.

Petitioner asserts that because Cisco’s Catalyst® 6000 multilayer switch could perform ACL filtering at layer 2 and layer 3, Patent Owner’s arguments about the incompatibility and infeasibility of implementing ACL filtering at layer 2 and layer 3 in a single device lack merit. Reply 14–15; *see id.* at 16–17. As support, Petitioner quotes Dr. Crovella’s testimony that an ordinarily skilled artisan “would have recognized that there is no incompatibility, complexity, or difficulty in implementing the combination of Yip and Gai since a suitable platform for implementing Gai’s teachings”

is Cisco’s Catalyst® 6000 multilayer switch “configurable to operate” at layer 2. *Id.* at 15 (quoting Ex. 1023 ¶ 12); *see id.* at 17.

(iii) Motivation to Combine: Gai and Kwan

Petitioner contends that an ordinarily skilled artisan would have been motivated to combine Kwan’s teachings with Gai’s teachings to achieve advantageous results, such as additional network security. *See* Pet. 17–21; Reply 15–19. Specifically, Petitioner asserts that Gai’s text-based ACLs include IP addresses that may be assigned either statically or dynamically, e.g., using the Dynamic Host Configuration Protocol (DHCP). Pet. 17–18 (citing Ex. 1007, 1:66–2:1). Petitioner asserts that “Kwan beneficially discloses how to learn dynamically assigned IP addresses.” *Id.* at 18 (citing Ex. 1007, 2:7–3:4).

Petitioner also asserts that an ordinarily skilled artisan “would have recognized that it would be beneficial to learn a new IP address” according to Kwan’s teachings so that Gai’s intermediate network device 316 could apply “security rules appropriate for—and potentially specific to—the device to which the IP address was dynamically assigned.” Pet. 18 (citing Ex. 1003 ¶ 66; Ex. 1007, 4:52–55); *see id.* at 29–30.

Petitioner contends that Kwan discloses:

- (1) network device 200 including an ACL-CAM containing IP address-MAC address pairs used to “control access and switching through the ports”;
- (2) several ways to learn a source IP address associated with a source MAC address, e.g., “by using a reverse address resolution protocol (RARP)” or “by listening to [a] DHCP response packet being returned to the host”; and
- (3) reducing or eliminating the “risk of possibly learning the wrong IP address” by seeding “the IP learning process

with the IP address properties that are consistent with the subnet to which the host is coupled.”

Pet. 18–19 (alteration by Petitioner) (quoting Ex. 1007, 5:40–41, 5:45–46, 6:15–18) (citing Ex. 1003 ¶ 67; Ex. 1007, 3:43–58, 4:10–48, 6:18–25).

Further, Petitioner asserts that “it would have been obvious to” an ordinarily skilled artisan “to implement Gai’s administrator-created text-based ACLs to include MAC addresses and seed IP address properties and to use this information to learn new IP addresses.” Pet. 20 (citing Ex. 1003 ¶ 70). Petitioner explains that including MAC addresses and seed IP address properties in Gai’s text-based ACLs would achieve the following advantageous results: first, permit Gai’s intermediate network device 316 to “process packets from a host that has a known MAC address but has been assigned a new IP address (e.g., using DHCP)”; second, “obviate the need for Gai’s administrator to manually update text-based ACLs when a host’s IP address changes or the network changes”; third, “allow the administrator to specify access control rules that are applied to a specific computer irrespective of the computer’s dynamically assigned IP address”; and fourth, “help combat source IP spoofing.” *Id.* at 20–21 (citing Ex. 1003 ¶¶ 70–71; Ex. 1006, 2:57–60, 4:6–13, 7:16–20, 18:3–5; Ex. 1007, 1:66–2:1, 3:1–4, 7:67–8:1); Reply 15; *see* Pet. 31, 53.

Petitioner asserts that “Dr. Cole agreed that supporting DHCP would be beneficial in contrast to the administrator manually updating the IP addresses.” Reply 16 (citing Ex. 1021, 36:11–37:2).

Petitioner also asserts that “it would have been obvious” when implementing Kwan’s teachings with Gai’s teachings to “apply one or more of Kwan’s IP learning techniques (e.g., RARP, DHCP)” and “limit IP

address learning to IP addresses that are consistent with the seed IP address properties in the ACLs, thereby lowering the ‘risk of possibly learning the wrong IP address.’” Pet. 20–21 (citing Ex. 1007, 5:38–67, 6:14–18, 8:25–38). Petitioner explains that doing so would beneficially “eliminate false learning” of source IP addresses assigned when “a DHCP server is not initially located.” *Id.* at 19, 21, 31 (citing Ex. 1007, 6:14–27).

Additionally, Petitioner contends that the proposed combination:

- (a) “merely represents a combination of prior art elements (MAC addresses, seed IP address properties, and RARP or DHCP learning techniques, per Kwan, with Gai’s administrator crated [sic, created] text-based ACLs) according to known methods to yield predictable results (facilitate filtering of packets based on MAC addresses and learning new IP addresses)”; and
- (b) “is merely the use of a known technique (using MAC addresses and seed IP address properties to learn new IP addresses using RARP and DHCP, per Kwan,) to improve a similar system (Gai’s network device 316) in the same way, including by (1) providing additional security by only permitting known MAC addresses on the network, (2) learning new IP addresses that are consistent with the seed IP address properties, (3) reducing false learning, and (4) combating source IP spoofing.”

Pet. 21 (citing Ex. 1003 ¶ 72); *see* Reply 16.

(iv) Reasonable Expectation of Success: Gai and Kwan

Petitioner asserts that an ordinarily skilled artisan would have had a reasonable expectation of success in combining Kwan’s teachings with Gai’s teachings because (1) Gai’s intermediate network device 316 and Kwan’s network device 200 both use ACLs to perform “analogous” switching functions and (2) “[m]odifying Gai’s administrator-created text-based ACLs

to include MAC addresses and seed IP address properties would have been ‘conventional’ and within the level of ordinary skill.” Pet. 18, 22 (citing Ex. 1003 ¶ 73; Ex. 1006, 2:58–60; Ex. 1007, 3:43–58); *see* Reply 19 (citing Ex. 1023 ¶ 15). Petitioner asserts that the “expectation of success is also supported by the specific details that Kwan provides to learn new IP addresses using RARP and DHCP” that were “standardized protocols and well known in the art.” Pet. 22 (citing Ex. 1003 ¶¶ 74–75; Ex. 1011, 21:1–3; Ex. 1014, 1:15–28; Ex. 1017, 5; Ex. 1018, 4).

As discussed above, Petitioner asserts that because Cisco’s Catalyst® 6000 multilayer switch could perform ACL filtering at layer 2 and layer 3, Patent Owner’s arguments about the incompatibility and infeasibility of implementing ACL filtering at layer 2 and layer 3 in a single device lack merit. Reply 16–17; *see id.* at 14–15; *supra* § III.D.4(a)(ii).

(b) Patent Owner’s Contentions

(i) Motivation to Combine: Gai and Yip

Patent Owner disputes that an ordinarily skilled artisan would have been motivated to combine Yip’s teachings with Gai’s teachings. *See* Resp. 7–20; Sur-reply 2–11. According to Patent Owner, a skilled artisan “would have considered these references in the context of the layers of the Open Systems Interconnection (OSI) Reference Model,” in particular, the data link layer (layer 2), the network layer (layer 3), and the transport layer (layer 4). Resp. 7; Sur-reply 2.

Patent Owner contends that at the time of the invention MAC addresses “were typically used only for granular hardware level device management” at the data link layer (layer 2) and ACLs were “hosted” in the network layer (layer 3) and the transport layer (layer 4). Resp. 15. Patent

Owner also contends that “[c]rossing these layers would lead to inefficiencies and increase network complexity, leading to potential new vulnerabilities and higher costs for implementation.” *Id.* (citing Ex. 2001 ¶ 64); *see id.* at 15–16 (citing Ex. 2001 ¶ 64).

Patent Owner contends that Gai “is directed to and discloses” a layer 3 intermediate network device and that Gai’s ACLs accomplish layer 3 switching. *See* Resp. 8–11 (citing Ex. 2001 ¶¶ 52–55); Sur-reply 4–6. According to Patent Owner, Gai’s intermediate network device 316 “preferably includes an Internet Protocol (IP) software layer,” and “IP message packets include a corresponding header which contains an IP source address and an IP destination address.” Resp. 8–9 (quoting Ex. 1006, 2:12–14, 5:26–27); *see* Sur-reply 6 (quoting Ex. 1006, 5:23–24). Patent Owner contends that Gai’s intermediate network device 316 has a “primary goal” of achieving higher switching speeds. Resp. 11–12 (citing Ex. 1006, 17:51–67; Ex. 2001 ¶ 56).

Patent Owner asserts that “Gai’s boilerplate recitation of possible applicability to ‘switches and/or layer 2 intermediate devices’ would have been considered” in “the context of Gai’s detailed disclosure of a Layer 3 device and its assertion that it could ‘operate with other, possibly far more complex, network topologies.’” Resp. 10 (quoting Ex. 1006, 5:46–47, 5:58–59); *see* Sur-reply 3 (citing Ex. 2001 ¶ 54). According to Patent Owner, an ordinarily skilled artisan would not have considered a layer 2 device “to be a more complex network topology.” Resp. 10.

Patent Owner argues that Petitioner improperly relies on information about Cisco’s Catalyst® 6000 multilayer switch in Exhibit 1022, i.e., Chapter 7 titled “Architectures with Bus-Based Switch Fabrics: Case

Study—Cisco Catalyst 6000 Series Switches” in the book *Switch/Router Architectures: Shared-Bus and Shared-Memory Based Systems*. See Sur-reply 4–5; Ex. 1022, 129. Specifically, Patent Owner asserts that Exhibit 1022 “is apparently dated 2018” and nothing in Exhibit 1022 indicates that it describes the Catalyst 6000 products as of Gai’s 1999 filing date. Sur-reply 4–5. In Patent Owner’s view, “it seems improbable that Cisco did not enhance and modify the Catalyst 6000 products over approximately 20 years.” *Id.* at 5.

Patent Owner asserts that Exhibit 1022 is:

- (1) improper “new evidence” that Petitioner “could have presented” with the Petition; and
- (2) “inadmissible hearsay” and “not relevant to any ground upon which trial was instituted.”

Sur-reply 4–5.

Further, Patent Owner asserts that Petitioner improperly relies on the Catalyst® 6000 multilayer switch because that device “is neither a patent nor a printed publication.” Sur-reply 10–11 (citing 35 U.S.C. § 311(b)).

Patent Owner contends that Yip “is directed to completely blocking access to a port until a lengthy authorization process is completed.”

Resp. 12; Sur-reply 6; *see* Resp. 14. As support, Patent Owner quotes Yip’s disclosure that a “network login controller operates in conjunction with”:

- (1) “a user interface to receive a user identification data from the port user”; and
- (2) “an authorization server to authenticate the user by sending a user authentication request containing the user identification data to the authentication server.”

Resp. 12 (quoting Ex. 1013, code (57)) (citing Ex. 2001 ¶ 58); Sur-reply 6 (quoting Ex. 1013, code (57)) (citing Ex. 2001 ¶ 58).

Patent Owner asserts that an ordinarily skilled artisan would not have looked to “Yip’s teaching of blocking a port until a lengthy authentication process had been completed in connection with Gai’s teaching of high-speed network switching.” Resp. 14. According to Patent Owner, blocking ports for “an indeterminate time would be antithetical to Gai’s goal of higher switching speeds and faster processing of messages,” and the proposed combination “would have been avoided as a potential performance killer.” *Id.* at 14–15 (citing Ex. 2001 ¶ 61).

Patent Owner contends that Yip:

- (1) “is not directed to access control lists”;
- (2) “does not disclose an ACL with a MAC address”;
- (3) “only discusses using a MAC address in alternate embodiments” and “in the background of the invention section of the patent specification”; and
- (4) “does not explain when or why or how a MAC address would be used.”

Resp. 14 (citing Ex. 1013, 6:23–28, 8:3–4; Ex. 2001 ¶ 60); Sur-reply 7–8 (citing Ex. 1013, 2:33–58). According to Patent Owner, an ordinarily skilled artisan would not have considered “Yip’s bare assertion that a MAC address could be used, without more, as teaching the use of MAC addresses.”

Resp. 14 (citing Ex. 2001 ¶ 60).

Patent Owner asserts that Yip discloses assigning temporary IP addresses and that “a MAC address may be used as part of Yip’s process for obtaining a temporary IP address.” Resp. 13 (citing Ex. 1013, 7:66–8:3, 8:8–16, 9:21–30; Ex. 2001 ¶ 59); Sur-reply 8–9 (citing Ex. 1013, 7:66–8:8, Fig. 5 (step 405)). Patent Owner asserts that assigning temporary IP addresses is “inconsistent” with Gai’s ACLs. Resp. 13. Patent Owner also

asserts that using a MAC address “as part of the process of obtaining a temporary IP address” in Yip does not “equate to using a MAC address in an access control list.” Sur-reply 8–9.

Additionally, Patent Owner contends that Yip “teaches away” from using MAC addresses for access control because they “are machine or hardware based.” Sur-reply 7. As support, Patent Owner quotes Yip’s disclosure as follows: “A major drawback to access lists, DoS, and SYN attack protections is that access to the network is machine- or hardware-based instead of user-based. Therefore, an unauthorized user who has access to an authorized machine can still gain access to the network, completely bypassing the intended security protection.” *Id.* at 7–8 (emphasis omitted) (quoting Ex. 1013, 2:56–61).

(ii) Reasonable Expectation of Success: Gai and Yip

Patent Owner contends that the “proposed combination of Gai and Yip would not have been viewed as a feasible option.” Resp. 15. According to Patent Owner, an ordinarily skilled artisan “would not think to combine ACLs and MAC addresses due to their inherent separation within network layers” of the OSI model and the “inherent incompatibility” of the combination. *Id.* at 15–16 (citing Ex. 2001 ¶ 64); *see id.* at 28 (citing Ex. 2001 ¶ 84).

(iii) Motivation to Combine: Gai and Kwan

Patent Owner disputes that an ordinarily skilled artisan would have been motivated to combine Kwan’s teachings with Gai’s teachings. *See* Resp. 7, 16–20; Sur-reply 2–6, 9–13. Specifically, Patent Owner asserts that Kwan’s teachings “are directed to” a layer 2 network device for “improving defenses against Source IP Spoofing” by attacking “the problem at the

subnet or Layer 2 level.” Resp. 16 (quoting Ex. 1007, 3:21–23). Patent Owner asserts that an ordinarily skilled artisan would have recognized that “what works for Layer 2 switching generally does not apply to Layer 3 switching.” *Id.* at 17–18.

Patent Owner contends that Kwan discloses “limiting the number of IP addresses associated with each port” and “limiting each port to a single host.” Resp. 17 (citing Ex. 1007, 6:30–31, 6:36–38, 6:60–7:5; Ex. 2001 ¶ 68); Sur-reply 11–12 (citing Ex. 1007, 6:36–38, 6:60–7:5; Ex. 2001 ¶ 68). Patent Owner contends that “limiting the number of IP addresses for each port” means that “there would be a limited number of already learned IP addresses.” Sur-reply 12.

Further, Patent Owner asserts that “limiting the number of hosts that can connect to a single port” conflicts with Gai’s goal of “achieving higher switching speeds.” Resp. 18 (citing Ex. 2001 ¶ 70). According to Patent Owner, “Kwan’s teachings are incompatible with Gai’s teachings and would, in fact, result in slower overall switching speeds.” Sur-reply 13.

Additionally, Patent Owner asserts that Kwan discloses “a lengthy and time-consuming process for learning the correct IP address.” Resp. 17 (citing Ex. 1007, 6:5–8, 6:25–27; Ex. 2001 ¶ 69); Sur-reply 11 (citing Ex. 1007, 6:5–8, 6:25–27; Ex. 2001 ¶ 69). Patent Owner also asserts that “requiring a lengthy process for learning the correct IP address” conflicts with Gai’s goal of “achieving higher switching speeds.” Resp. 18 (citing Ex. 2001 ¶ 70).

(iv) Reasonable Expectation of Success: Gai and Kwan

Patent Owner asserts that an ordinarily skilled artisan would not have “viewed as feasible” combining “the functionality of ACLs and MAC

addresses, which is a requirement necessary for a combination of Gai and Kwan to function as proposed by Petitioner.” Resp. 18 (citing Ex. 2001 ¶ 72). Patent Owner also asserts that “adding dynamic IP learning functionality to ACLs including MAC addresses would introduce new vulnerabilities into the network, such as IP spoofing the MAC address into applying incorrect security controls.” *Id.* (citing Ex. 2001 ¶ 73). Therefore, according to Patent Owner, an ordinarily skilled artisan “would have viewed a combination of IP address properties and MAC addresses in text-based ACLs as far too complex and vulnerable to integrate into a network with the certainty needed for network security.” *Id.* at 19 (citing Ex. 2001 ¶ 73).

(c) Analysis

(i) Motivation to Combine: Gai and Yip

For the reasons explained below, we agree with Petitioner that an ordinarily skilled artisan would have been motivated to combine Yip’s teachings with Gai’s teachings in the way Petitioner proposes. *See* Pet. 15–16; Reply 6–15; Ex. 1003 ¶¶ 45, 51–58; Ex. 1023 ¶¶ 6–8, 11–13.

First, Gai describes “intermediate network devices” as including bridges, switches, and routers. Ex. 1006, 1:59–2:22; *see id.* at 5:35–44; Ex. 1003 ¶ 106; Ex. 1023 ¶ 6. Regarding the preferred embodiment, Gai explains that “[p]referably, intermediate network device 316 is a layer 3 intermediate device and thus operates up to the network layer of the communication protocol stack implemented within the network 300.” Ex. 1006, 5:22–25; *see* Ex. 1003 ¶ 106. But Gai further explains that “the present invention may also be utilized in whole or in part with other intermediate network devices, such as switches and/or layer 2 intermediate devices, which are also intended to broadly cover any intermediate device

operating primarily at the data link layer.” Ex. 1006, 5:44–49; *see* Ex. 1023 ¶¶ 6, 13. Hence, Patent Owner’s arguments that Gai’s disclosures relate only to layer 3 devices lack merit. *See* Ex. 1023 ¶¶ 7, 13; Resp. 8–12; Sur-reply 3–6.

Based on Gai’s statement that “the present invention will operate with other, possibly far more complex, network topologies,” than illustrated in Figure 3, Patent Owner asserts that an ordinarily skilled artisan would not have considered a layer 2 device “to be a more complex network topology.” Resp. 10; *see* Ex. 1006, 5:57–59. But Patent Owner does not explain how a single device equates to a network topology. *See* Resp. 10. In any event, Gai discloses that intermediate network device 316 “operates up to the network layer [layer 3] of the communication protocol stack.” Ex. 1006, 5:22–25; *see* Ex. 1003 ¶ 106. When operating “up to” the network layer (layer 3), intermediate network device 316 also operates at lower layers, including the data link layer (layer 2). *See* Ex. 1021, 111:16–22.

Second, Yip explains that previous “network security techniques have been implemented at a connection point (i.e. at the LAN switch level) to prevent intruder and hacker attacks.” Ex. 1013, 2:33–35; *see* Ex. 1003 ¶ 45. For instance, techniques “have been designed and implemented in LAN switches to prohibit cyber-attacks, such as access control lists (ACLs).” Ex. 1013, 2:35–38; *see* Ex. 1003 ¶ 45. Yip also explains that ACLs “were developed to combat cyber-attacks on the LAN switch by providing an administrator-controlled list of Internet Protocol (IP) addresses or media access control (MAC) addresses that were authorized to access the network.” Ex. 1013, 2:43–47; *see* Ex. 1003 ¶¶ 45, 56; Ex. 1023 ¶ 11.

Hence, Yip discloses ACLs with MAC addresses. Ex. 1013, 2:43–47; *see* Ex. 1003 ¶¶ 45, 56; Ex. 1023 ¶ 11. Patent Owner’s contention that Yip “does not disclose an ACL with a MAC address” lacks merit. *See* Sur-reply 7. Yip’s disclosure of ACLs with MAC addresses means that ACL filtering occurred at layer 2 in the prior art. Ex. 1023 ¶ 11.

Third, that Yip discloses using MAC addresses “in the background of the invention section” and “in alternate embodiments,” as Patent Owner contends, does not matter. *See* Resp. 14; Sur-reply 7; Ex. 1013, 2:43–47, 6:23–27; Ex. 1023 ¶ 11. “A reference constitutes prior art for all that it teaches as of its earliest accorded filing date.” *In re Riggs*, 131 F.4th 1377, 1385 (Fed. Cir. 2025). For instance, “[e]ven if a reference discloses an inoperative device, it is prior art for all that it teaches.” *Beckman Instrs., Inc. v. LKB Produkter AB*, 892 F.2d 1547, 1551 (Fed. Cir. 1989).

Fourth, Patent Owner mischaracterizes Yip when asserting that using a MAC address “as part of the process of obtaining a temporary IP address” in Yip does not “equate to using a MAC address in an access control list.” *See* Sur-reply 8–9. Yip explains that a user may begin the authentication process and initially gain access to the network login controller and the user interface on the packet-forwarding device by using one of three alternative addresses as follows:

- (1) “a temporary IP address,” i.e., “a temporary layer-3 address,” that “is discarded upon successful authentication”;
- (2) a MAC address, i.e., “a static layer-2 address,” that “may be adequate for purposes of obtaining access” to the network login controller and the user interface; and
- (3) “a previously obtained IP address, such as in the case of an Internet service provider environment where the user

uses the same port and VLAN for authentication each time.”

Ex. 1013, 6:15–35, 7:66–8:16, 9:21–24, Fig. 5 (steps 405 and 410); *see id.* at 3:64–4:3; Ex. 1023 ¶ 11.

Hence, contrary to Patent Owner’s assertion, Yip does not disclose using a MAC address “as part of the process of obtaining a temporary IP address.” *See* Sur-reply 8–9. Instead, “for purposes of obtaining access,” Yip discloses using a MAC address as an alternative to a temporary IP address. Ex. 1013, 6:15–27, 7:66–8:8; *see id.* at 3:64–4:3; Ex. 1023 ¶ 11. For example, Yip explains that in “an alternate embodiment” to an embodiment using “a temporary layer-3 address,” “a static layer-2 address, such as the user’s end station MAC address may be adequate for purposes of obtaining access.” Ex. 1013, 6:19–27; *see* Ex. 1023 ¶ 11.

Fifth, Patent Owner mischaracterizes the proposed combination when asserting that an ordinarily skilled artisan would not have looked to “Yip’s teaching of blocking a port until a lengthy authentication process had been completed in connection with Gai’s teaching of high-speed network switching.” *See* Resp. 14. Petitioner does not propose using Yip’s authentication process in Gai’s system. *See* Pet. 15–16; Reply 6–15.

Sixth, we disagree with Patent Owner that Yip “teaches away” from using MAC addresses for access control. *See* Sur-reply 7–8. Yip’s disclosure that “an unauthorized user who has access to an authorized machine can still gain access to the network, completely bypassing the intended security protection,” applies to any authorized machine regardless of the data identifying the authorized machine, e.g., a MAC address at the data link layer (layer 2) or an IP address at the network layer (layer 3). *See*

Ex. 1013, 2:58–61. That disclosure does not “criticize, discredit, or otherwise discourage” using MAC addresses for access control and, therefore, does not teach away from doing so. *See DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1327 (Fed. Cir. 2009).

Seventh, as Petitioner asserts, including MAC addresses in ACLs “was known in the art.” Ex. 1014, 4:13–15, 6:28–32, 8:27–47, 11:46–62, Figs. 2A, 2C; Ex. 1016, claims 1–2; Ex. 1017, 55; Ex. 1018, 13; Ex. 1021, 50:22–51:6; *see* Ex. 1003 ¶ 55; Pet. 15; Reply 13–14. As an example, a patent filed in 2003 and issued in 2008 discloses (1) switches “implemented as OSI (Open Systems Interconnection) layer 2 devices,” (2) “using a CAM (Content Addressable Memory) and/or ACL (Access Control List)” in a switch, and (3) storing the “combination of source IP address, MAC address, and interface ID” as a table entry “associated with a particular client.” Ex. 1014, 4:13–15, 6:28–32, 8:27–47, 11:46–62, Figs. 2A, 2C.

Eighth, as Petitioner also asserts, an ordinarily skilled artisan would have been motivated to include MAC addresses in Gai’s text-based ACLs to “beneficially allow for dynamically generating TCAM ACLs with MAC addresses to thereby restrict or permit access based on MAC address.” Ex. 1003 ¶ 57; *see* Pet. 15–16. Including MAC addresses in Gai’s text-based ACLs would “improve security because only specific MAC addresses would be permitted to communicate packets over the network.” Ex. 1003 ¶ 57; *see* Pet. 16. Including MAC addresses in Gai’s text-based ACLs would also advance “Gai’s goal of providing security and implementing additional features with its ACLs.” Ex. 1003 ¶ 57; *see* Ex. 1006, 8:3–6; Pet. 16.

Ninth, “[t]here is a motivation to combine when a known 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 ‘prior art elements according to their established functions.’” *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1380–81 (Fed. Cir. 2023) (citations omitted) (quoting *KSR*, 550 U.S. at 417; *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 799–800 (Fed. Cir. 2021)). Here, Petitioner identifies the known technique of including MAC addresses in ACLs used to improve network security in network devices that would improve network security in Gai’s network device when used according to the known technique. *See* Pet. 16; Reply 12; Ex. 1003 ¶ 58; Ex. 1006, 5:44–49; Ex. 1013, 2:43–47; Ex. 1014, 4:13–15, 6:28–32, 8:27–47, 11:46–62, Figs. 2A, 2C.

For the reasons discussed above, an ordinarily skilled artisan would have been motivated to combine Yip’s teachings with Gai’s teachings in the way Petitioner proposes, and Patent Owner’s contentions to the contrary lack merit.

(ii) Reasonable Expectation of Success: Gai and Yip

As Petitioner asserts, an ordinarily skilled artisan would have had a reasonable expectation of success in combining Yip’s teachings with Gai’s teachings because (1) “both Gai and Yip disclose similar network devices that use ACLs” and (2) “[a]ny modification needed to implement Gai’s ACLs to include MAC address would have been conventional and well within the level of skill in the art.” Ex. 1003 ¶ 59; *see* Pet. 16. Also, other known implementations of ACLs with MAC addresses support the expectation of success. Ex. 1003 ¶ 60; Ex. 1013, 2:43–47; Ex. 1014, 4:13–15, 6:28–32, 8:27–47, 11:46–62, Figs. 2A, 2C; Ex. 1016, claims 1–2;

Ex. 1017, 55; Ex. 1018, 13; Ex. 1021, 50:22–51:6; Ex. 1023 ¶ 15; *see* Pet. 16–17.

Further, we agree with Petitioner that Patent Owner’s arguments about the incompatibility and infeasibility of implementing ACL filtering at layer 2 and layer 3 in a single device lack merit. *See* Reply 14–17.

Specifically, Gai identifies “the Catalyst® 6000 family of multi layer [sic, multilayer] switches” from Cisco Systems, Inc. as a “suitable platform for intermediate network device 316.” Ex. 1006, 6:62–65; *see* Ex. 1003 ¶ 106; Ex. 1023 ¶ 12. Dr. Cole admits that “a multilayer switch is a router” and that “means it’s operating on layers 2 and 3.” Ex. 1021, 111:14–112:4.

Additionally, the information about Cisco’s Catalyst® 6000 multilayer switch in Exhibit 1022:

- (1) confirms that a single device could perform ACL filtering at layer 2 and layer 3; and
- (2) refutes Patent Owner’s arguments about the incompatibility and infeasibility of a single device performing ACL filtering at layer 2 and layer 3.

See Ex. 1022, 141–43; Ex. 1023 ¶¶ 9–10, 12; Resp. 15–16.

In particular, the information about Cisco’s Catalyst® 6000 multilayer switch in Exhibit 1022 indicates that the switch includes a Layer 2/4 engine, an ACL table connected to the Layer 2/4 engine, and a Layer 3 engine connected to the Layer 2/4 engine. Ex. 1022, 141. Dr. Crovella explains that a multilayer switch operates on multiple layers and that the Catalyst® 6000 multilayer switch includes “operat[ions] at Layer 2 to perform ACL filtering.” Ex. 1023 ¶¶ 8–9. Thus, the Catalyst® 6000 multilayer switch demonstrates the feasibility of a single device performing ACL filtering at layer 2 and layer 3.

We disagree with Patent Owner that Exhibit 1022 is improper “new evidence.” *See* Sur-reply 4. In the Response, Patent Owner asserted that an ordinarily skilled artisan “would not think to combine ACLs and MAC addresses due to their inherent separation within network layers” of the OSI model and the “inherent incompatibility” of the combination. Resp. 15–16; *see id.* at 28. In the Reply, Petitioner relied on Exhibit 1022 to show that the Catalyst® 6000 multilayer switch could perform ACL filtering at layer 2 and layer 3 and refute Patent Owner’s assertions concerning “inherent separation” and “inherent incompatibility” not limited temporally. Reply 10–11, 14–17; *see* Resp. 15–16, 28.

Petitioner properly relies on Exhibit 1022 to refute Patent Owner’s assertions concerning “inherent separation” and “inherent incompatibility” not limited temporally. *See* Resp. 15–16, 28; Reply 10–11, 14–17; *Rembrandt Diagnostics, LP v. Alere, Inc.*, 76 F.4th 1376, 1384–85 (Fed. Cir. 2023) (determining that motivation-to-combine arguments in a petitioner reply properly addressed arguments in a patent owner response); *Apple Inc. v. Andrea Elecs. Corp.*, 949 F.3d 697, 706–07 (Fed. Cir. 2020) (determining that unpatentability arguments in a petitioner reply properly addressed arguments in a patent owner response); 37 C.F.R. § 42.23(b).

As for Patent Owner’s assertion that Petitioner “could have presented” Exhibit 1022 with the Petition, Patent Owner “conflates capability with obligation.” *See* Sur-reply 4; *Provisur Techs., Inc. v. Weber, Inc.*, 50 F.4th 117, 122 (Fed. Cir. 2022). Although Petitioner “could have presented” Exhibit 1022 with the Petition, nothing obligated Petitioner to do so.

As for Patent Owner’s assertion that Exhibit 1022 is “inadmissible hearsay” and “not relevant to any ground upon which trial was instituted,”

we disagree. *See* Sur-reply 4–5. The information about the Catalyst® 6000 multilayer switch in Exhibit 1022 rebuts Patent Owner’s arguments regarding reasonable expectation of success. *See* Resp. 15–16; Reply 10–11, 14–17; Ex. 1022, 141–43; Ex. 1023 ¶¶ 9–10, 12. Moreover, Patent Owner did not timely object to Exhibit 1022 or move to exclude Exhibit 1022. *See* 37 C.F.R. § 42.64(b)(1) (explaining that “[o]nce a trial has been instituted, any objection must be filed within five business days of service of evidence to which the objection is directed”).

As for Patent Owner’s assertion that Petitioner improperly relies on the Catalyst® 6000 multilayer switch because that device “is neither a patent nor a printed publication,” we disagree. *See* Sur-reply 10–11 (citing 35 U.S.C. § 311(b)). Section 311(b) provides that a petitioner “may request to cancel as unpatentable” claims “only on the basis of prior art consisting of patents or printed publications.” 35 U.S.C. § 311(b). As the “basis” for its request to cancel the challenged claims, Petitioner relies on “prior art consisting of patents or printed publications,” e.g., on Gai, Yip, and Kwan to show where each limitation in claims 1 and 3 “is found in the prior art.” *See* Pet. 9–85; Reply 5–26; 37 C.F.R. § 42.104(b)(4).

Petitioner does not rely on the Catalyst® 6000 multilayer switch as the “basis” for its request to cancel the challenged claims. *See* Pet. 9–85; Reply 5–26. Rather, Petitioner properly relies on the Catalyst® 6000 multilayer switch to rebut Patent Owner’s arguments regarding reasonable expectation of success. *See* Reply 10–11, 14–17; *see also Anacor Pharms., Inc. v. Iancu*, 889 F.3d 1372, 1380 (Fed. Cir. 2018) (explaining that there is “no blanket prohibition against the introduction of new evidence during an inter partes review”).

(iii) Motivation to Combine: Gai and Kwan

For the reasons explained below, we agree with Petitioner that an ordinarily skilled artisan would have been motivated to combine Kwan’s teachings with Gai’s teachings in the way Petitioner proposes. *See* Pet. 17–21; Reply 15–19; Ex. 1003 ¶¶ 47–50, 62–72, 91–92, 98, 101, 121; Ex. 1023 ¶¶ 14–15.

First, as Petitioner asserts, Kwan “discloses how to learn dynamically assigned IP addresses.” Ex. 1007, 5:38–67; *see* Ex. 1003 ¶ 49; Pet. 18–19. An ordinarily skilled artisan “would have recognized that it would be beneficial to learn a new IP address” according to Kwan’s teachings so that Gai’s intermediate network device 316 could apply “security rules appropriate for—and potentially specific to—the device to which the IP address” was dynamically assigned. Ex. 1003 ¶ 66; *see* Ex. 1007, 4:52–55.

Second, as Petitioner also asserts, Kwan discloses reducing or eliminating the “risk of possibly learning the wrong IP address” by seeding “the IP learning process with the IP address properties that are consistent with the subnet to which the host is coupled.” Ex. 1007, 6:14–25; *see* Ex. 1003 ¶¶ 50, 69; Pet. 19. Including MAC addresses and seed IP address properties in Gai’s text-based ACLs would achieve the following advantageous results: first, permit Gai’s intermediate network device 316 to “process packets from a host that has a known MAC address but has been assigned a new IP address (e.g., using DHCP)”; second, “obviate the need for Gai’s administrator to manually generate updated text-based ACLs when a host’s IP address changes or the network changes”; third, “allow the administrator to specify access control rules that are applied to a specific computer irrespective of the IP address assigned dynamically to that

computer”; and fourth, “increase the efficiency and effectiveness of combating source IP spoofing.” Ex. 1003 ¶¶ 70–71; *see id.* ¶¶ 91–92, 98; Ex. 1006, 2:57–60, 7:16–20, 18:3–5; Ex. 1007, 1:66–2:1, 3:1–4, 7:67–8:1; Ex. 1021, 36:11–37:2.

For example, “Kwan’s DHCP and RARP techniques would be beneficial because they would allow Gai’s system to support dynamically assigned IP addresses, whose use was prevalent.” Ex. 1003 ¶ 121; *see* Ex. 1007, 7:61–66. Also, limiting IP address learning to IP addresses that are consistent with the seed IP address properties in the ACLs would beneficially “eliminate false learning” of source IP addresses assigned when “a DHCP server is not initially located.” Ex. 1003 ¶¶ 71, 101; Ex. 1007, 6:18–25; *see* Ex. 1003 ¶¶ 50, 69.

Third, “[t]here is a motivation to combine when a known 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 ‘prior art elements according to their established functions.’” *Intel*, 61 F.4th at 1380–81. Here, Petitioner identifies the known techniques of using MAC addresses and seed IP address properties to learn new IP addresses used to improve network security in network devices that would improve network security in Gai’s network device when used according to the known techniques. *See* Pet. 21; Reply 16; Ex. 1003 ¶ 72; Ex. 1007, 3:1–4, 5:38–67, 6:14–25.

Fourth, that Kwan’s teachings “are directed to” a layer 2 network device for “improving defenses against Source IP Spoofing” by attacking “the problem at the subnet or Layer 2 level,” as Patent Owner asserts, does not matter. *See* Resp. 16. As discussed above, Gai explains that “the

present invention may also be utilized in whole or in part with other intermediate network devices, such as switches and/or layer 2 intermediate devices, which are also intended to broadly cover any intermediate device operating primarily at the data link layer.” Ex. 1006, 5:44–49; *see* Ex. 1023 ¶¶ 6, 13.

Further, while Kwan discloses that network device 200 “provides layer 2 switching functions,” Kwan also discloses that network device 200 “utilize[s] source IP address information,” i.e., layer 3 information, and correlates a source IP address with a MAC address to enable access control and switching based on IP address-MAC address pairs stored in an ACL-CAM. Ex. 1007, 3:42–45, 4:10–12, 4:19–47; *see id.* at 5:38–67, 6:28–30. Thus, Kwan’s network device 200 operates differently than a “typical layer 2 switch” that “would not analyze the source IP address in connection with this switching function, and would not use the source IP address to provide source IP anti-spoofing operations.” *Id.* at 4:6–9.

Fifth, Patent Owner mischaracterizes Kwan when contending that Kwan discloses “limiting each port to a single host.” *See* Resp. 17. Kwan explains that “source IP Address spoofing is a common technique used in denial of service attacks (DoS)” and that other types of “source IP address spoofing attacks are widely known, and include attacks such as distributed denial of service attacks (DDoS), Worm attacks, and Man In the Middle attacks.” Ex. 1007, 1:21–26. To thwart certain types of spoofing attacks, Kwan’s network device 200 permits “dynamically adjusting inbound source IP address anti-spoofing blocking criteria for each port” to permit the “blocking of data packets at the port of the network device based on the source IP address contained in the data packet.” *Id.* at 4:58–61, 6:66–7:1.

In particular, “a system administrator can specify how many devices or IP addresses to permit per port of the network device 200.” *Id.* at 4:61–63.

For instance, “the system administrator could control the maximum number of source IP addresses which are learned from a port” to better prevent “certain types of spoofing attacks (such as DoS attacks).” Ex. 1007, 5:4–8, 6:63–66; *see id.* at 6:60–63. By “limiting the number of source IP addresses on a port, an attacking host could only use a limited number of spoofed IP addresses before the maximum number of source IP addresses for the port would be exceeded.” *Id.* at 7:2–5. Thus, Kwan discloses limiting the number of source IP addresses on a port as an option to better prevent “certain types of spoofing attacks (such as DoS attacks).” *See id.* at 4:58–63, 5:4–8, 6:60–7:5.

Additionally, when describing the process for learning IP address-MAC address pairs and then storing the learned pairs in the ACL-CAM, Kwan explains that if “there is more than one host device allowed per port, this process of determining MAC address and source IP address pairs will be repeated for each learned IP address on the port.” Ex. 1007, 6:28–36. Thus, Kwan contemplates “more than one host device” per port. *See id.*

Hence, contrary to Patent Owner’s contention, Kwan does not disclose “limiting each port to a single host.” *See* Ex. 1007, 4:58–63, 5:4–17, 6:28–38, 6:60–7:5; Resp. 17.

Sixth, we disagree with Patent Owner that “limiting the number of hosts that can connect to a single port” conflicts with Gai’s goal of “achieving higher switching speeds.” *See* Resp. 18. As Dr. Crovella testifies, “there is no logical relationship” between the switching speeds and “the number of hosts that can connect to a single port.” Ex. 1023 ¶ 14.

Hence, an ordinarily skilled artisan “would have understood that the switching speeds are not diminished if the number of hosts are limited per port.” *Id.* We credit Dr. Crovella’s testimony.

Seventh, we disagree with Patent Owner that Kwan’s “process for learning the correct IP address” conflicts with Gai’s goal of “achieving higher switching speeds.” *See* Resp. 18. As Dr. Crovella testifies, an ordinarily skilled artisan “would have recognized that Kwan’s technique to learn a new IP address (e.g., one that was assigned with DHCP) does not impact switching speeds of an already learned” IP address. Ex. 1023 ¶ 14. Instead, “Kwan’s technique would benefit Gai because a new IP address would be learned quickly without manual administrator intervention, which is time intensive.” *Id.*; *see* Ex. 1003 ¶ 70. We credit Dr. Crovella’s testimony. Additionally, Dr. Cole agreed that using DHCP instead of static IP addresses would be “much more scalable” since “there’s no manual configuration there.” Ex. 1021, 36:11–25.

For the reasons discussed above, an ordinarily skilled artisan would have been motivated to combine Kwan’s teachings with Gai’s teachings in the way Petitioner proposes, and Patent Owner’s contentions to the contrary lack merit.

(iv) Reasonable Expectation of Success: Gai and Kwan

As Petitioner asserts, an ordinarily skilled artisan would have had a reasonable expectation of success in combining Kwan’s teachings with Gai’s teachings because (1) Gai’s intermediate network device 316 and Kwan’s network device 200 both use ACLs to perform “analogous” switching functions and (2) modifying Gai’s administrator-created text-based ACLs to include MAC addresses and seed IP address properties would have been

conventional and “well within the level of ordinary skill.” *See* Ex. 1003 ¶¶ 67, 73–74; Ex. 1006, 4:26–40, 16:63–17:3, 17:26–44; Ex. 1007, 3:43–58; Pet. 18, 22. For example, the RARP and DHCP techniques disclosed in Kwan for learning new IP addresses based on MAC addresses rest on “standardized protocols” that were “well known in the art.” Ex. 1003 ¶ 74; *see* Ex. 1007, 5:38–58; Ex. 1011, 21:1–3; Ex. 1014, 1:16–28. Further, “the specific details that Kwan provides to learn new IP addresses based on MAC addresses using RARP and DHCP techniques” support the expectation of success. Ex. 1003 ¶ 74.

Moreover, other known implementations of ACLs with MAC addresses support the expectation of success. Ex. 1003 ¶ 60; Ex. 1013, 2:43–47; Ex. 1014, 4:13–15, 6:28–32, 8:27–47, 11:46–62, Figs. 2A, 2C; Ex. 1016, claims 1–2; Ex. 1017, 55; Ex. 1018, 13; Ex. 1021, 50:22–51:6; Ex. 1023 ¶ 15.

Additionally, we disagree with Patent Owner that “adding dynamic IP learning functionality to ACLs including MAC addresses would introduce new vulnerabilities into the network, such as IP spoofing the MAC address into applying incorrect security controls.” *See* Resp. 18. As Dr. Crovella testifies, an ordinarily skilled artisan would have understood that in the proposed combination “vulnerabilities are reduced and IP spoofing the MAC address would not be an issue.” Ex. 1023 ¶ 15.

As Dr. Crovella further testifies, an administrator of the proposed combination provides a “seed IP address” and MAC addresses, e.g., “as text inputs in the ACL.” Ex. 1023 ¶ 15. Due to the administrator’s multiple inputs, “spoofing in the combined system is reduced because an IP address attempting to spoof the MAC address” would have to spoof not only the IP

address resulting from the “seed IP address” but also the paired MAC address. *Id.* According to Dr. Crovella, spoofing both addresses “would be very difficult.” *Id.* We credit Dr. Crovella’s testimony.

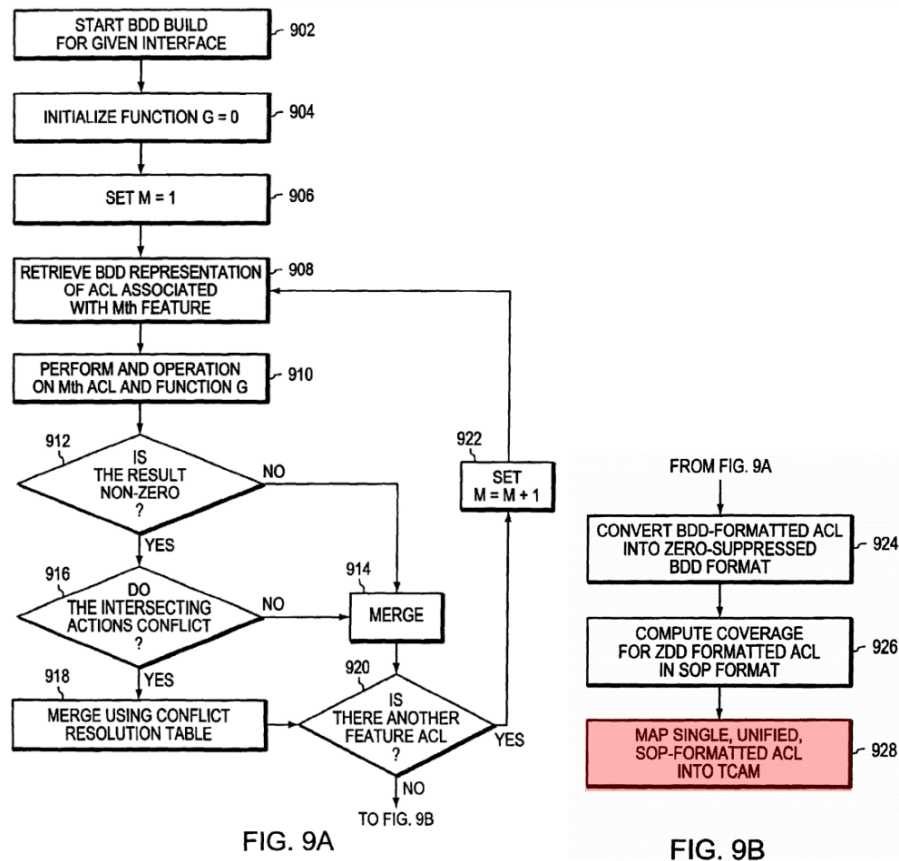
5. INDEPENDENT CLAIM 1

(a) Preamble 1.0

Claim 1 recites in its preamble “[a] method of developing an access control list.” Ex. 1001, 10:12.

Petitioner contends that the combined disclosures in Gai, Yip, and Kwan teach claim 1’s preamble for several related reasons. *See* Pet. 22–25. First, Petitioner asserts that Gai discloses “a method and apparatus for efficiently organizing . . . access control lists (ACLs).” *Id.* at 22 (alteration by Petitioner) (emphasis omitted) (quoting Ex. 1006, 3:55–57). Petitioner also asserts that Gai’s Figures 9A and 9B illustrate “a method for dynamically generating optimized ACLs” stored in a ternary content addressable memory (TCAM). *Id.* at 23 (citing Ex. 1003 ¶ 79).

To support its assertions, Petitioner provides a highlighted version of Gai's Figures 9A and 9B as reproduced below (Pet. 24):



Figures 9A and 9B depict steps performed by an ACL converter in a network switch to generate “a single, unified ACL for a given interface.” Ex. 1006, 12:20–22, Figs. 9A–9B. The above highlighted version of Figures 9A and 9B includes pink highlighting over step 928 for “map single, unified SOP-formatted ACL into TCAM” in Figure 9B.⁷ See Pet. 24; Ex. 1003 ¶ 79.

⁷ The acronym “SOP” stands for “sum of products.” Ex. 1006, 4:22–23, code (57).

Second, Petitioner asserts that the combination with Yip modifies Gai's method "such that the TCAM ACL is updated to include MAC addresses." Pet. 24 (citing Ex. 1003 ¶ 81); *see id.* at 15–16, 20.

Third, Petitioner asserts that the combination with Kwan modifies Gai's method "such that the TCAM ACL is updated to include . . . newly learned IP addresses." Pet. 24 (citing Ex. 1003 ¶ 81); *see id.* at 18–20.

Therefore, according to Petitioner, "Gai in combination with Yip and Kwan discloses a method of dynamically generating an optimized TCAM ACL, which renders obvious the preamble." Pet. 24–25 (citing Ex. 1003 ¶ 82).

Patent Owner makes no arguments specific to claim 1's preamble. *See, e.g.*, Resp. 6–20; Sur-reply 2–13. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Generally, a preamble does not limit a claim. *Allen Eng'g Corp. v. Bartell Indus., Inc.*, 299 F.3d 1336, 1346 (Fed. Cir. 2002). We need not decide whether claim 1's preamble limits the claim because, for the reasons stated by Petitioner and supported by Dr. Crovella's testimony, we agree with Petitioner that the combined disclosures in Gai, Yip, and Kwan teach claim 1's preamble. *See* Pet. 22–25; Ex. 1003 ¶¶ 76–82.

(b) Limitation 1.1

Claim 1 recites "developing an enhanced access control list including data related to at least one of user names, DNS names, Windows domain names, and physical addresses." Ex. 1001, 10:14–16 (limitation 1.1).

Petitioner contends that the combined disclosures in Gai, Yip, and Kwan teach limitation 1.1 for several related reasons. *See* Pet. 25–32. First,

Petitioner asserts that Gai teaches “developing an enhanced access control list” because Gai discloses that an administrator creates one or more text-based ACLs used “for security” and to “implement additional features,” such as “packet filtering based on source and destination IP addresses, source and destination port, protocol, QoS, encryption, NAT, etc.”⁸ *Id.* at 25 (emphasis omitted) (citing Ex. 1003 ¶ 85; Ex. 1006, 2:46–57, 3:24–30, 7:29–9:21, Figs. 5A–5E, 10A–10B); *see id.* at 28.

Second, Petitioner asserts that Yip teaches including “data related to . . . physical addresses” in an ACL because Yip discloses that ACLs “were developed to combat cyber-attacks on the LAN Switch by providing an administrator-controlled list of Internet Protocol (IP) addresses or media access control (MAC) addresses that were authorized to access the network.” Pet. 26 (emphasis omitted) (quoting Ex. 1013, 2:43–47) (citing Ex. 1003 ¶¶ 89–90).

Additionally, Petitioner contends that Gai “contemplates that additional ‘message criteria’ may be included in the ACLs.” Pet. 26–27 (citing Ex. 1006, 7:32–34). According to Petitioner, an ordinarily skilled artisan “would have understood that MAC addresses are message criteria (since the Ethernet messages sent and received by Gai’s switch would have contained source and destination MAC addresses) and also that the MAC addresses may be used to provide additional security.” *Id.* at 27.

Third, Petitioner asserts that Kwan teaches “how to automatically learn new IP addresses based on known MAC addresses” because “Kwan discloses that ‘the source IP address can be learned by using a reverse

⁸ The acronym “QoS” stands for “quality of service.” Ex. 1006, 3:29. The acronym “NAT” stands for “Network Address Translation.” *Id.* at 9:15.

address resolution protocol (RARP) which provides for sending out the MAC address on the subnet, and in response the host having the MAC address responds with its IP address.” Pet. 28–29 (quoting Ex. 1007, 5:40–43). Petitioner asserts that Kwan also discloses learning a new IP address “by listening to the DHCP response packet being returned to the host . . . [which] contains the source IP Address for the host.” *Id.* at 29 (alterations by Petitioner) (quoting Ex. 1007, 5:45–46).

Fourth, Petitioner asserts that “because Gai’s TCAM ACL is generated based on the text-based ACLs (which in the proposed combination would include MAC addresses), the TCAM ACL would also include both MAC and IP addresses, analogous to Kwan.” Pet. 30 (citing Ex. 1007, 4:34–39, 5:64–67).

Fifth, Petitioner asserts that “Kwan discloses that the system administrator provides seed IP address properties” representing “data (text data such as IP subnet) that is used to restrict access to the network such that only IP addresses consistent with the seed IP address properties will be learned and permitted to communicate on the network.” Pet. 30 (citing Ex. 1007, 6:14–25).

Sixth, Petitioner asserts that it would have been obvious “in view of Kwan” to “include seed IP address properties in Gai’s administrator-created text-based ACLs, to beneficially reduce or ‘eliminate false learning’ in certain instances” and “beneficially help avoid spoofing.” Pet. 31 (quoting Ex. 1007, 6:22–23).

Therefore, according to Petitioner, “Gai in combination with Yip and Kwan discloses creating one or more text-based ACLs that include MAC

addresses and seed IP address properties, which renders obvious”
limitation 1.1. Pet. 32 (citing Ex. 1003 ¶ 104).

Patent Owner disputes that an ordinarily skilled artisan would have been motivated to combine the teachings of Gai, Yip, and Kwan to yield claim 1’s “enhanced access control list” limitation. Resp. 19; *see* Sur-reply 2–13. Patent Owner makes no other arguments specific to limitation 1.1. *See, e.g.*, Resp. 6–20; Sur-reply 2–13.

For the reasons stated by Petitioner and supported by Dr. Crovella’s testimony, we agree with Petitioner that the combined disclosures in Gai, Yip, and Kwan teach limitation 1.1. *See* Pet. 25–32; Ex. 1003 ¶¶ 83–104. For the reasons discussed above, we consider Patent Owner’s motivation-to-combine arguments unavailing. *See supra* § III.D.4(c); Resp. 19.

(c) Limitations 1.2.1–1.2.4

Claim 1 recites:

[1.2.1] converting, in a network switch, at least one of:

[1.2.2] user names into corresponding IP and physical addresses according to data in the enhanced access control list, wherein converting user names into corresponding IP and physical addresses according to data in the enhanced access control list includes:

detecting login packets being communicated over the network;

determining a MAC address from the login packets;

detecting server message block login packets being communicated over the network;

determining an IP address from the server message block login packets; and

developing records in the access control list
using the obtained IP address for the respective
user name;

[1.2.3] DNS names into corresponding IP
addresses according to data in the enhanced access
control list; and

[1.2.4] physical addresses into IP addresses
according to data in the enhanced access control list.

Ex. 1001, 10:17–35 (limitations 1.2.1–1.2.4).

Petitioner contends that the combined disclosures in Gai, Yip, and Kwan teach limitations 1.2.1 and 1.2.4, i.e., “converting, in a network switch, . . . physical addresses into IP addresses according to data in the enhanced access control list,” for several related reasons. *See* Pet. 32–39. First, Petitioner asserts that Gai teaches “a network switch” because Gai discloses intermediate network device 316 with circuitry for performing “switching functions” in computer network 300. *Id.* at 32 (citing Ex. 1006, 5:22–34, 6:62–65).

Second, Petitioner asserts that Kwan discloses two techniques for “converting, in a network switch, . . . physical addresses into IP addresses” as follows:

- (1) converting using the DHCP technique; and
- (2) converting using the RARP technique.

See Pet. 36–38.

Regarding the DHCP technique, Petitioner contends that “Kwan discloses listening to DHCP response packets to learn new IP addresses according to MAC addresses.” Pet. 36. Regarding the RARP technique, Petitioner contends that “Kwan discloses that ‘the source IP address can be learned by using a reverse address resolution protocol (RARP) which

provides for sending out the MAC address on the subnet, and in response the host having the MAC address responds with its IP address.” *Id.* at 37 (quoting Ex. 1007, 5:40–43).

Third, Petitioner asserts that an ordinarily skilled artisan would have implemented the proposed combination such that Gai’s intermediate network device 316 “converts physical addresses of devices on the network into new IP addresses according to data (e.g., known MAC addresses and seed IP address properties)” that “in the proposed combination would be included in one or more text-based ACLs” corresponding to the claimed “enhanced access control list.” Pet. 38–39 (citing Ex. 1003 ¶ 122).

Therefore, according to Petitioner, “Gai in combination with Yip and Kwan” discloses “converting in the network device 316 physical addresses of devices on the network into IP addresses (e.g., using a DHCP technique or a RARP technique) according to data (e.g., known MAC addresses and seed IP address) in one or more text-based ACLs, which renders obvious” limitations 1.2.1 and 1.2.4. Pet. 39 (citing Ex. 1003 ¶ 123).

Patent Owner makes no arguments specific to limitations 1.2.1 and 1.2.4. *See, e.g.*, Resp. 6–20; Sur-reply 2–13.

For the reasons stated by Petitioner and supported by Dr. Crovella’s testimony, we agree with Petitioner that the combined disclosures in Gai, Yip, and Kwan teach limitations 1.2.1 and 1.2.4. *See* Pet. 32–39; Ex. 1003 ¶¶ 105–123.

(d) Limitation 1.3

Claim 1 recites “developing, in the network switch, the access control list from each of the operations of converting.” Ex. 1001, 10:36–37 (limitation 1.3).

Petitioner contends that the combined disclosures in Gai, Yip, and Kwan teach limitation 1.3 for several related reasons. *See* Pet. 39–42. First, Petitioner asserts that “Kwan discloses that once a new IP address has been successfully learned (e.g., using a DHCP technique or a RARP technique), the learned IP address is ‘loaded into the table.’” *Id.* at 40 (emphasis omitted) (quoting Ex. 1007, 5:50). According to Petitioner, Kwan’s “table is embodied as an access control list, which are data fields, included in a content addressable memory 240, which is referred to as an ACL-CAM.” *Id.* (emphases omitted) (quoting Ex. 1007, 4:36–39).

Second, Petitioner asserts that an ordinarily skilled artisan would have recognized that Kwan’s ACL-CAM “is a specialized memory circuit that is designed to allow its entire contents to be searched for a matching value all at once and, consequently, very fast.” Pet. 40 (citing Ex. 1007, 4:35–39).

Third, Petitioner asserts that an ordinarily skilled artisan “implementing Kwan’s DHCP or RARP techniques in the combination with Gai” would have found it obvious to “update Gai’s TCAM ACL with the new IP address once learned” so that Gai’s intermediate network device 316 “would permit packets that have the new IP address.” Pet. 41 (citing Ex. 1006, 18:3–5). According to Petitioner, updating Gai’s TCAM ACL “is consistent with Gai’s recognition that ACLs may be ‘routinely up-dated or changed.’” *Id.* (emphasis omitted) (quoting Ex. 1006, 18:47–48). Further, Petitioner asserts that “Kwan recognizes the importance of updating the ACL-CAM because ‘the source IP addresses assigned for a given host can change over time.’” *Id.* (emphasis omitted) (quoting Ex. 1007, 7:67–8:1).

Fourth, Petitioner asserts that an ordinarily skilled artisan “seeking to update Gai’s TCAM ACL to include newly learned IP addresses (per

Kwan)” would have found it obvious to “first update one or more of Gai’s text-based ACLs to include the new IP addresses, and then to dynamically reoptimize the updated text-based ACLs to generate an updated TCAM ACL that includes the new IP addresses.” Pet. 41–42. According to Petitioner, this processing sequence would allow for Gai’s intermediate network device 316 to apply the optimized TACM ACLs with the new IP addresses to newly received packets. *Id.* at 42.

Therefore, according to Petitioner, “Gai in combination with Yip and Kwan discloses developing a reoptimized TCAM ACL in the network device 31[6] that includes new IP addresses from the operation of converting, which renders obvious” limitation 1.3. Pet. 42 (citing Ex. 1003 ¶ 131).

Patent Owner disputes that an ordinarily skilled artisan would have been motivated to combine the teachings of Gai, Yip, and Kwan to yield claim 1’s “dynamic access control list” limitation. Resp. 19; *see* Sur-reply 2–13; Tr. 22:18–22. Patent Owner makes no other arguments specific to limitation 1.3. *See, e.g.*, Resp. 6–20; Sur-reply 2–13.

For the reasons stated by Petitioner and supported by Dr. Crovella’s testimony, we agree with Petitioner that the combined disclosures in Gai, Yip, and Kwan teach limitation 1.3. *See* Pet. 39–42; Ex. 1003 ¶¶ 124–131. For the reasons discussed above, we consider Patent Owner’s motivation-to-combine arguments unavailing. *See supra* § III.D.4(c); Resp. 19.

(e) Conclusion Concerning Obviousness/Nonobviousness for Claim 1

For the reasons discussed above, the combined disclosures in Gai, Yip, and Kwan teach claim 1’s subject matter. *See supra* §§ III.D.5(a)–(d). Moreover, an ordinarily skilled artisan would have been motivated to

combine the teachings of Gai, Yip, and Kwan in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.D.4(c). Hence, Petitioner has shown by a preponderance of the evidence that claim 1 is unpatentable under § 103(a) because the claim would have been obvious over Gai, Yip, and Kwan.

6. DEPENDENT CLAIM 3

Claim 3 depends directly from claim 1 and specifies that “each physical address comprises a MAC address.” Ex. 1001, 10:42–43.

Petitioner contends that “the combination of Gai, Yip, and Kwan discloses that the text-based ACLs include MAC addresses of devices authorized to access the network,” thus rendering claim 3 obvious. Pet. 42 (citing Ex. 1003 ¶ 132).

Patent Owner disputes that the combined disclosures in Gai, Yip, and Kwan teach claim 3’s subject matter for the same reasons Patent Owner disputes that the combined disclosures teach claim 1’s subject matter. *See, e.g.*, Resp. 6–20; Sur-reply 2–13.

For the reasons stated by Petitioner and supported by Dr. Crovella’s testimony, we agree with Petitioner that the combined disclosures in Gai, Yip, and Kwan teach claim 3’s subject matter. *See* Pet. 42; Ex. 1003 ¶ 132. Moreover, an ordinarily skilled artisan would have been motivated to combine the teachings of Gai, Yip, and Kwan in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.D.4(c). Hence, Petitioner has shown by a preponderance of the evidence that claim 3 is unpatentable under § 103(a) because the claim would have been obvious over Gai, Yip, and Kwan. For the reasons

discussed above, we consider Patent Owner’s arguments regarding claim 1 unavailing. *See supra* § III.D.4(c).

E. Alleged Obviousness over Gai, Yip, Kwan, and Georgiou: Claims 15, 17, and 19–21

Petitioner contends that claims 15, 17, and 19–21 are unpatentable under § 103(a) because the claims would have been obvious over Gai, Yip, Kwan, and Georgiou. *See* Pet. 43–85; Reply 20–26. Patent Owner disputes Petitioner’s contentions. *See* Resp. 21–33; Sur-reply 13–19.

Above, we provided overviews of Gai, Yip, and Kwan. *See supra* §§ III.D.1–III.D.3. Below, we provide an overview of Georgiou. Then, we consider the obviousness issues. For the reasons explained below, we agree with Petitioner that claims 15, 17, and 19–21 are unpatentable under § 103(a) because the claims would have been obvious over Gai, Yip, Kwan, and Georgiou.

1. OVERVIEW OF GEORGIOU (EXHIBIT 1008)

Georgiou is a U.S. patent titled “Dynamic Reallocation of Data Stored in Buffers Based on Packet Size,” filed on July 9, 2003, and issued on February 21, 2006. Ex. 1008, codes (12), (22), (45), (54). Georgiou states that the invention “generally relates to the implementation of computer networks, and more particularly, to a method and apparatus for efficient utilization of memory and reduced memory waste in storing data blocks of network traffic.” *Id.* at 1:8–11; *see id.* at code (57).

Georgiou explains that packets of varying sizes are sent and received in various networks and that “various techniques are used to manage the incoming stream of varying sizes of packets.” Ex. 1008, 1:13–16, 1:20–21. Georgiou also explains that “[t]ypical arrangements include employing some

form of logic, either hardware centric or software centric, to receive and temporarily store the incoming packets in a memory area, e.g., a buffer pool or equivalent, until subsequent processing can access and retrieve the packets, as appropriate, for action on the packet contents.” *Id.* at 1:22–27.

For example, “when packets arrive from the network at an input port, the hardware attached to the port usually communicates this information to a processor which performs routing actions and then passes the processed packet to an output port for delivery to its intended destination.” Ex. 1008, 1:49–54. “The hardware attached to the input port is often a simple” direct memory access (DMA) circuit or controller that “receives the packet, writes it to memory, and then indicates to the controlling processor that a packet has been received.” *Id.* at 1:54–57; *see id.* at 3:42–46.

Georgiou endeavors to provide “a flexible buffer management method and system for efficient utilization of memory and reducing memory waste in storing data blocks (e.g., packets) of network traffic.” Ex. 1008, 3:14–17. In particular, “after reception of a packet from the network interface, the packet is typically temporarily stored in an inbound buffer in the network interface from where it is then transferred to memory to await subsequent processing.” *Id.* at 3:17–22.

Buffer memory includes “two or more portions (i.e., buffer pools) according to packet sizes with buffers allocated in each portion suitable for storing packets according to the packet sizes associated with the portion.” Ex. 1008, 3:22–25. Hence, one portion of buffer memory is used for smaller packet sizes, and another portion of buffer memory is used for larger packet sizes. *Id.* at code (57). “This buffer sizing leads to optimization of memory utilization which is directly related to overhead costs such as memory costs,

speed performance, packet processing reliability, and the like.” *Id.* at 3:57–61.

The “allocation of available memory area is performed dynamically.” Ex. 1008, 5:54–55. Thus, if “the number of available buffers in one set falls under a particular threshold, free memory area from the other set can be reassigned to the first set.” *Id.* at 5:60–63. When reassigning free memory area, “big memory buffers are partitioned into a number of small buffers,” or “multiple small buffers are merged into a larger buffer.” *Id.* at 5:63–66. “This dynamic reassignment of buffers makes [the] system adaptable to sudden network traffic pattern change.” *Id.* at 5:66–67.

2. WHETHER AN ORDINARILY SKILLED ARTISAN WOULD
HAVE BEEN MOTIVATED TO COMBINE THE TEACHINGS OF
THE REFERENCES WITH A REASONABLE EXPECTATION OF SUCCESS

(a) Petitioner’s Contentions

(i) Motivation to Combine

Petitioner contends that an ordinarily skilled artisan would have been motivated to combine Georgiou’s teachings with the teachings of Gai, Yip, and Kwan to “produce predictable and beneficial results,” including improved packet processing. *See* Pet. 44–47, 53, 64, 67–68; Reply 20–22. Specifically, Petitioner asserts that:

- (1) some packets in the proposed Gai-Yip-Kwan combination would be forwarded to “Gai’s CPU for additional processing,” e.g., “learning the new IP address”;
- (2) an ordinarily skilled artisan “would have recognized that in the instance where there are a significant number of packets that need processing, the CPU may not be able to keep up with the packet flow”; and

- (3) Georgiou discloses temporarily storing packets in dynamic memory while awaiting processing, e.g., “until subsequent processing can access and retrieve the packets, as appropriate, for action on the packet contents.”

Pet. 45 (citing Ex. 1003 ¶¶ 138–139; Ex. 1008, 1:22–27, 1:54–57, 3:18–22, 3:42–46, 5:51–67).

Therefore, according to Petitioner, it would have been obvious in view of Georgiou “to implement Gai’s network switch to store packets forwarded to a CPU for additional processing (e.g., encryption, logging, learning IP addresses, etc.) in its dynamic memory.” Pet. 46. Petitioner asserts that temporarily storing packets in Gai’s dynamic memory would beneficially “allow the packets awaiting processing to be retained until the CPU is freed up, thereby facilitating processing of packets (e.g., encrypt, log, learn new IP address, etc.).” *Id.* (citing Ex. 1003 ¶ 140). Petitioner asserts that temporarily storing packets in Gai’s dynamic memory would also beneficially “make more efficient use of Gai’s network bandwidth” by “reduc[ing] the number of packets that need to be retransmitted” due to dropping because the packets are “stored in dynamic memory” instead of “dropped for lack of CPU processing bandwidth.” *Id.* (citing Ex. 1003 ¶ 141); *see id.* at 68 (citing Ex. 1003 ¶ 195; Ex. 1007, 5:22–6:30; Ex. 1008, 9:7–12).

Petitioner explains that in the proposed combination Gai’s forwarding entity 404 would forward most packets to their destinations and “only packets that Gai does not forward” due to a need for additional processing, e.g., encryption, logging, learning IP addresses, etc., “would be stored in

dynamic memory 409, as Georgiou teaches.” Reply 22 (citing Ex. 1006, 1:22–27, 5:51–67, 17:44–48; Ex. 1023 ¶ 17; Pet. 67–68).

Additionally, Petitioner contends that the “combination of Georgiou and Gai (as modified per Yip and Kwan)” is:

- (a) “merely combining prior art elements (storing packets in memory, per Georgiou, with Gai’s dynamic memory) according to known methods (Georgiou describes exemplary methods of implementing the storing of packets in memory, including using a DMA circuit) to yield the predictable result of retaining packets until the CPU has sufficient bandwidth to process the packets”; and
- (b) “the use of a known technique (storing packets that await processing in memory, per Georgiou) to improve a similar system (Gai’s network device) in the same way, including (1) retaining the packets until CPU has sufficient bandwidth to process the packets, (2) facilitate processing of packets and (3) conserving network bandwidth by avoiding packet retransmission.”

Pet. 46–47 (citing Ex. 1003 ¶¶ 142–143).

(ii) Reasonable Expectation of Success

Petitioner asserts that an ordinarily skilled artisan would have had a reasonable expectation of success in combining Georgiou’s teachings with the teachings of Gai, Yip, and Kwan given “the similarity in Georgiou’s and Gai’s systems.” Pet. 47. Petitioner also asserts that any modification of Gai needed to accommodate Georgiou’s teachings “would have been a conventional and simple implementation and well within the level of one of ordinary skill in the art.” *Id.* (citing Ex. 1003 ¶¶ 145–146; Ex. 1008, 1:54–57; Ex. 1009, 1:32–34; Ex. 1010 ¶ 216; Ex. 1011, 11:43–45; Ex. 1012, code (57)).

Additionally, Petitioner explains that using a DMA circuit or controller and dynamic memory as Georgiou teaches “was well known in the art and such well known devices would add minimal complexity to Gai’s system that already has dynamic memory 409.” Reply 22 (citing Ex. 1023 ¶ 17).

(b) Patent Owner’s Contentions

(i) Motivation to Combine

Patent Owner contends that an ordinarily skilled artisan considering Petitioner’s proposed combination “would instantly note that the reliance on dynamic memory to store packets would bottleneck the system greatly within a relatively fast time frame as packets fill up the dynamic memory and slow down the stream of data to a crawl during filtering processes.” Resp. 25; *see id.* at 24. Patent Owner also contends that “Petitioner does not show where or how inbound packets would be temporarily stored in Petitioner’s proposed combination.” Sur-reply 14.

Patent Owner asserts that temporarily storing packets in dynamic memory “would lead to further network inefficiencies as the flow of packets would still outpace processing capabilities, meaning that there would be a net increase in the overall number of packets over time, regardless of how many packets can be redirected to dynamic memory.” Resp. 25 (citing Ex. 2001 ¶ 83). Patent Owner also asserts that temporarily storing packets in dynamic memory “would be incompatible with Gai’s goal of higher switching speeds and faster processing of messages.” *Id.* at 26 (citing Ex. 2001 ¶ 94).

(ii) Reasonable Expectation of Success

Patent Owner contends that an ordinarily skilled artisan would have viewed “a combination of switch hardware storing packets and storing packets in the CPU as an unrealistic and impractical goal to implement in the network.” Resp. 25–26 (citing Ex. 2001 ¶ 83). According to Patent Owner, “implementing this process would be extremely costly and inefficient, as well as conceptually incompatible with the typical methods of switch hardware to forward packets at the highest sustainable rate as designed.” *Id.* at 25 (citing Ex. 2001 ¶ 83).

(c) Analysis

(i) Motivation to Combine

For the reasons explained below, we agree with Petitioner that an ordinarily skilled artisan would have been motivated to combine Georgiou’s teachings with the teachings of Gai, Yip, and Kwan in the way Petitioner proposes. *See* Pet. 44–47, 53, 64, 67–68; Reply 20–22; Ex. 1003 ¶¶ 51–58, 62–72, 91–92, 98, 101, 121, 135–144, 157, 186, 194–195; Ex. 1023 ¶ 17.

First, Gai discloses forwarding some packets to the “CPU for additional processing (e.g., encryption, logging, etc.).” Ex. 1006, 13:41–44; *see id.* at 4:29–37, 12:2–7, 17:44–48; Ex. 1003 ¶¶ 138, 154. “In particular, upon receipt of a packet at a first interface, a forwarding entity at the intermediate network device tests the packet against the single, unified ACL stored in the corresponding portion of the CAM.” Ex. 1006, 4:29–32; *see* Ex. 1003 ¶ 161. “When a match is obtained, the corresponding decision is returned to the forwarding entity, which then takes the appropriate action (e.g., forward, discard, log and forward, transfer to CPU for additional processing, etc.).” Ex. 1006, 4:32–37; *see id.* at 17:40–48; Ex. 1003 ¶ 161.

Second, an ordinarily skilled artisan “would have recognized that in the instance where there are significant number of packets that need processing (e.g., encryption, logging, learning new IP address, etc.), the CPU may not be able to keep up with the packet flow.” Ex. 1003 ¶ 138.

Third, Georgiou discloses temporarily storing packets in dynamic memory while awaiting processing, e.g., “until subsequent processing can access and retrieve the packets, as appropriate, for action on the packet contents.” Ex. 1008, 1:22–27, 3:17–22, 3:42–46, 5:51–67; *see* Ex. 1003 ¶¶ 133, 139, 194. For instance, a “simple” DMA controller may “receive[] the packet, write[] it to memory, and then indicate[] to the controlling processor that a packet has been received.” Ex. 1008, 1:54–57; *see id.* at 3:42–46; Ex. 1003 ¶¶ 133–134, 139. The “allocation of available memory area is performed dynamically” to make the system “adaptable” to changes. Ex. 1008, 5:54–55, 5:66–67.

Fourth, Georgiou’s dynamic memory is analogous to Gai’s dynamic memory 409. Ex. 1003 ¶ 195.

Fifth, an ordinarily skilled artisan would have recognized that temporarily storing packets in Gai’s dynamic memory 409 would beneficially “allow the packets awaiting processing to be retained until the CPU is freed up, thereby facilitating processing of packets (e.g., encrypt, log, learn new IP address, etc.).” Ex. 1003 ¶ 140. A skilled artisan would have recognized that temporarily storing packets in Gai’s dynamic memory 409 would also beneficially “make more efficient use of Gai’s network bandwidth” by “reduc[ing] the number of packets that need to be retransmitted” due to dropping because the packets are “stored in dynamic memory” instead of “dropped for lack of CPU processing bandwidth.” *Id.*

¶ 141. Temporarily storing packets in Gai’s dynamic memory 409 “would allow for CPU 406 to access and retrieve the stored packets, as appropriate, and take action on the packet contents (e.g., encrypt, learn new IP address, dynamically generate updated BDD ACLs, etc.), without dropping packets for lack of processing bandwidth.” *Id.* ¶ 195.

Sixth, Petitioner explains that in the proposed combination Gai’s forwarding entity 404 would forward most packets to their destinations and “only packets that Gai does not forward” due to a need for additional processing, e.g., encryption, logging, learning IP addresses, etc., “would be stored in dynamic memory 409, as Georgiou teaches.” *See* Reply 22; Ex. 1003 ¶ 140; Ex. 1023 ¶ 17. Hence, “in the proposed combination only a small number of packets (e.g., packets that need additional processing by CPU 406) are stored in the dynamic memory 409 and the majority of packets are forwarded by the forwarding entity 404 to the various interfaces” of Gai’s intermediate network device 316. Ex. 1023 ¶ 17.

Seventh, because “only a small number of packets (e.g., packets that need additional processing by CPU 406) are stored in the dynamic memory 409” in the proposed combination, we disagree with Patent Owner that “the flow of packets would still outpace processing capabilities, meaning that there would be a net increase in the overall number of packets over time, regardless of how many packets can be redirected to dynamic memory.” *See* Resp. 25; Ex. 1023 ¶ 17.

Eighth, we disagree with Patent Owner that temporarily storing packets in Gai’s dynamic memory 409 “would be incompatible with Gai’s goal of higher switching speeds and faster processing of messages.” *See* Resp. 26. Gai discloses forwarding some packets to the “CPU for additional

processing (e.g., encryption, logging, etc.).” Ex. 1006, 13:41–44; *see id.* at 4:29–37, 12:2–7, 17:44–48; Ex. 1003 ¶¶ 138, 154. So additional processing of some packets by the CPU does not conflict with Gai’s objective “to achieve much higher switching speeds than the prior art devices.” *See* Ex. 1006, 17:63–65; Ex. 1023 ¶ 17.

Further, “the benefits, both lost and gained, should be weighed against one another” for a proposed combination. *Winner Int’l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 n.8 (Fed. Cir. 2000). Here, an ordinarily skilled artisan would have recognized that temporarily storing packets in Gai’s dynamic memory 409 would beneficially:

- (1) “allow the packets awaiting processing to be retained until the CPU is freed up, thereby facilitating processing of packets”; and
- (2) “make more efficient use of Gai’s network bandwidth” by “reduc[ing] the number of packets that need to be retransmitted” due to dropping because the packets are “stored in dynamic memory” instead of “dropped for lack of CPU processing bandwidth.”

Ex. 1003 ¶¶ 140–141. These benefits outweigh the minimal delay due to temporary storage of a small number of packets not immediately forwarded to their destinations. Ex. 1023 ¶ 17; *see* Ex. 1003 ¶¶ 140–141.

Ninth, “[t]here is a motivation to combine when a known 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 ‘prior art elements according to their established functions.’” *Intel*, 61 F.4th at 1380–81. Here, Petitioner identifies Georgiou’s known technique for temporarily storing packets in dynamic memory while awaiting processing used to improve packet processing in network devices

that would improve packet processing in Gai's network device when used according to the known techniques. *See* Pet. 47; Reply 22; Ex. 1003 ¶ 143; Ex. 1008, 1:22–27, 3:17–22, 3:42–46, 5:51–67.

For the reasons discussed above, an ordinarily skilled artisan would have been motivated to combine Georgiou's teachings with the teachings of Gai, Yip, and Kwan in the way Petitioner proposes, and Patent Owner's contentions to the contrary lack merit.

(ii) Reasonable Expectation of Success

As Petitioner asserts, any modification of Gai needed to accommodate Georgiou's teachings "would have been a conventional and simple implementation and well within the level of one of ordinary skill in the art" given "the similarity in Georgiou's and Gai's systems." Ex. 1003 ¶¶ 145–146; *see* Ex. 1008, 1:54–57; Ex. 1009, 1:32–34; Ex. 1010 ¶ 216; Ex. 1011, 11:43–45; Ex. 1012, code (57); Ex. 1023 ¶ 17; Pet. 47. For instance, using a DMA circuit or controller and dynamic memory as Georgiou teaches "was well known in the art and such well known devices would add minimal complexity to Gai's system that already has dynamic memory 409." Ex. 1023 ¶ 17; *see* Ex. 1008, 1:54–57; Ex. 1009, 1:32–34; Ex. 1010 ¶ 216; Ex. 1011, 11:43–45; Ex. 1012, code (57).

Also, because using "such well known devices would add minimal complexity to Gai's system that already has dynamic memory 409," we disagree with Patent Owner that the proposed combination would have been "extremely costly and inefficient." *See* Resp. 25; Ex. 1023 ¶ 17.

3. INDEPENDENT CLAIM 15

(a) Preamble 15.0

Claim 15 recites in its preamble “[a] network switching circuit.”
Ex. 1001, 11:57.

Petitioner contends that Gai teaches claim 15’s preamble because Gai discloses intermediate network device 316 with circuitry for performing “switching functions” in computer network 300. Pet. 48 (emphasis omitted) (citing Ex. 1003 ¶ 147; Ex. 1006, 5:3–59, 6:27–65); *see id.* at 32.

Patent Owner makes no arguments specific to claim 15’s preamble. *See, e.g.*, Resp. 21–33; Sur-reply 13–19. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Generally, a preamble does not limit a claim. *Allen Eng’g*, 299 F.3d at 1346. We need not decide whether claim 15’s preamble limits the claim because, for the reasons stated by Petitioner and supported by Dr. Crovella’s testimony, we agree with Petitioner that Gai teaches claim 15’s preamble. *See* Pet. 48–49; Ex. 1003 ¶¶ 76–82.

(b) Limitations 15.1.1–15.1.5

Claim 15 recites:

[15.1.1] a forwarding circuit operable to detect specific received packets and [15.1.2] to provide the specific packets on a processor port, and [15.1.3] further operable to receive packets on one of a plurality of ports including the processor port [15.1.4] and to forward each received packet to a port corresponding to a destination address contained in the packet [15.1.5] subject to access restrictions contained in a dynamic access control list.

Ex. 1001, 11:58–12:3 (limitations 15.1.1–15.1.5).

Petitioner contends that the combined disclosures in Gai, Yip, and Kwan teach limitations 15.1.1–15.1.5 for several related reasons. *See* Pet. 49–65. First, Petitioner asserts that Gai teaches “a forwarding circuit” because Gai’s intermediate network device 316 includes forwarding entity 404. *Id.* at 49–50 (citing Ex. 1003 ¶¶ 150–151; Ex. 1006, 3:37–40, 6:18–30, 8:26–27, 17:58–63).

Second, Petitioner asserts that “Gai in combination with Kwan” teaches “a forwarding circuit operable to detect specific received packets” (limitation 15.1.1) because:

- (1) Gai’s forwarding entity 404 is configured to “forward or switch network messages” corresponding to “received packets” communicated over computer network 300;
- (2) Gai’s forwarding entity 404 utilizes “a TCAM ACL to identify specific received packets that need additional processing (e.g., packets that should be encrypted, logged, etc.)”;
- (3) Kwan’s network device 200 includes “an access control list, which are data fields, included in a content addressable memory 240,” i.e., ACL-CAM 240; and
- (4) Kwan’s ACL-CAM 240 contains “source IP address and MAC address pairs” used to (a) “identify specific received packets that have a new IP address that has not been learned” and (b) “dynamically learn the new IP addresses based on the MAC addresses.”

Pet. 50–52 (citing Ex. 1003 ¶¶ 153–156; Ex. 1006, 1:37–2:41, 4:41–42, 5:3–59, 5:66–6:12, 6:27–30, 7:32–34, 9:27–31, 11:60–12:7, 13:3–45; Ex. 1007, 4:34–48, 5:25–30, 5:38–67, 6:28–67, 7:61–66, 8:17–51, Fig. 3) (emphasis omitted).

Third, Petitioner asserts that “Gai in combination with Kwan” teaches “operable . . . to provide the specific packets on a processor port” (limitation 15.1.2) because:

- (1) Gai’s intermediate network device 316 includes CPU 406;
- (2) Gai’s forwarding entity 404 provides some packets to a port of CPU 406 for additional processing, e.g., to perform encryption or for logging; and
- (3) “Kwan discloses that if a packet has a new IP address, a source IP address detector 236 of a port security processor 242 is used to learn the new IP address.”

Pet. 53–55 (citing Ex. 1003 ¶¶ 159–163; Ex. 1006, 4:29–37, 7:34–43, 11:60–12:7, Fig. 4; Ex. 1007, 5:38–67, 8:17–47, Fig. 3). According to Petitioner, “Gai in combination with Kwan discloses that forwarding entity 404 identifies specific received packets that need additional processing (e.g., encrypted, logged, etc., and packets that have a new IP address that has not been learned).” *Id.* at 53 (citing Ex. 1003 ¶¶ 159–160).

Fourth, Petitioner asserts that “Gai in combination with Kwan” teaches “further operable to receive packets on one of a plurality of ports including the processor port” (limitation 15.1.3) because:

- (1) “Gai’s forwarding entity 404 receives IP messages (packets) on a plurality of interfaces 402a–e corresponding to ports”;
- (2) “in the combination of Gai and Kwan the forwarding entity 404 forwards to the CPU 406 specific packets”;
- (3) “[i]t would have been obvious to” an ordinarily skilled artisan “for Gai’s CPU 406 to send the packets back to the forwarding entity 404 as appropriate,” e.g., after encryption to output on a port and transmit to a destination; and

- (4) “Kwan’s packets with a new IP address are disclosed as being sent to the destination after successfully learning the IP address.”

Pet. 56–60 (citing Ex. 1003 ¶¶ 166–197; Ex. 1006, 1:37–2:41, 4:41–42, 5:14–22, 6:27–30, 7:66–8:6, 8:36–55, 16:63–17:6, Fig. 4; Ex. 1007, 5:30–36, 8:43–55, Fig. 3).

Fifth, Petitioner asserts that Gai teaches “further operable . . . to forward each received packet to a port corresponding to a destination address contained in the packet” (limitation 15.1.4) because “Gai’s forwarding entity 404 is configured to forward each incoming packet to an output port corresponding to an IP destination address extracted from the packet.” Pet. 60–62 (citing Ex. 1003 ¶¶ 114, 174–175, 177–179; Ex. 1006, 5:60–66, 6:27–30, 19:6–14, Fig. 4). According to Petitioner, an ordinarily skilled artisan “would have understood that the forwarding entity 404 selects an interface and associated port for forwarding based on the destination address contained in the message (e.g., packet), as was common in the art.” *Id.* at 61 (citing Ex. 1003 ¶ 176; Ex. 1007, 1:52–61, 2:1–51, 3:53–4:6; Ex. 1008, 1:49–54).

Sixth, Petitioner asserts that “Gai in combination with Yip and Kwan” teaches “subject to access restrictions contained in a dynamic access control list” (limitation 15.1.5) because:

- (1) the combined disclosures in the references teach the claimed “dynamic access control list” for the reasons discussed for claim 1’s preamble and limitation 1.3;
- (2) Gai’s forwarding entity 404 uses a TCAM ACL “to determine if access should be restricted (e.g., ‘deny’) or if forwarding is permitted (‘permit’)”; and

- (3) Kwan discloses “an access control list, which are data fields, included in a content addressable memory 240, which is referred to as an ACL-CAM . . . [to] control access and switching through the ports.”

Pet. 63–65 (alterations by Petitioner) (emphases omitted) (citing Ex. 1003 ¶¶ 180–187; Ex. 1006, 4:26–30, 7:24–39, 8:7–27, 9:31–36, 17:28–48, Figs. 5A–5E, 8, 10A–10B, 11; Ex. 1007, 4:34–48, 4:56–63, 7:61–66, 8:14–46, 9:4–16, code (57), Figs. 3–4).

Patent Owner makes no arguments specific to limitations 15.1.1–15.1.5. *See, e.g.*, Resp. 21–33; Sur-reply 13–19.

For the reasons stated by Petitioner and supported by Dr. Crovella’s testimony, we agree with Petitioner that the combined disclosures in Gai, Yip, and Kwan teach limitations 15.1.1–15.1.5. *See* Pet. 49–65; Ex. 1003 ¶¶ 150–187.

(c) Limitations 15.2.1–15.2.4

Claim 15 recites:

[15.2.1] a memory circuit coupled to the forwarding circuit, [15.2.2] the memory circuit operable to store packets and [15.2.3] operable to store an enhanced access control list and [15.2.4] a dynamic access control list.

Ex. 1001, 12:4–7 (limitations 15.2.1–15.2.4).

(i) Petitioner’s Contentions

Petitioner contends that the combined disclosures in Gai, Yip, Kwan, and Georgiou teach limitations 15.2.1–15.2.4 for several related reasons. *See* Pet. 65–69; Reply 23–26. First, Petitioner asserts that Gai teaches “a memory circuit” because Gai’s intermediate network device 316 includes NVRAM 408, dynamic memory 409, and TCAM 410 that collectively correspond to “a memory circuit.” *See* Pet. 65–67; Reply 23; Tr. 42:20–25.

Petitioner asserts that “the use of ‘a’ or ‘an’ in an open-ended ‘comprising’ claim connotes ‘one or more.’” Reply 24 (citing *Celgene Corp. v. Peter*, 931 F.3d 1342, 1350 (Fed. Cir. 2019)).

Second, Petitioner asserts that Gai teaches “a memory circuit coupled to the forwarding circuit” (limitation 15.2.1) because Gai’s intermediate network device 316 includes forwarding entity 404 (i) directly coupled to TCAM 410 and (ii) indirectly coupled to NVRAM 408 and dynamic memory 409 via CPU 406. Pet. 65–66 (citing Ex. 1003 ¶¶ 188–191; Ex. 1006, 5:65–6:30, Fig. 4); *see id.* at 67 (citing Ex. 1003 ¶ 191).

As support, Petitioner provides the following highlighted and annotated version of Gai’s Figure 4 (Pet. 66):

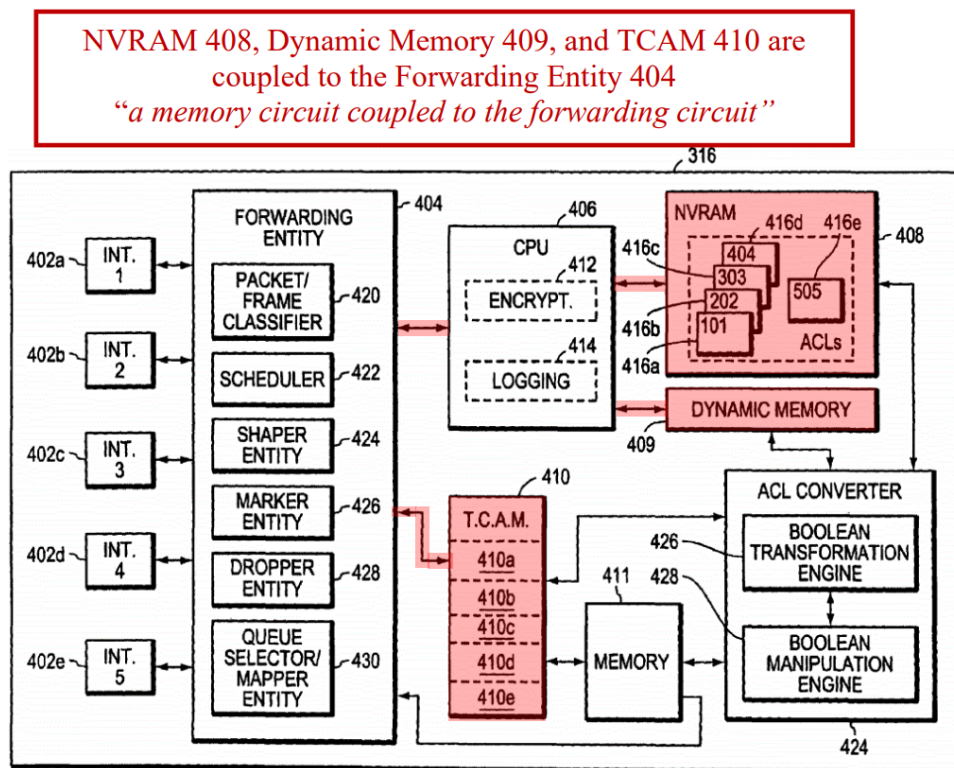


FIG. 4

Figure 4 illustrates intermediate network device 316 including, among other things, forwarding entity 404, CPU 406, NVRAM 408, dynamic

memory 409, TCAM 410, memory 411, and ACL converter 424. Ex. 1006, 4:52–54, 5:60–6:12, 6:36–41, Fig. 4. The above highlighted and annotated version of Figure 4 includes:

- (1) red highlighting over NVRAM 408, dynamic memory 409, and TCAM 410;
- (2) red highlighting over the bidirectional path between forwarding entity 404 and CPU 406;
- (3) red highlighting over the bidirectional path between CPU 406 and NVRAM 408;
- (4) red highlighting over the bidirectional path between CPU 406 and dynamic memory 409;
- (5) red highlighting over the bidirectional path between forwarding entity 404 and TCAM 410; and
- (6) the red annotation “NVRAM 408, Dynamic Memory 409, and TCAM 410 are coupled to the Forwarding Entity 404 ‘*a memory circuit coupled to the forwarding circuit.*’”

See Pet. 66; Ex. 1003 ¶ 189.

According to Petitioner, an ordinarily skilled artisan would have understood that both NVRAM 408 and dynamic memory 409 are coupled to forwarding entity 404 because both NVRAM 408 and dynamic memory 409 are coupled to CPU 406 and CPU 406 is coupled to forwarding entity 404. Pet. 66.

Third, Petitioner asserts that “Gai in combination with Georgiou” teaches “the memory circuit operable to store packets” (limitation 15.2.2) because:

- (1) Gai’s intermediate network device 316 includes dynamic memory 409 as part of the claimed “memory circuit”;
- (2) “Georgiou’s memory is dynamic memory”; and

- (3) Georgiou discloses that “[t]ypical arrangements include . . . receive and temporarily store the incoming packets in a memory . . . until subsequent processing can access and retrieve the packets, as appropriate, for action on the packet contents.”

Pet. 67–68 (alterations by Petitioner) (emphasis omitted) (quoting Ex. 1008, 1:22–27) (citing Ex. 1003 ¶¶ 192–194; Ex. 1008, 1:13–21, 3:17–22, 5:51–67).

According to Petitioner, “it would have been obvious to” an ordinarily skilled artisan in view of Georgiou “to store in Gai’s dynamic memory 409 (analogous to the dynamic memory of Georgiou) packets forwarded to CPU 406 for processing, until CPU 406 has sufficient processing bandwidth.” Pet. 67–68.

Fourth, Petitioner asserts that “Gai in combination with Yip and Kwan” teaches “the memory circuit . . . operable to store an enhanced access control list” (limitation 15.2.3) because:

- (1) the combined disclosures in the references teach the claimed “enhanced access control list” for the reasons discussed for limitation 1.1;
- (2) Gai’s intermediate network device 316 includes NVRAM 408 as part of the claimed “memory circuit”; and
- (3) Gai discloses NVRAM 408 as operable to store “administrator generated text-based ACLs (including MAC addresses and seed IP address properties)” that correspond to the claimed “enhanced access control list.”

Pet. 68–69 (emphasis omitted) (citing Ex. 1003 ¶¶ 197–200; Ex. 1006, 2:58–65, 4:8–13, 6:13–18, 7:15–8:6, 9:18–25); *see* Reply 23.

Fifth, Petitioner asserts that “Gai in combination with Yip and Kwan” teaches “the memory circuit . . . operable to store . . . a dynamic access control list” (limitation 15.2.4) because:

- (1) the combined disclosures in the references teach the claimed “dynamic access control list” for the reasons discussed for claim 1’s preamble and limitation 1.3;
- (2) Gai’s intermediate network device 316 includes TCAM 410 as part of the claimed “memory circuit”; and
- (3) Gai discloses TCAM 410 as operable to store dynamically generated and optimized “versions of the ACLs” that correspond to the claimed “dynamic access control list.”

Pet. 69 (emphasis omitted) (citing Ex. 1003 ¶¶ 201–204; Ex. 1006, 4:26–29, 20:65–67); *see* Reply 23.

Sixth, Petitioner asserts that the ’518 patent’s specification does not require “a single memory circuit” that stores “packets, enhanced control lists, and dynamic control lists.” Reply 24 (emphasis omitted). As support, Petitioner cites the following disclosure in the specification:

The selected packets are stored in the packet memory 306 for processing by the processor 302. Also stored in either the packet memory 306 or memory in the processor 302 is the enhanced access control list 108 (FIG. 2) along with required programming instructions for execution by the processor to control the overall operation of the switch 102.

Id. (citing Ex. 1001, 9:31–36). According to Petitioner, an ordinarily skilled artisan would not understand claim 15 to require “a single memory circuit” in view of the specification. *Id.* at 25 (citing Ex. 1023 ¶ 18).

(ii) Patent Owner’s Contentions

Patent Owner disputes that the combined disclosures in Gai, Yip, Kwan, and Georgiou teach limitations 15.2.1–15.2.4. *See* Resp. 28–33;

Sur-reply 14–19. Regarding the word “a” in the phrase “a memory circuit,” Patent Owner asserts that the “claims and the written description make clear that the singular meaning applies” instead of the “general rule that ‘a’ or ‘an’ in a patent claim carries the meaning of ‘one or more.’” Sur-reply 14–15 (citing *Tivo, Inc. v. EchoStar Commc’ns Corp.*, 516 F.3d 1290, 1303 (Fed. Cir. 2008); *Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1344 (Fed. Cir. 2008)).

As support, Patent Owner provides the following highlighted version of the ’518 patent’s Figure 3 (Sur-reply 15):

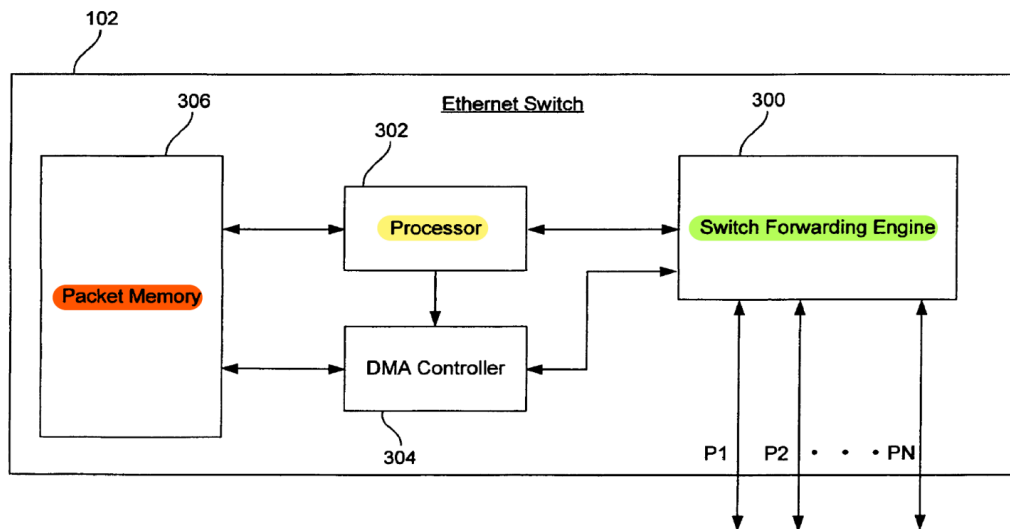


FIG. 3

Figure 3 illustrates Ethernet switch 102 including switch forwarding engine 300, processor 302, DMA controller 304, and packet memory 306. Ex. 1001, 9:9–19, 9:28–30, Fig. 3. The above highlighted version of Figure 3 includes green highlighting over switch forwarding engine 300, yellow highlighting over processor 302, and red highlighting over packet memory 306. See Sur-reply 15. According to Patent Owner, packet memory 306 corresponds to the claimed “memory circuit.” *Id.*; see Tr. 32:21–23.

As further support, Patent Owner quotes the following disclosure in the '518 patent:

The switch 102 further includes a direct memory access (DMA) controller 304 that transfers the packets selected by the switch forwarding engine 300 to a packet memory 306. The selected packets are stored in the packet memory 306 for processing by the processor 302. Also stored in either the packet memory 306 or memory in the processor 302 is the enhanced access control list 108 (FIG. 2) along with required programming instructions for execution by the processor to control the overall operation of the switch 102. To store a selected packet from the switch forwarding engine 300, the processor 302 programs required registers in the DMA controller 304. The switch forwarding engine 300 then supplies the packet to the DMA controller 304 which, in turn, stores the packet in the packet memory 306. The processor 302 accesses the stored packets in the packet memory 306 along with the stored enhanced access control list 108 (FIG. 2) to generate the dynamic access control list 104 (FIG. 2).

Sur-reply 16 (quoting Ex. 1001, 9:28–44).

Patent Owner asserts that the claimed “memory circuit” was “emphasized” during the '518 patent’s prosecution because the applicant distinguished a cited reference by arguing that the reference:

- (1) “does not disclose or suggest a memory circuit in a network switching circuit that is operable to store an enhanced access control list and a dynamic access control list”; and
- (2) “does not disclose or suggest a memory circuit in a network switching circuit that stores an enhance[d] access control list and a dynamic access control list.”

Sur-reply 17–18 (quoting Ex. 1002, 102, 141) (citing Ex. 1002, 104, 142).

Therefore, according to Patent Owner, “the specification, claims, and prosecution history all show that ‘a’ memory circuit should be construed as a single memory circuit.” Sur-reply 18.

Further, Patent Owner asserts that Petitioner identifies “four separate circuits in Gai” (NVRAM 408, dynamic memory 409, TCAM 410, and memory 411 coupled to TCAM 410) as corresponding to the claimed “a memory circuit.” Resp. 28–29 (emphasis omitted); *see* Sur-reply 18–19. Patent Owner asserts that “four different memory circuits (or devices)” do not “correspond to a single memory circuit” as required by claim 15. Resp. 30 (emphasis omitted).

Patent Owner also asserts that even if an ordinarily skilled artisan “would have considered adding an additional DMA circuit operable to store packets,” as Petitioner proposes based on Georgiou’s teachings, the “resulting quintet of circuits would not have corresponded to” the claimed “a memory circuit,” i.e., “a single memory circuit.” Resp. 32 (emphasis omitted) (citing Ex. 2001 ¶ 101); Sur-reply 19.

Additionally, Patent Owner contends that “Gai does not disclose or teach a memory circuit operable to store packets.” Resp. 32 (citing Ex. 1006, 6:27–31, 16:67–17:1; Ex. 2001 ¶ 101); *see* Sur-reply 19. According to Patent Owner, an ordinarily skilled artisan would have understood that:

- (1) “transient packets would not be stored in non-volatile RAM (NVRAM)”;
- (2) “transient packets would not be stored in ternary content addressable memory (TCAM)”;

- (3) TCAM 410 and its associated memory 411 are not “operable to store packets and operable to store an enhanced access control list”; and
- (4) “the different types of memory in Gai – non-volatile RAM, dynamic memory, and content addressable memory – could not be combined into a single memory circuit operable to store packets, enhanced control lists, and dynamic control lists.”

Resp. 30–31 (citing Ex. 2001 ¶¶ 92, 98–99); Sur-reply 19.

Patent Owner asserts that Gai describes ACL converter 424 as “operatively coupled” to NVRAM 408, dynamic memory 409, and TCAM 410 and its associated memory 411. Resp. 31 (citing Ex. 1006, 6:36–41). Patent Owner asserts that an ordinarily skilled artisan “would have recognized that an ACL converter does not correspond to either the claimed processor or forwarding circuit” and “would therefore not couple the memory to either the processor or the forwarding circuit.” *Id.* at 31–32 (citing Ex. 2001 ¶ 100).

Patent Owner also disputes that an ordinarily skilled artisan would have been motivated to combine the teachings of Gai, Yip, Kwan, and Georgiou to yield claim 15’s “dynamic access control list” limitation. Resp. 22.

(iii) Analysis

For the reasons explained below, we agree with Petitioner that the combined disclosures in Gai, Yip, Kwan, and Georgiou teach limitations 15.2.1–15.2.4. *See* Pet. 65–69; Reply 23–26; Ex. 1003 ¶¶ 188–204; Ex. 1023 ¶ 18. First, as Petitioner asserts, Gai teaches “a memory circuit” because Gai’s intermediate network device 316 includes NVRAM 408, dynamic memory 409, and TCAM 410 that collectively correspond to “a

memory circuit.” *See* Pet. 65–67; Reply 23; Ex. 1003 ¶¶ 188–191; Ex. 1023 ¶ 18.

Second, we disagree with Patent Owner that “the specification, claims, and prosecution history all show that ‘a’ memory circuit should be construed as a single memory circuit” insofar as “a single memory circuit” includes only one component. *See* Sur-reply 18. Claim 15 uses the word “circuit,” and nothing in the claim language indicates that the word “circuit” connotes only one component. Ex. 1001, 11:57–12:17, 12:27–52.

If anything, the word “circuit” connotes multiple components. For instance, the Microsoft Computer Dictionary (5th ed. 2002) defines “circuit” as follows: “A combination of electrical components interconnected to perform a particular task.” Microsoft Comput. Dictionary at 99 (Ex. 3001, 3).

Further, the ’518 patent’s specification describes a preferred embodiment where different components store different types of data as recited in claim 15. *See* Ex. 1001, 9:31–36. In particular, the specification explains that “selected packets are stored in the packet memory 306” and that “stored in either the packet memory 306 or memory in the processor 302 is the enhanced access control list 108.” *Id.* at 9:31–34.

Thus, limiting “a memory circuit” to a single component would exclude a preferred embodiment from claim scope. A construction excluding a preferred embodiment from claim scope is “rarely, if ever correct.” *PPC Broadband, Inc. v. Corning Optical Commc’ns RF, LLC*, 815 F.3d 747, 755 (Fed. Cir. 2016); *see Google LLC v. EcoFactor, Inc.*, 92 F.4th 1049, 1058–59 (Fed. Cir. 2024).

Additionally, the specification explains that “[o]ne skilled in the art will also appreciate that the functions performed by” packet memory 306 “may be combined to be performed by fewer elements or divided out and performed by more elements.” Ex. 1001, 9:65–10:3. According to claim 15, the “memory circuit” performs three functions: (1) stores packets; (2) stores an enhanced access control list; and (3) stores a dynamic access control list. *Id.* at 12:4–7. According to the specification, those functions may be performed by multiple elements or components. *Id.* at 9:65–10:3.

“Even when the specification describes only a single embodiment, the claims of the patent will not be read restrictively unless the patentee has demonstrated a clear intention to limit the claim scope using ‘words or expressions of manifest exclusion or restriction.’” *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 906 (Fed. Cir. 2004) (quoting *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1327 (Fed. Cir. 2002)). Here, Patent Owner does not identify in the ’518 patent’s specification “words or expressions of manifest exclusion or restriction” that limit “a memory circuit” to a single component. *See* Resp. 28–33; Sur-reply 14–19.

As for the ’518 patent’s prosecution history, Patent Owner does not assert that a statement during prosecution by the applicant resulted in prosecution disclaimer limiting “a memory circuit” to a single component. *See* Resp. 28–33; Sur-reply 14–19. “For a statement during prosecution to qualify as a disavowal of claim scope, it must be ‘so clear as to show reasonable clarity and deliberateness,’ and ‘so unmistakable as to be unambiguous evidence of disclaimer.’” *Genuine Enabling Tech. LLC v. Nintendo Co.*, 29 F.4th 1365, 1374 (Fed. Cir. 2022) (quoting *Omega Eng’g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1325 (Fed. Cir. 2003)). Here, Patent

Owner does not identify in the '518 patent's prosecution history "unambiguous evidence of disclaimer." *See* Sur-reply 17–18 (citing Ex. 1002, 102, 104, 140, 142).

Third, as Petitioner asserts, Gai teaches "a memory circuit coupled to the forwarding circuit" (limitation 15.2.1) because Gai's intermediate network device 316 includes forwarding entity 404 (i) directly coupled to TCAM 410 and (ii) indirectly coupled to NVRAM 408 and dynamic memory 409 via CPU 406. *See* Pet. 65–66; Ex. 1003 ¶¶ 188–191; Ex. 1006, 6:23–27, Fig. 4. Regarding indirectly coupled, the '518 patent's specification describes a preferred embodiment with switch forwarding engine 300 indirectly coupled to packet memory 306 via DMA controller 304. Ex. 1001, 3:42–44, 9:9–16, 9:28–30, Fig. 3. According to Patent Owner, switch forwarding engine 300 corresponds to the claimed "forwarding circuit," and packet memory 306 corresponds to the claimed "memory circuit." Sur-reply 15–16; *see* Tr. 32:21–23.

Further, even if claim 15 required "a memory circuit **directly** coupled to the forwarding circuit," Gai's intermediate network device 316 would satisfy that requirement. Intermediate network device 316 includes forwarding entity 404 directly coupled to TCAM 410, and claim 15 does not require coupling between each component comprising the "memory circuit" and each component comprising the "forwarding circuit." *See* Ex. 1001, 11:57–12:17; Ex. 1003 ¶¶ 189–190; Ex. 1006, 6:23–27, Fig. 4.

Fourth, for the reasons stated by Petitioner and supported by Dr. Crovella's testimony, we agree with Petitioner that the combined disclosures in Gai, Yip, Kwan, and Georgiou teach "the memory circuit operable to store packets and operable to store an enhanced access control

list and a dynamic access control list” (limitations 15.2.2–15.2.4). *See* Pet. 67–69; Ex. 1003 ¶¶ 192–204.

Fifth, Patent Owner’s contention that “Gai does not disclose or teach a memory circuit operable to store packets” does not address the proposed combination. *See* Resp. 32; Sur-reply 19. Petitioner relies on the combined disclosures in Gai and Georgiou to teach “the memory circuit operable to store packets” (limitation 15.2.2). *See* Pet. 67–68; Ex. 1003 ¶¶ 192–196. Where obviousness rests on a combination of references, a patentee cannot establish nonobviousness by attacking the references individually. *See In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986).

Sixth, Patent Owner’s assertion that an ordinarily skilled artisan “would have recognized that an ACL converter does not correspond to either the claimed processor or forwarding circuit” and “would therefore not couple the memory to either the processor or the forwarding circuit” misunderstands Gai’s arrangement in the proposed combination. *See* Resp. 31–32. There is no need to modify Gai’s intermediate network device 316 to achieve the claimed couplings because intermediate network device 316 already has “the memory” coupled to both “the processor” and “the forwarding circuit.” *See* Ex. 1003 ¶¶ 40, 188–191, 206–208; Ex. 1006, 5:60–6:18, Fig. 4.

Specifically, for the reasons discussed above in this section, Gai teaches “a memory circuit coupled to the forwarding circuit” (limitation 15.2.1) because Gai’s intermediate network device 316 includes forwarding entity 404 (i) directly coupled to TCAM 410 and (ii) indirectly coupled to NVRAM 408 and dynamic memory 409 via CPU 406. *See* Pet. 65–66; Ex. 1003 ¶¶ 188–191; Ex. 1006, 6:23–27, Fig. 4. Additionally,

for the reasons explained below, Gai teaches “a processor coupled to . . . the memory circuit” (limitation 15.3.1) because Gai’s intermediate network device 316 includes CPU 406 (i) directly coupled to NVRAM 408 and dynamic memory 409 and (ii) indirectly coupled to TCAM 410 via dynamic memory 409 and ACL converter 424. *See* Pet. 70–71; Ex. 1003 ¶¶ 205–208; *infra* § III.E.3(d). Moreover, claim 15 does not require coupling between each component comprising the “processor” and each component comprising the “memory circuit.” *See* Ex. 1001, 11:57–12:17; Ex. 1003 ¶¶ 206–207.

Seventh, for the reasons discussed above, we consider Patent Owner’s motivation-to-combine arguments unavailing, e.g., that an ordinarily skilled artisan would not have been motivated to combine the teachings of Gai, Yip, Kwan, and Georgiou to yield claim 15’s “dynamic access control list” limitation. *See supra* §§ III.D.4(c), III.E.2(c); Resp. 22.

(d) Limitations 15.3.1–15.3.5

Claim 15 recites:

[15.3.1] a processor coupled to the forwarding circuit and to the memory circuit, [15.3.2] the processor operable to define the specific packets detected by the forwarding circuit and [15.3.3] operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and [15.3.4] store the dynamic access control list in the memory circuit, and [15.3.5] further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets.

Ex. 1001, 12:8–17 (limitations 15.3.1–15.3.5).

Petitioner contends that the combined disclosures in Gai, Yip, Kwan, and Georgiou teach limitations 15.3.1–15.3.5 for several related reasons. *See* Pet. 70–79. First, Petitioner asserts that Gai teaches “a processor

coupled to the forwarding circuit and to the memory circuit”
(limitation 15.3.1) because Gai’s intermediate network device 316 includes forwarding entity 404, CPU 406, NVRAM 408, dynamic memory 409, and TCAM 410 with CPU 406 (i) directly coupled to forwarding entity 404, NVRAM 408, and dynamic memory 409 and (ii) indirectly coupled to TCAM 410 via dynamic memory 409 and ACL converter 424. *Id.* at 70–71 (citing Ex. 1003 ¶¶ 205–208; Ex. 1006, 6:13–27, 6:36–41, 6:52–55, Fig. 4).

As support, Petitioner provides the following highlighted and annotated version of Gai’s Figure 4 (Pet. 71):

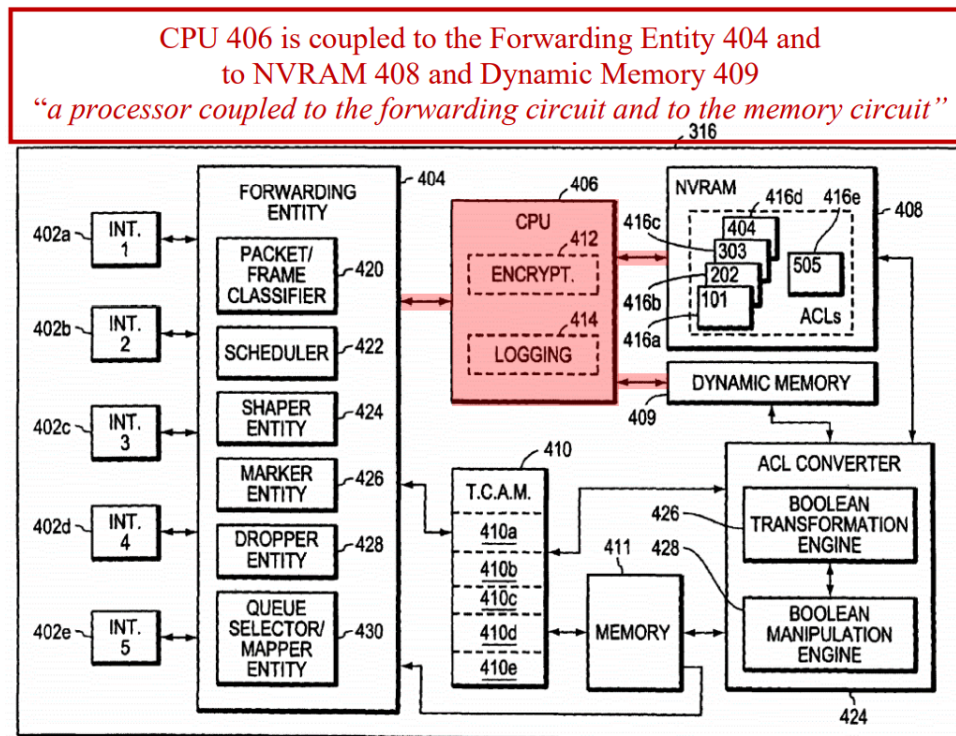


FIG. 4

Figure 4 illustrates intermediate network device 316 including, among other things, forwarding entity 404, CPU 406, NVRAM 408, dynamic memory 409, TCAM 410, memory 411, and ACL converter 424. Ex. 1006, 4:52–54, 5:60–6:12, 6:36–41, Fig. 4. The above highlighted and annotated version of Figure 4 includes:

- (1) red highlighting over CPU 406;
- (2) red highlighting over the bidirectional path between forwarding entity 404 and CPU 406;
- (3) red highlighting over the bidirectional path between CPU 406 and NVRAM 408;
- (4) red highlighting over the bidirectional path between CPU 406 and dynamic memory 409; and
- (5) the red annotation “CPU 406 is coupled to the Forwarding Entity 404 and to NVRAM 408 and Dynamic Memory 409 ‘*a processor coupled to the forwarding circuit and to the memory circuit.*’”

See Pet. 71; Ex. 1003 ¶ 207.

Second, Petitioner asserts that “Gai in combination with Yip and Kwan” teaches “the processor operable to define the specific packets detected by the forwarding circuit” (limitation 15.3.2) because:

- (1) “Gai in combination with Kwan discloses that forwarding entity 404 identifies specific received packets that need additional processing (e.g., encrypted, logged, etc., and packets that have a new IP address that has not been learned)” for the reasons discussed for limitations 15.1.1 and 15.1.4;
- (2) “Gai in combination with Yip and Kwan discloses that Gai’s CPU 406 executes ACL converter 424 software to dynamically generate an optimized TCAM ACL from one or more text-based ACLs” for the reasons discussed for claim 1’s preamble and limitation 1.3; and
- (3) Gai’s CPU 406 “define[s] the specific packets” that forwarding entity 404 identifies for additional processing by (a) “executing ACL converter 424” to “dynamically generate” the unified ACL for the TCAM and (b) “storing the unified ACL in the TCAM.”

Pet. 71–73 (emphasis omitted) (citing Ex. 1003 ¶¶ 209–213; Ex. 1006, 6:52–55, 9:4–27, 9:42–11:4, 12:20–16:17, Figs. 4, 6–7, 9A–9B).

Third, Petitioner asserts that “Gai in combination with Yip, Kwan, and Georgiou” teaches “operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and store the dynamic access control list” (limitation 15.3.3) because:

- (1) “Gai in combination with Georgiou discloses storing packets for processing in dynamic memory 409” for the reasons discussed for limitation 15.2.2;
- (2) Gai in combination with Yip and Kwan discloses “one or more text-based ACLs, which include MAC addresses and seed IP address properties,” thus rendering obvious “an enhanced access control list” for the reasons discussed for limitation 1.1;
- (3) Gai in combination with Yip and Kwan discloses “dynamically generating an optimized TCAM ACL from one or more text-based ACLs,” thus rendering obvious “a dynamic access control list” for the reasons discussed for claim 1’s preamble and limitation 1.3;
- (4) Georgiou discloses that the “process[or] can access and retrieve the packets [from memory], as appropriate, for action on the packet contents”;
- (5) Kwan discloses that “port security processor 242 is used to learn the new IP addresses”;
- (6) “it would have been obvious to” an ordinarily skilled artisan for Gai’s CPU 406 “to retrieve from dynamic memory 409 packets with a new IP address and process these packets per Kwan’s DHCP technique or RARP technique to learn the new IP address”;
- (7) Gai’s CPU 406 would in the learning process use “seed IP address properties in one or more text-based ACLs

and only match a new IP address with a MAC address that is consistent”; and

- (8) Gai’s CPU 406 “would then use the one or more text-based ACLs (including the newly learned IP address) to dynamically generate an optimized TCAM ACL.”

Pet. 73–75 (alterations by Petitioner) (emphasis omitted) (quoting Ex. 1008, 1:26–27) (citing Ex. 1003 ¶¶ 214–217; Ex. 1007, 4:56–58, 5:38–67, 6:14–25, 8:17–47, Fig. 3; Ex. 1008, 3:17–22).

Fourth, Petitioner asserts that Gai teaches “store the dynamic access control list in the memory circuit” (limitation 15.3.4) because:

- (1) “Gai’s TCAM 410 stores the dynamically generated optimized ACL,” thus rendering obvious “stor[ing] the dynamic access control list in the memory circuit”;
- (2) “Gai’s CPU 406 generates the TCAM ACL by executing software of ACL converter 424, among other operations”;
- (3) Gai discloses “executable program instructions . . . [for] storing the ACL corresponding to the second boolean representation at the memory device” and “the memory device is a content addressable memory (CAM)”;
- (4) “[i]t would have been obvious to” an ordinarily skilled artisan “for Gai’s CPU 406, which operates by executing program instructions, to execute the program instructions to store the dynamically generated optimized ACL in TCAM 410.”

Pet. 75–76 (alterations by Petitioner) (emphasis omitted) (citing Ex. 1003 ¶¶ 218–221; Ex. 1006, 6:52–59, 9:22–10:48, 20:38–53, 22:15–29).

Fifth, Petitioner asserts that “Gai in combination with Kwan” teaches “further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets” (limitation 15.3.5) because:

- (1) “Gai in combination with Kwan discloses that the forwarding entity 404 is operable to receive packets on one of a plurality of ports including CPU 406 port” for the reasons discussed above for limitation 15.1.3;
- (2) “it would have been obvious to” an ordinarily skilled artisan “for Gai’s CPU 406 to provide the packets after encryption and learning a new IP address[] (among other packet processing operations) to its port so that the packet may be sent to the destination”;
- (3) Kwan’s Figure 3 shows that packets are passed to “a destination port once the IP address has been learned”; and
- (4) “it would have been obvious to” an ordinarily skilled artisan “for Gai’s CPU 406 to provide packets, after successfully learning a new IP address, to the forwarding entity 404 port so that the packets may be passed to the destination device.”

Pet. 76–79 (citing Ex. 1003 ¶¶ 222–226; Ex. 1006, Fig. 4; Ex. 1007, Fig. 3); *see supra* § III.E.3(b).

Patent Owner makes no arguments specific to limitations 15.3.1–15.3.5. *See, e.g.*, Resp. 21–33; Sur-reply 13–19.

For the reasons stated by Petitioner and supported by Dr. Crovella’s testimony, we agree with Petitioner that the combined disclosures in Gai, Yip, Kwan, and Georgiou teach limitations 15.3.1–15.3.5. *See* Pet. 70–79; Ex. 1003 ¶¶ 205–226.

(e) Conclusion Concerning Obviousness/Nonobviousness for Claim 15

For the reasons discussed above, the combined disclosures in Gai, Yip, Kwan, and Georgiou teach claim 15’s subject matter. *See supra* §§ III.E.3(a)–(d). Moreover, an ordinarily skilled artisan would have been motivated to combine the teachings of Gai, Yip, Kwan, and Georgiou in the

way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.E.2(c). Hence, Petitioner has shown by a preponderance of the evidence that claim 15 is unpatentable under § 103(a) because the claim would have been obvious over Gai, Yip, Kwan, and Georgiou.

4. INDEPENDENT CLAIM 19

(a) Preamble 19.0

Claim 19 recites in its preamble “[a] computer network.” Ex. 1001, 12:27.

Petitioner contends that Gai teaches claim 19’s preamble because Gai discloses computer network 300. Pet. 79 (citing Ex. 1003 ¶ 230).

Patent Owner makes no arguments specific to claim 19’s preamble. *See, e.g.*, Resp. 21–33; Sur-reply 13–19. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic Drinkware*, 800 F.3d at 1378.

Generally, a preamble does not limit a claim. *Allen Eng’g*, 299 F.3d at 1346. We need not decide whether claim 19’s preamble limits the claim because, for the reasons stated by Petitioner and supported by Dr. Crovella’s testimony, we agree with Petitioner that Gai teaches claim 19’s preamble. *See* Pet. 79; Ex. 1003 ¶ 230.

(b) Limitation 19.1.1

Claim 19 recites “a network switch.” Ex. 1001, 12:28 (limitation 19.1.1).

Petitioner contends that Gai teaches limitation 19.1.1 because Gai discloses intermediate network device 316 with circuitry for performing

switching functions in computer network 300. Pet. 79–80 (citing Ex. 1003 ¶ 231); *see id.* at 32, 48.

Patent Owner makes no arguments specific to limitation 19.1.1. *See, e.g.,* Resp. 21–33; Sur-reply 13–19.

For the reasons stated by Petitioner and supported by Dr. Crovella’s testimony, we agree with Petitioner that Gai teaches limitation 19.1.1. *See* Pet. 79–80; Ex. 1003 ¶ 231.

(c) Limitations 19.1.2–19.1.6, 19.2.1–19.2.4, and 19.3.1–19.3.5

Claim 19 requires that the “network switch” include a “forwarding circuit,” a “memory circuit,” and a “processor” as similarly recited in claim 15. Ex. 1001, 12:28–50 (claim 19); *see id.* at 11:58–12:17 (claim 15). Specifically, limitations 19.1.2–19.1.6 are identical to limitations 15.1.1–15.1.5, limitations 19.2.1–19.2.4 are identical to limitations 15.2.1–15.2.4, and limitations 19.3.1–19.3.5 are identical to limitations 15.3.1–15.3.5. *Compare id.* at 11:58–12:17 (claim 15), *with id.* at 12:29–50 (claim 19).

Petitioner contends that the combined disclosures in Gai, Yip, Kwan, and Georgiou teach limitations 19.1.2–19.1.6, 19.2.1–19.2.4, and 19.3.1–19.3.5 for the reasons Petitioner contends that the combined disclosures teach limitations 15.1.1–15.1.5, 15.2.1–15.2.4, and 15.3.1–15.3.5. Pet. 80–81; *see id.* at 49–79.

Patent Owner disputes that the combined disclosures in Gai, Yip, Kwan, and Georgiou teach limitations 19.1.2–19.1.6, 19.2.1–19.2.4, and 19.3.1–19.3.5 for the same reasons Patent Owner disputes that the combined disclosures teach limitations 15.1.1–15.1.5, 15.2.1–15.2.4, and 15.3.1–15.3.5. *See* Resp. 21–33; Sur-reply 13–19.

For the reasons discussed above for claim 15, we agree with Petitioner that the combined disclosures in Gai, Yip, Kwan, and Georgiou teach limitations 19.1.2–19.1.6, 19.2.1–19.2.4, and 19.3.1–19.3.5. *See* Pet. 49–81; Reply 23–26; Ex. 1003 ¶¶ 150–226, 232–245; Ex. 1023 ¶ 18; *supra* §§ III.E.3(b)–(d). For the reasons discussed above for claim 15, we consider Patent Owner’s patentability arguments unavailing. *See supra* § III.E.3(c)(iii).

(d) Limitation 19.4

Claim 19 recites “a plurality of hosts, each host coupled to a respective port of the network switch.” Ex. 1001, 12:51–52 (limitation 19.4).

Petitioner contends that Gai teaches limitation 19.4 because:

- (1) Gai’s intermediate network device 316 includes ports;
- (2) Gai’s computer network 300 includes end stations 306–312 coupled via LAN 302 or LAN 304 to intermediate network device 316; and
- (3) end stations 306–312 “correspond to ‘hosts’ as that term is used in the ’518 patent.”

Pet. 81–83 (emphasis omitted) (citing Ex. 1001, 1:5–21, 2:37–40; Ex. 1003 ¶¶ 246–252; Ex. 1006, 2:1–3, 5:3–13, 5:60–66, 17:4–6, Fig. 3; Ex. 1007, 3:46–50).

Patent Owner makes no arguments specific to limitation 19.4. *See, e.g.,* Resp. 21–33; Sur-reply 13–19.

For the reasons stated by Petitioner and supported by Dr. Crovella’s testimony, we agree with Petitioner that Gai teaches limitation 19.4. *See* Pet. 81–83; Ex. 1003 ¶¶ 246–252.

(e) Conclusion Concerning Obviousness/Nonobviousness for Claim 19

For the reasons discussed above, the combined disclosures in Gai, Yip, Kwan, and Georgiou teach claim 19’s subject matter. *See supra* §§ III.E.4(a)–(d). Moreover, an ordinarily skilled artisan would have been motivated to combine the teachings of Gai, Yip, Kwan, and Georgiou in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.E.2(c). Hence, Petitioner has shown by a preponderance of the evidence that claim 19 is unpatentable under § 103(a) because the claim would have been obvious over Gai, Yip, Kwan, and Georgiou.

5. DEPENDENT CLAIMS 17, 20, AND 21

(a) Claims 17 and 21

Claim 17 depends directly from claim 15 and recites “wherein the switch comprises an Ethernet switch and wherein the packets comprise Ethernet packets.” Ex. 1001, 12:21–23. Claim 21 depends directly from claim 19 and recites “wherein the network comprises an Ethernet network, and wherein the switch comprises an Ethernet switch and the packets comprise Ethernet packets.” *Id.* at 12:55–58.

Petitioner contends that Gai teaches the limitations in claims 17 and 21 because Gai discloses that (1) computer network 300 may use a “LAN standard (e.g., Ethernet)” and (2) intermediate network device 316 on computer network 300 may switch Ethernet packets. Pet. 79, 85 (emphasis omitted) (citing Ex. 1003 ¶¶ 227, 257; Ex. 1006, 2:14–16, 5:3–64; Ex. 1007, 1:32–43). Petitioner contends that Gai’s intermediate network device 316 supports the “processing of Ethernet LAN packets” and, therefore, corresponds to the claimed “Ethernet switch.” *Id.* at 79 (emphasis omitted).

Petitioner also contends that “Gai’s disclosure of Ethernet LAN is consistent with the ’518 patent’s embodiment.” *Id.* (citing Ex. 1001, 1:5–21; Ex. 1003 ¶¶ 228–229).

Patent Owner disputes that the combined disclosures in Gai, Yip, Kwan, and Georgiou teach the subject matter of claims 17 and 21 for the reasons Patent Owner disputes that the combined disclosures teach the subject matter of claims 15 and 19. *See* Resp. 21–33; Sur-reply 13–19.

For the reasons stated by Petitioner and supported by Dr. Crovella’s testimony, we agree with Petitioner that Gai teaches the limitations in claims 17 and 21. *See* Pet. 79, 85; Ex. 1003 ¶¶ 227–229, 257. For the reasons discussed above, we consider Patent Owner’s arguments regarding claims 15 and 19 unavailing. *See supra* §§ III.E.3(c)(iii), III.E.4(c).

(b) Claim 20

Claim 20 depends directly from claim 19 and recites “wherein at least some of the hosts comprise personal computer systems.” Ex. 1001, 12:53–54.

Petitioner contends that Gai and Kwan each teach claim 20’s limitation. Pet. 84. Specifically, Petitioner asserts that Gai’s Figure 3 depicts some of the end stations 306–312 as personal computers. *Id.* (citing Ex. 1003 ¶¶ 253–254). Additionally, Petitioner asserts that Kwan discloses that “host devices . . . such as personal computers can be coupled to” various ports of network device 200. *Id.* (alteration by Petitioner) (emphasis omitted) (quoting Ex. 1007, 3:46–47).

Further, Petitioner asserts that it would have been obvious to “implement at least some of Gai’s end stations as personal computers, in view of Kwan, because such an implementation would allow for users to use

their personal computers and access or exchange content with other users of other personal computers or with other network devices,” e.g., “send a print request to end station 314, illustrated as a printer.” Pet. 84 (citing Ex. 1003 ¶ 255).

Patent Owner disputes that the combined disclosures in Gai, Yip, Kwan, and Georgiou teach claim 20’s subject matter for the same reasons Patent Owner disputes that the combined disclosures teach claim 19’s subject matter. *See* Resp. 21–33; Sur-reply 13–19.

For the reasons stated by Petitioner and supported by Dr. Crovella’s testimony, we agree with Petitioner that Gai and Kwan each teach claim 20’s limitation. *See* Pet. 84; Ex. 1003 ¶¶ 253–256. Additionally, for the reasons discussed above, we consider Patent Owner’s arguments regarding claim 19 (claim 20’s base claim) unavailing. *See supra* §§ III.E.3(c)(iii), III.E.4(c).

(c) Summary for Dependent Claims 17, 20, and 21

For the reasons discussed above, the combined disclosures in Gai, Yip, Kwan, and Georgiou teach the subject matter of claims 17, 20, and 21. *See supra* §§ III.E.3(a)–(d), III.E.4(a)–(d), III.E.5(a)–(b). Moreover, an ordinarily skilled artisan would have been motivated to combine the teachings of Gai, Yip, Kwan, and Georgiou in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § III.E.2(c). Hence, Petitioner has shown by a preponderance of the evidence that claims 17, 20, and 21 are unpatentable under § 103(a) because the claims would have been obvious over Gai, Yip, Kwan, and Georgiou.

IV. CONCLUSION

Based on the evidence presented with the Petition, the evidence introduced during the trial, and the parties' respective arguments, Petitioner has shown by a preponderance of the evidence that:

- (1) claims 1 and 3 are unpatentable under § 103(a) because the claims would have been obvious over Gai, Yip, and Kwan; and
- (2) claims 15, 17, and 19–21 are unpatentable under § 103(a) because the claims would have been obvious over Gai, Yip, Kwan, and Georgiou.

In summary:⁹

Claim(s)	35 U.S.C. §	Reference(s)/ Basis	Claim(s) Shown Unpatentable	Claim(s) Not Shown Unpatentable
1, 3	103(a)	Gai, Yip, Kwan	1, 3	
15, 17, 19–21	103(a)	Gai, Yip, Kwan, Georgiou	15, 17, 19–21	
Overall Outcome			1, 3, 15, 17, 19–21	

⁹ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding after the issuance of this Final Written Decision, we draw Patent Owner's attention to the April 2019 Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. §§ 42.8(a)(3), (b)(2).

V. ORDER

Accordingly, it is

ORDERED that claims 1, 3, 15, 17, and 19–21 in the '518 patent are determined to be unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, the 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.

IPR2024-00734
Patent 7,623,518 B2

For PETITIONER:

Theodore M. Foster
David L. McCombs
Gregory P. Huh
HAYNES AND BOONE, LLP
ipr.theo.foster@haynesboone.com
david.mccombs.ipr@haynesboone.com
gregory.huh.ipr@haynesboone.com

For PATENT OWNER:

Robert A. Auchter
AUCHTER PLLC
robert@auchterlaw.com

Brett E. Cooper
BC LAW GROUP, P.C.
bcooper@bc-lawgroup.com
Lionra_Counsel@b-clg.com