Trials@uspto.gov
571.272.7822

Paper 38
Date: November 13, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ZSCALER, INC.,
Petitioner,
v.

SYMANTEC CORPORATION,
Patent Owner.

IPR2018-00920
Patent 9,525,696 B2

Before JEFFREY S. SMITH, BRYAN F. MOORE, and NEIL T. POWELL, *Administrative Patent Judges*.

SMITH, *Administrative Patent Judge*.

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

I. INTRODUCTION

Petitioner filed a Petition for *inter partes* review of claims 1–19 of U.S. Patent No. 9,525,696 B2 (Ex. 1001, "the '696 patent"). Paper 1

("Pet."). Patent Owner filed a Preliminary Response. Paper 9 ("Prelim. Resp."). On November 14, 2018, we instituted an *inter partes* review of all the challenged claims. Paper 11. Patent Owner filed a Response to the Petition. Paper 19 ("PO Resp."). Petitioner filed a Reply. Paper 23 ("Pet. Reply"). Patent Owner filed a Sur-Reply. Paper 26 ("PO Sur-Reply"). An oral hearing was held August 8, 2019. Paper 37.

This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a). For the reasons discussed below, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–19 of the '696 patent are unpatentable.

A. Related Matters

The '696 patent, along with several other patents, is the subject of *Symantec Corporation and Symantec Limited v. Zscaler, Inc.*, No. 17-cv-04414 (N.D. Cal.), transferred from No. 17-cv-00806 (D. Del.), which was filed June 22, 2017. Pet. 2–3; Paper 5 (Patent Owner's Mandatory Notice).

The '696 patent shares common parent applications with U.S. Patent No. 8,402,540 B2 ("the '540 patent"). The '540 patent is the subject of IPR2018-00930. Pet. 4; Paper 5.

B. The '696 Patent

The '696 patent relates generally to protecting computer systems from viruses, attacks from hackers, spyware, spam, and other malicious activities. Ex. 1001, 1:59–63. A flow processing facility inspects payloads of network traffic packets and provides security and protection to a computer. *Id.* at Abstract. Figure 1 of the '696 patent is reproduced below.

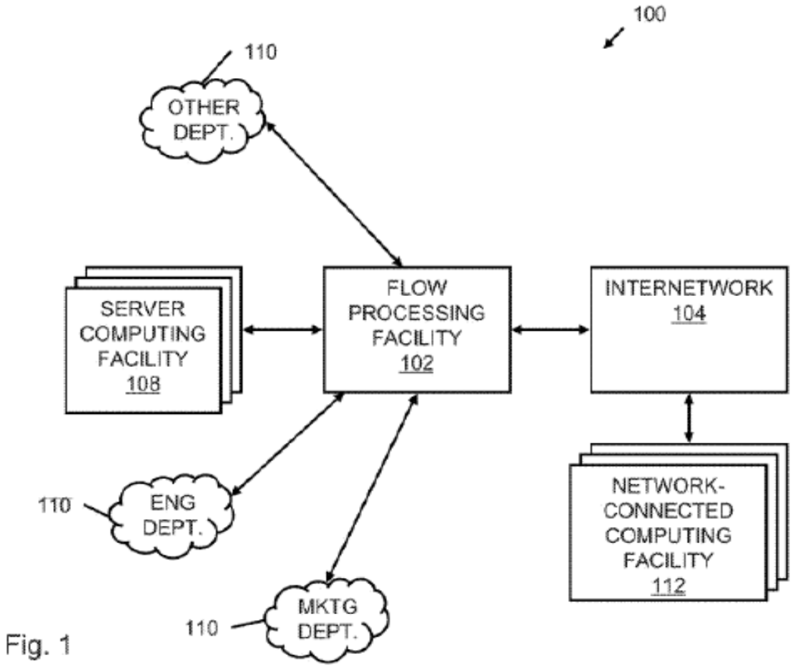

100
110
OTHER DEPT.
SERVER COMPUTING FACILITY 108
FLOW PROCESSING FACILITY 102
INTERNETWORK 104
110
ENG DEPT.
NETWORK-CONNECTED COMPUTING FACILITY 112
110
MKTG DEPT.

Fig. 1

Figure 1 above shows networked computing environment 100 for data flow processing, including flow processing facility 102 coupled to internetwork 104, network-connected computing facility 112, a plurality of server computing facilities 108, and a number of departmental computing facilities 110, such as an engineering department, a marketing department, and another department. Ex. 1001, 19:57–65, 20:7–8. Flow processing facility 102 receives data flows from the computing facilities via internetwork 104 and processes the data flows. *Id.* at 20:29–35. A virtualization aspect of flow processing facility 102 enables the flow processing facility to provide features and functions tailored to users of data flows. *Id.* at 22:16–19. For example, virtualization can present server computing facility 108 with different policies and applications than it provides to network-connected computing facility 112. *Id.* at 22:21–25. A subscriber profile can relate an application to a subscriber. *Id.* at 37:58–59.

Figure 30 below shows a schematic of an enterprise network. *Id.* at 89:27–28.

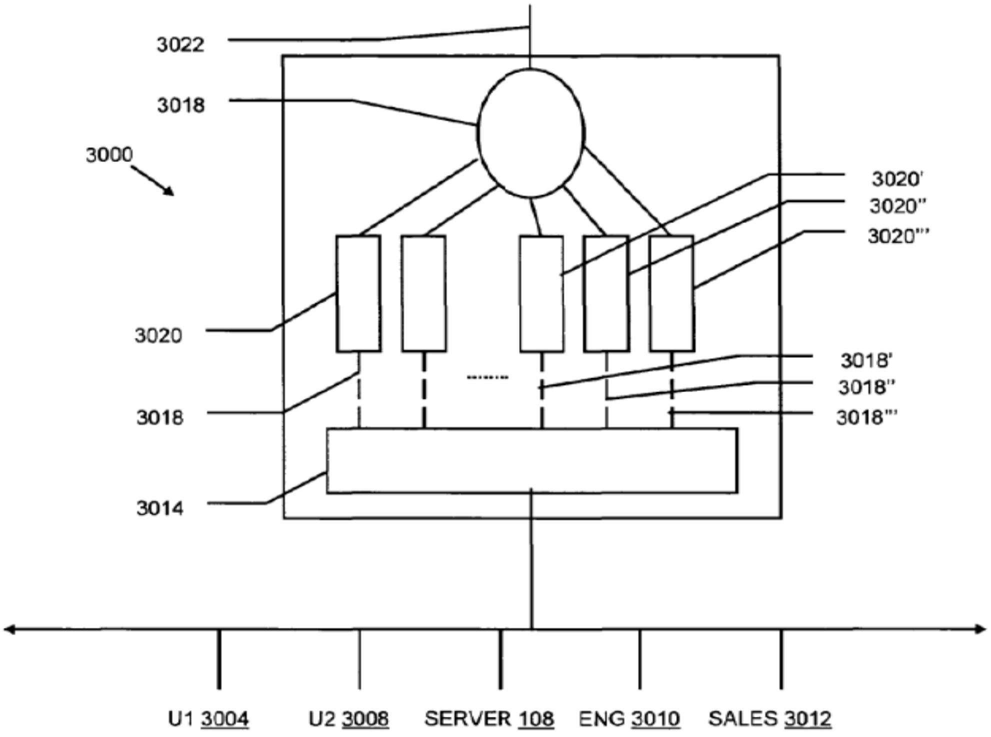


FIG. 30

Figure 30 above shows network participants of network 3000 include user1 3004, user2 3008, and server 108, and participant types of network 3000 include engineering 3010 and sales 3012. *Id.* at 89:42–45. Each of the network participants and participant types has a physical connection to flow processing 102. *Id.* at 89:45–48. Virtualization model 3014 of flow processing facility 102 uniquely identifies data flows 444 from each participant and routes the data flow to virtual network 3018 associated with the relevant participant. *Id.* at 90:3–9. Security policy 3020 may direct all aspects of flow processing facility 102, including an anti-virus feature, an anti-spam feature, an anti-spyware feature, or anti-worm feature, to be applied to data flow 444 of virtual network 3018. *Id.* at 90:19–26.

C. Illustrative Claim

Claims 1 and 13 of the challenged claims of the ’969 patent are independent. Claim 1 is illustrative of the claimed subject matter:

> 1. A flow processing facility for implementing a security policy, comprising:
>
> a plurality of application processing hardware modules, each configured with an application for processing data packets;
>
> a subscriber profile for identifying data packets associated with the subscriber profile in a stream of data packets; and
>
> a network processing module for identifying one or more of the plurality of application processing modules for processing the identified data packets based on an association of the application configured on each application processing module with the subscriber profile and for transmitting the identified data packets in at least one of series and parallel to the identified application processing modules based on the security policy.

Ex. 1001, 123:48–63.

D. References

Petitioner relies on the following references. Pet. 5–6.

Name	Reference	Exhibit
Nortel	WO 00/33204, issued June 8, 2000	1004
Stone	US 5,598,410, issued Jan. 28, 1997	1005
Alles	US 6,466,976 B1, issued Oct. 15, 2002, filed Dec. 3, 1998	1006
Lin	US 6,633,563 B1, issued Oct. 14, 2003, filed Mar. 2, 1999	1007

E. Asserted Grounds of Unpatentability

Petitioner contends that claims 1–19 of the ’696 patent are unpatentable based on the following grounds:

Claims Challenged	35 U.S.C. §	Reference(s)
1, 9–13, 16–19	103	Nortel
2–8, 14, 15	103	Nortel, Stone
1, 9–13, 16–19	103	Alles, Lin
2–8, 14, 15	103	Alles, Lin, Stone

II. ANALYSIS

A. Claim Construction

In an *inter partes* review proceeding based on a petition filed before November 13, 2018, a claim in an unexpired patent is interpreted according to “its broadest reasonable construction in light of the specification of the patent in which it appears.” 37 C.F.R. § 42.100(b) (2017).[1] Under this standard, “the words of a claim ‘are generally given their ordinary and customary meaning’ . . . that the term would have to a person of ordinary skill in the art in question at the time of the invention.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc) (citations omitted). “[T]he person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which [it] appears, but in the context of the entire patent, including the specification.”

[1] A recent amendment to this rule does not apply here because the Petition was filed before November 13, 2018. *See* Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b) effective November 13, 2018).

Id. at 1313. For example, a "claim construction that excludes [a] preferred embodiment [described in the specification] 'is rarely, if ever, correct and would require highly persuasive evidentiary support.'" *Adams Respiratory Therapeutics, Inc. v. Perrigo Co.*, 616 F.3d 1283, 1290 (Fed. Cir. 2010) (citation omitted). But "a claim construction must not import limitations from the specification into the claims." *Douglas Dynamics, LLC v. Buyers Prods. Co.*, 717 F.3d 1336, 1342 (Fed. Cir. 2013) (citation omitted). Therefore, "it is improper to read limitations from a preferred embodiment described in the specification—even if it is the only embodiment—into the claims absent a clear indication in the intrinsic record that the patentee intended the claims to be so limited." *Dealertrack, Inc. v. Huber*, 674 F.3d 1315, 1327 (Fed. Cir. 2012) (citation omitted).

For purposes of this decision, we determine no terms need an explicit construction to resolve a controversy. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (only those terms which are in controversy need to be construed and only to the extent necessary to resolve the controversy). We address claim interpretation to the extent necessary within the unpatentability analysis.

B. Asserted Obviousness over Nortel: Claims 1, 9–13, and 16–19

1. Nortel (Ex. 1004)

Nortel relates to a method for providing desired service policies to subscribers accessing the Internet. Ex. 1004, 1:4–6. An internet service node ("ISN") enables providing the desired service policies to each subscriber. Ex. 1004, Abstract. The ISN contains multiple processor groups, with each subscriber being assigned to a processor group. *Id.* The assigned processor group may be configured with processing rules that provide the service policies desired by a subscriber. *Id.* A content addressable memory with masks for individual locations determines the processor group to which received data is to be assigned. *Id.*

Figure 4 of Nortel illustrates details of an ISN and is reproduced below.

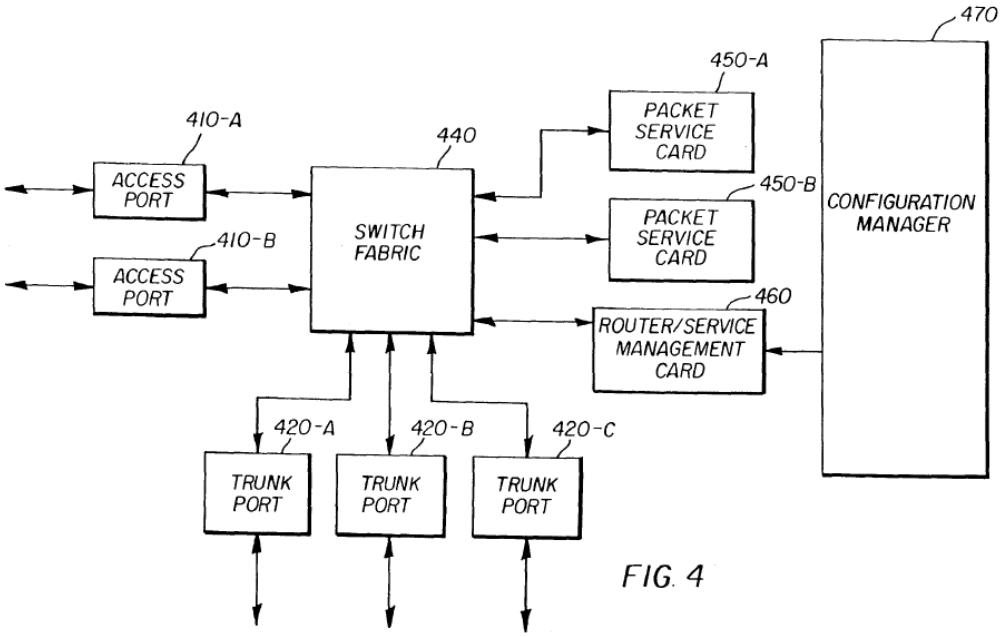


FIG. 4

Figure 4 above shows an ISN including access ports 410-A, 410-B; trunk ports 420-A, 420-B, 420-C; switch fabric 440; packet service cards 450-A, 450-B; router/service management card 460; and configuration manager 470. Ex. 1004, 17:17–23.

Configuration manager 470 provides a user interface to enable different service policies to be specified for different subscribers. Ex. 1004, 18:13–15. Switch fabric 440 receives bit groups from access ports 410 and forwards the bit groups to packet service cards 450. *Id.* at 19:7–8. Different service policy types are implemented in different packet service cards 450. *Id.* at 19:12–13. Each subscriber may be assigned to a packet service card providing the desired service policy types. *Id.* at 13–14. By assigning the data processing for each subscriber to a specific packet service card, each packet service card may be configured only with the processing rules corresponding to the subscribers assigned to it. *Id.* at 20:14–18.

Figure 5 of Nortel is reproduced below.

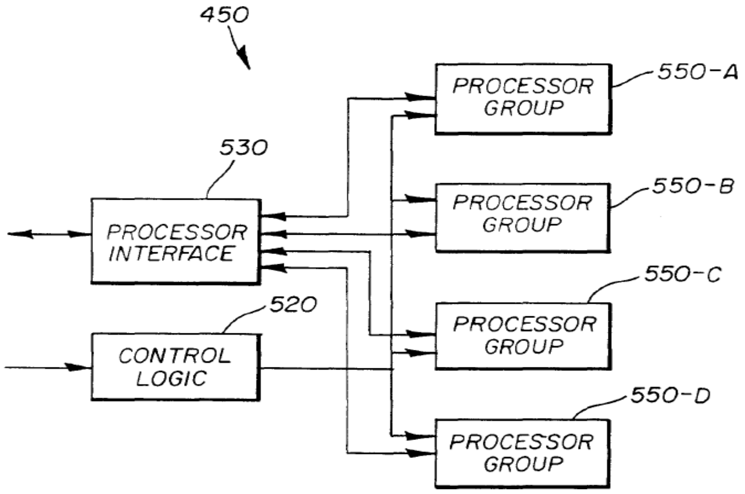


FIG. 5

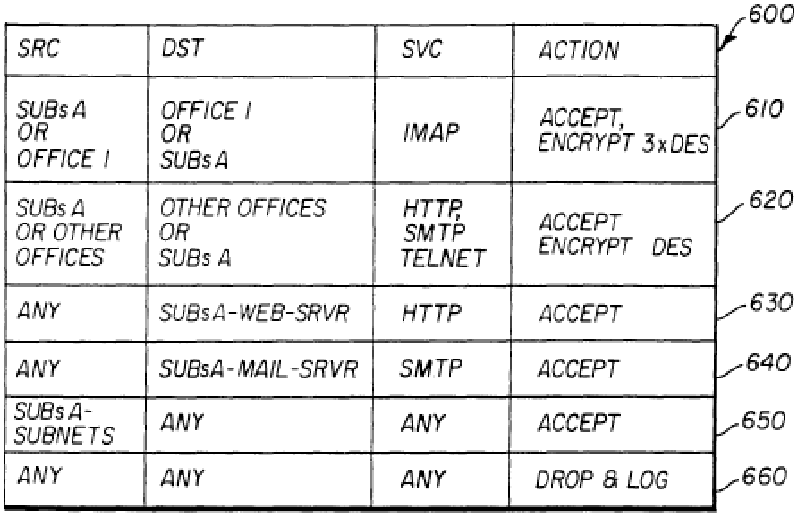
Figure 5 of Nortel above is a block diagram illustrating details of packet service card 450. Ex. 1004, 21:14–15. Packet service card 450 includes processor groups 550-A through 550-D, processor interface 530, and control logic 520. *Id.* at 21:15–16. Control logic 520 determines which of the processors in a processor group processes a packet. *Id.* at 21:19–20. Control logic 520 operates in conjunction with configuration manager 470 to instantiate, or configure, processor groups 550 with processing rules related to assigned subscribers, to ensure processor group 550 performs operations specified by the processing rules. *Id.* at 21:21–23, 21:30–31. Several subscribers may be assigned to each processor group. *Id.* at 22:8.

2. Claims 1, 9–13, and 16–19

Claim 1 recites "a plurality of application processing hardware modules, each configured with an application for processing data packets." Claim 13 recites a similar limitation. Petitioner contends these limitations are taught by Nortel, in view of the knowledge of a person of ordinary skill in the art, based on Nortel's teaching of an ISN including a plurality of packet service cards. Pet. 21–22 (citing Ex. 1004, Fig. 4, 3:5–7, 17:18–21, 20:19–20), 31. According to Petitioner, each packet service card in Nortel has a plurality of processor groups, and each processor group processes data using processing rules, where the processing rules corresponding to a subscriber are assigned to a pre-specified processor or group of processors. Pet. 22–23 (citing Ex. 1004, Fig. 5, 3:5–9, 4:20–23, 9:16–19, 19:12–24, 21:14–16, 22:14–15; Ex. 1003 ¶¶ 76–80).

Petitioner contends that a person of ordinary skill in the art "would have understood Nortel's processing rules to comprise applications." Pet. 25. Specifically, Petitioner contends that Nortel discloses that the processing rules on the packet service cards implement policies relating to firewalls, security, anti-spoofing, virtual private networks, encryption, tunneling, and traffic steering, which, according to Petitioner's declarant Dr. Markus Jakobsson, were well-known in the art to be performed by application programs. Pet. 24 (citing Ex. 1004, 14:28–15:2; Ex. 1003 ¶¶ 80–83; Ex. 1012, 6). Petitioner contends that Nortel's disclosure of an exemplary structure shown in Figure 6A, containing multiple processing rules, teaches that each processing rule is a software structure containing a classifier and an action, with the classifier specifying the data flows and conditions under which the associated action needs to be applied. Pet. 24–25 (citing Ex. 1004, Fig. 6A, 15:4–6; Ex. 1003 ¶¶ 84–85).

Figure 6A of Nortel is reproduced below.



SRC	DST	SVC	ACTION
SUBs A OR OFFICE I	OFFICE I OR SUBs A	IMAP	ACCEPT, ENCRYPT 3xDES
SUBs A OR OTHER OFFICES	OTHER OFFICES OR SUBs A	HTTP, SMTP TELNET	ACCEPT ENCRYPT DES
ANY	SUBsA-WEB-SRVR	HTTP	ACCEPT
ANY	SUBsA-MAIL-SRVR	SMTP	ACCEPT
SUBs A- SUBNETS	ANY	ANY	ACCEPT
ANY	ANY	ANY	DROP & LOG

600
610
620
630
640
650
660

FIG. 6A

Figure 6A above shows table 600 illustrating exemplary processing rules 610–660 for providing desired service policies to subscribers. Ex. 1004, 8:24–25, 23:1. A classifier for a security policy is chosen to include data required for identifying flows. *Id.* at 23:1–3. Dr. Jakobsson testifies that rule 610 shown in Figure 6A of Nortel illustrates that a data flow with the classifier specified by a source or destination address in the SRC and DST columns, and transmitted using a specified service in the SVC column, is processed by the corresponding action in the ACTION column, which is shown in Figure 6A as an encryption function. Ex. 1003 ¶¶ 84–85 (citing Ex. 1004, Fig. 6A, 15:4–6, 23:3–6). Dr. Jakobsson testifies that security functions were well-known in the art to be provided by software applications. Ex. 1003 ¶ 83. Dr. Jakobsson further testifies that Nortel discloses each processor group is configured to process data in accordance with the processing rules. Ex. 1003 ¶¶ 80, 85.

Petitioner contends that "it would have been obvious to a POSA that Nortel's processing rules comprise applications," because a person of ordinary skill would have understood the term "application" to include any software or instructions, other than the operating system, used to perform specific functions on a computer, such as Nortel's processing rules for performing desired security functions to specified data flows. Pet. 35–36 (citing Ex. 1012, 4; Ex. 1013, 4; Ex. 1014, 4; Ex. 1003 ¶¶ 149–154). Dr. Jakobsson testifies that a person of ordinary skill in the art would have understood each processing rule in Figure 6A of Nortel comprises software instructions to perform specific functions, such as the corresponding associated action in the ACTION column for each rule, on data that matches the identified source, destination, and service classifiers. Ex. 1003 ¶ 154 (citing Ex. 1004, 23:3–6. Dr. Jakobsson testifies that a person of ordinary skill in the art "would have had a reasonable expectation of success in implementing Nortel's security-related processing rules as applications," because using generic computer processors with well-known security applications would successfully provide the security functionalities of Nortel. *Id.* ¶ 155 (citing Ex. 1012 6). Dr. Jakobsson testifies that a person of ordinary skill in the art "would have had a reasonable expectation that security applications that were known in the art could readily and successfully be used to provide the security functionalities disclosed in Nortel." *Id.*

We credit Dr. Jakobsson's testimony, which is supported by evidence cited above, and determine the Petition and supporting evidence show that a person of ordinary skill in the art would have understood Nortel's processing rules comprise software instructions to perform specific functions, and that a person of ordinary skill would have considered software instructions to perform specific functions to be applications. We rely on Nortel's teaching of a processor group configured with processing rules to provide service policies such as security functions, and Dr. Jakobsson's testimony and his supporting evidence that a person of ordinary skill in the art would have understood that security functions are provided by software applications, to determine that Nortel and the knowledge of a person of ordinary skill in the art teaches "a plurality of application processing hardware modules, each configured with an application for processing data packets" as recited in claim 1 and the corresponding limitation of 13. Ex. 1004, 3:5–9, 23:1–29, Fig. 6A; Ex. 1003 ¶¶ 80–85 (citing Ex. 1004, 3:5–9, 9:12–14, 9:16–19, 14:28–15:2, 15:4–6, 23:3–6, Fig. 6A; Ex. 1012, 4, 6; Ex. 1013, 4).

Claim 1 recites "a subscriber profile for identifying data packets associated with the subscriber profile in a stream of data packets." Claim 13 recites a similar limitation. Petitioner contends this limitation is taught by Nortel, in view of the knowledge of a person of ordinary skill in the art, in light of Nortel's teaching of classifiers to associate incoming data packets with a subscriber. Pet. 25–26 (citing Ex. 1003 ¶¶ 87–88), 31–32. Petitioner, relying on testimony of Dr. Jakobsson, contends that Nortel's classifiers are stored in a profile using a content addressable memory ("CAM") having a search field to store data identifying a subscriber, and a mask field storing a mask specifying individual bit positions to be examined in incoming data. *Id.* at 26 (citing Ex. 1003 ¶¶ 89–91). In particular, Petitioner contends that Nortel discloses storing a destination address in the CAM in order to identify data packets for a subscriber assigned to the destination address. *Id.* (citing Ex. 1004, 27:12–25, 28:12–32; Ex. 1003 ¶¶ 89 ("The CAM has a search field, which stores data identifying a subscriber."), 90 ("For example, in the case of IP protocol packets . . . , Nortel discloses . . . Destination IP address of the received packet = IP address assigned to the specific subscriber.")).

Patent Owner contends that Nortel does not teach the claimed subscriber profile, because, according to Patent Owner, Nortel makes clear that its classifiers are not stored in a profile using a CAM. PO Resp. 34–37 (citing Ex. 1004, 3:23–25, 17:28–18:4, 26:4–7, 26:10–11, 27:12–22, 28:28–31, 31:10–13; Ex. 2006 ¶¶ 75–77); PO Sur-Reply 7–10 (citing, inter alia, Ex. 1004, Fig. 6A, 23:3–5; Ex. 2006 ¶ 63). Patent Owner contends that Nortel's "CAM may be used to identify incoming data packets; however, Nortel does **not** state that the CAM implements classifiers or processing rules." PO Resp. 37; *see id.* at 37–39. According to Patent Owner, Nortel distinguishes between information stored in the CAM search fields and the classifier stored in the processing rules. *Id.* at 38 (citing Ex. 2006 ¶ 86). Patent Owner contends that Nortel describes a classifier as a specific collection of information, including data flows and conditions, and that the conditions are not stored in the CAM. *Id.* at 37–39.

Nortel discloses storing source and destination IP addresses in the classifiers (Ex. 1004, Fig. 6A, 23:1–10) as well as in the CAM (Ex. 1004, 28:10–11, 30:25–26, 32:13–18, 33:7). Even were we to accept Patent Owner's contention that Nortel's classifier includes conditions that are not stored in the CAM, we agree with Petitioner and Dr. Jakobsson that Nortel discloses storing an IP address assigned to a specific subscriber in the CAM in order to identify data packets having a matching destination IP address.

Pet. 26 (citing Ex. 1004, 27:12–25, 28:12–32; Ex. 1003 ¶¶ 89 ("The CAM has a search field, which stores data identifying a subscriber."), 90 ("For example, in the case of IP protocol packets . . . , Nortel discloses . . . Destination IP address of the received packet = IP address assigned to the specific subscriber.")). Storing an IP address assigned to a specific subscriber in the CAM in order to identify data packets having a matching destination IP address is sufficient to meet the claim language "a subscriber profile for identifying data packets associated with the subscriber profile in a stream of data packets."

Patent Owner contends that we should reject Dr. Jakobsson's testimony because, according to Patent Owner, Dr. Jakobsson's testimony that a classifier portion of a service policy would be implemented in a CAM is unsupported by Nortel. PO Resp. 39–42. Patent Owner relies on testimony from both Dr. Jakobsson and Dr. Chatterjee to support the contention that Nortel's processing rules, including the classifier and service policy, are configured in the processor groups of Nortel's packet service cards, not in the CAM. *Id.* at 40–41 (citing Ex. 2007 108:11–15, 119:22–120:6; Ex. 2006 ¶¶ 90–96). Petitioner contends that Dr. Jakobsson provides facts, data, and analysis to support his opinions. Pet. Reply 25–27. We agree with Petitioner. Dr. Jakobsson's testimony that the CAM stores a destination IP address to identify a subscriber is supported by the cited portions of Nortel. Ex. 1003 ¶¶ 89–91 (citing Ex. 1004, 27:12–25, 28:12–27, 28:31–32).

We rely on Dr. Jakobsson's testimony and supporting evidence and determine that the destination address stored in the CAM of Nortel, which "uniquely identifies the subscriber" as taught by Nortel (Ex. 1004, 27:28–

29), teaches "a subscriber profile for identifying data packets associated with the subscriber profile in a stream of data packets" as recited in claims 1 and 13.

Claim 1 recites

> a network processing module for identifying one or more of the plurality of application processing modules for processing the identified data packets based on an association of the application configured on each application processing module with the subscriber profile and for transmitting the identified data packets in at least one of series and parallel to the identified application processing modules based on the security policy.

Claim 13 recites a similar limitation. Petitioner contends these limitations are taught by Nortel's teaching of a switch fabric including a CAM that identifies the subscriber of originating data packets as discussed above and also identifies processors for providing the subscriber's desired service policies to the data packets, and that the switch fabric forwards the data packets to the identified processors. Pet. 27–29 (citing Ex. 1004, Abstract, 3:10–14, 4:20–22, 4:32, 5:16–29, 9:9–11, 9:16–19, 9:29–31, 10:16–18, 19:7–8, 19:12–20:3, 27:12–25, 28:5–32, Fig. 4; Ex. 1003 ¶¶ 94–95, 97–102), 32–33.

Patent Owner contends that Nortel discloses identifying a processor based on the specific subscriber to whom the received data relates, and not on an association between the application configured on the processor with the subscriber profile. PO Resp. 24 (citing Ex. 1004, 3:10–12). According to Patent Owner, the CAM of Nortel has no knowledge of the applications applied by the processors; therefore, the CAM could not identify a processor based on an association of the application configured on the processor with the subscriber profile. *Id.* at 24–26, 28–29 (citing Ex. 1004, 5:18–21, 26:22–

24, 27:12–15, 27:18–22, Fig. 7B; Ex. 2006 ¶¶ 75–77); PO Sur-Reply 14–15 (citing Ex. 1018, 23:10–21; Ex. 1004, 5:18–21).

We disagree with Patent Owner. Nortel discloses assigning each subscriber to a processor group. Ex. 1004, 3:5–6. Nortel discloses forwarding received data to a specific processor group based on the specific subscriber related to the data, so that the "processor group may apply the processing rules related to the subscriber to provide the service policies desired by the subscriber." *Id.* at 3:13–14. Nortel discloses determining the specific processor group to which the data is to be forwarded by examining the IP destination address located in the IP header. *Id.* at 5:4–10. Nortel discloses that the

> search field of each location [in CAM] may be configured to store the data identifying a subscriber [such as the IP destination address], and the output field may be configured to store data identifying a processor or group of processors capable of providing the desired service policies to the subscribers related to the CAM entry.

Id. at 5:18–21; *see id.* at 30:25–26 (disclosing "the assignment of IP packets to processors based on the source or destination IP addresses"). In other words, associating an IP destination address that identifies a subscriber with a processor group that applies processing rules capable of providing the subscriber's desired service policies meets the limitation "identifying one or more of the plurality of application processing modules for processing the identified data packets based on an association of the application configured on each application processing module with the subscriber profile" as recited in claim 1 and the corresponding recitation in claim 13.

Patent Owner contends that the CAM's identification of a processor in Nortel cannot be based on an association of the service policy configured on the processor with the subscriber profile, because Nortel explains that the service policy may not even be configured on the processor until after the data flow is received. PO Resp. 29. According to Patent Owner, processing rules may be generated dynamically when a subscriber is establishing a dial-up connection and an IP address is allocated to the subscriber. *Id.* (citing Ex. 1004, 15:19–31). Patent Owner contends that, in this case, when the CAM identifies the processor associated with the subscriber, the purported application to be applied by the processor may not even be configured on the processor. *Id.* at 29–30 (citing Ex. 1004, 15:32–16:2).

Petitioner contends that Patent Owner's argument is irrelevant, because Nortel discloses that some processing rules are constructed statically. Pet. Reply 8–9 (citing Ex. 1004, 4:2–3, 23:20–23). Petitioner contends that because Nortel teaches that this limitation is practiced at least some of the time, it is irrelevant that Nortel may also disclose other modes of operation. *Id.* at 9 (citing *Unwired Planet, LLC v. Google Inc.*, 841 F.3d 995, 1002 (Fed. Cir. 2016) ("[C]ombinations of prior art that sometimes meet the claim elements are sufficient to show obviousness.")). We agree with Petitioner for the reasons given by Petitioner. In addition, contrary to Patent Owner's contention, Nortel discloses that the portion of the processing rule that is generated dynamically when a user establishes a dial-up connection is allocating an IP address to the subscriber, not configuring an application on a processor. Ex. 1004, 15:19–25.

Patent Owner contends that even if the identified processors provide the subscriber's desired service policies, Petitioner does not contend that a service policy is an application. PO Resp. 25, 30–31 (citing Pet. 24). We disagree with Patent Owner for the reasons discussed above in our analysis of the "application processing hardware module" limitation. As we discussed above, we credit Dr. Jakobsson's testimony and supporting evidence in determining that Nortel's disclosure of a packet service card that is configured to implement processing rules to perform a specific function, such as security or encryption, teaches an "application processing hardware module[]" that is configured with an "application for processing data packets," such as a security application or an encryption application, as recited in claim 1 and similarly recited in claim 13.

Dr. Jakobsson testifies that the identification of a processor in Nortel is based on an association of the application configured on the processor with the subscriber profile, because the processor identified by the output field of the CAM is "capable of providing the desired service policies related to the CAM entry" in the search field (such as the IP destination address). Ex. 1003 ¶ 95 (citing Ex. 1004, 5:16–29, 27:12–25, 28:5–32). In particular, Dr. Jakobsson testifies that the CAM matches the destination address of incoming data with a particular subscriber's destination address and identifies processors capable of providing the subscriber's desired service policies based on the destination address. Ex. 1003 ¶¶ 90, 94–103 (citing Ex. 1004, Abstract, 3:10–14, 4:20–22, 4:32, 5:16–19, 9:9–11, 9:16–19, 9:29–31, 10:16–18, 19:7–8, 19:15–20:3, 27:12–25, 28:5–32, Fig. 4).

We credit Dr. Jakobsson's testimony and supporting evidence in determining that Nortel's disclosure of a CAM that identifies and forwards IP packets to a processor or group of processors capable of providing a subscriber's desired service policies based on the subscriber's destination address teaches "a network processing module for identifying one or more of the plurality of application processing modules for processing the identified data packets based on an association of the application configured on each application processing module with the subscriber profile" as recited in claim 1 and the similar limitation recited in claim 13. Ex. 1003 ¶¶ 90, 94–103; Ex. 1004, 3:5–14, 5:4–32, 26:4–7, 26:29–31, 27:12–31, 28:5–32, 30:25–32, 31:14–24.

Claim 13 recites "a security policy for determining a portion of the identified data packets to be processed by each of the applications." Petitioner, relying on testimony of Dr. Jakobsson, contends Nortel teaches this limitation in teaching "a security policy (processing rule) for determining a portion (those matching the classifier) of the identified data packets (data packets identified by classifiers) to be processed by the applications (processor groups that apply the specified actions)." Pet. 32 (citing Ex. 1003 ¶¶ 123–126). We credit Dr. Jakobsson's testimony and supporting evidence and determine that Nortel in view of the knowledge of a person of ordinary skill in the art teaches this limitation.

For the reasons given above, we determine that the Petition and supporting evidence show, by a preponderance of the evidence, that Nortel in view of the knowledge of a person of ordinary skill in the art would have rendered claims 1 and 13 obvious.

Claim 9 recites "wherein transmitting the identified packets in series to the applications includes transmitting the identified data packets to be processed by a first application before being processed by a second application." Claim 11 recites a similar limitation. Petitioner contends these limitations are taught by Nortel, in view of the knowledge of a person of ordinary skill in the art, based on Nortel's teaching of forwarding data processed by one of the service cards to another packet service card. Pet.

29–31 (citing Ex. 1004, 21:1–7; Ex. 1003 ¶¶ 106–107). Petitioner also contends this limitation is taught by Nortel's teaching of applying processing rules in an order to ensure predictable and desired service policies, where different processing rules are implemented by different applications. *Id.* at 29–30 (citing Ex. 1004, 9:16–19, 17:6–8, 20:7–8, 22:22–25; Ex. 1003 ¶ 108). We determine that the Petition and supporting evidence show, by a preponderance of the evidence, that Nortel in view of the knowledge of a person of ordinary skill in the art teaches the additional limitations of claims 9 and 11 and would have rendered claims 9 and 11 obvious.

Claim 10 recites "the second application is selected from a list consisting of an anti-virus application, a URL filter, a content filter, a firewall, an intrusion prevention service, and a database protection application." Claim 12 recites a similar limitation. Petitioner contends these limitations are taught by Nortel's teaching of rules for firewall parameters, and that a person of ordinary skill in the art would have understood that the processing rules are applications. Pet. 30–31 (citing Ex. 1004, 14:28–15:1; Ex. 1003 ¶¶ 111–112). We determine that the Petition and supporting evidence show that Nortel in view of the knowledge of a person of ordinary skill in the art teaches the additional limitations of claims 10 and 12 and would have rendered claims 10 and 12 obvious.

Claim 16 recites "wherein the plurality of applications includes a monitoring application and a network data processing application, wherein the monitoring application includes an intrusion detection application and wherein the network data processing application includes at least one of a URL filter, a content filter, a firewall, and an intrusion prevention application." Petitioner contends Nortel, in view of the knowledge of a person of ordinary skill, teaches this limitation for the reasons discussed for claim 10. Pet. 33. Petitioner also contends Nortel teaches this limitation in teaching a virtual private network with encryption and tunneling, which is intrusion prevention. *Id.* (citing Ex. 1004, 14:31–32; Ex. 1003 ¶¶ 128–134). We determine that the Petition and supporting evidence show that Nortel in view of the knowledge of a person of ordinary skill in the art teaches the additional limitation of claim 16 and would have rendered claim 16 obvious.

Claim 17 recites "wherein the plurality of applications includes a plurality of monitoring applications for monitoring data flows at a plurality of protocol layers, wherein the plurality of monitoring applications includes at least one intrusion detection application for detecting intrusions at a portion of the plurality of protocol layers." Petitioner contends Nortel teaches this limitation in teaching processing rules for monitoring application layer protocols such as SMTP and TELNET, and transport layer protocols such as TCP and UDP. Pet. 33–34 (citing Ex. 1004, 23:1–29; Ex. 1014, 8–10; Ex. 1015, 4–5; Ex. 1003 ¶¶ 137–141). Petitioner also contends that Nortel teaches this limitation in teaching service policies and processing rules that perform intrusion detection, such as rules relating to firewall parameters. *Id.* at 34 (citing Ex. 1004, 14:28–15:1; Ex. 1003 ¶ 142). We determine that the Petition and supporting evidence show that Nortel in view of the knowledge of a person of ordinary skill in the art teaches the additional limitation of claim 17 and would have rendered claim 17 obvious.

Claim 18 recites "transmitting the identified data packets to be processed by a first application before being processed by a second application that is selected from a list consisting of an anti-virus application, a URL filter, a content filter, a firewall, an intrusion prevention service, and a database protection application." Claim 19 recites a similar limitation. Petitioner contends that "transmitting the identified packets to be processed by a first application before being processed by a second application" is taught by Nortel in view of the knowledge of a person of ordinary skill for the reasons discussed for claim 9. Pet. 34–35. Petitioner contends an "application that is selected from a list consisting of an anti-virus application, a URL filter, a content filter, a firewall, an intrusion prevention service, and a database protection application" is taught by Nortel in view of the knowledge of a person of ordinary skill for the reasons discussed for claim 10. *Id.* at 35. We determine that the Petition and supporting evidence show that Nortel in view of the knowledge of a person of ordinary skill in the art teaches the additional limitations of claims 18 and 19 and would have rendered claims 18 and 19 obvious.

C. Asserted Obviousness over Nortel and Stone: Claims 2–8, 14, and 15

1. Stone (Ex. 1005)

Stone discloses a method and apparatus for accelerated packet processing. Ex. 1005, Title. A protocol data unit processor transfers protocol data units, or data packets, within a communications network. *Id.* at Abstract, 1:31–35. The processor includes a preprocessor to establish subsequent processing requirements of a particular data packet. *Id.* Multiple preprocessors connected in either parallel or series may be used to increase the throughput of data packets. *Id.* at 11:59–61. In a parallel configuration, first and second preprocessors establish subsequent processing requirements of a particular received data packet. *Id.* at 12:58–65.

2. Claims 2–8, 14, and 15

Claim 2 recites "transmitting the identified packets in parallel to the applications includes parallel transmitting of the identified data packets to each of the identified application processor modules." Claim 14 recites a similar limitation. Petitioner, relying on testimony of Dr. Jakobsson, contends the cited art renders these limitations obvious because it would have been obvious to a person of ordinary skill in the art to apply Stone's teaching of parallel transmission to Nortel's ISN, such that the switch fabric transmits data packets in parallel to the packet service cards. Pet. 37–38 (citing Ex. 1004, 21:1–5, 22:31–32, 23:1–29, Figs. 4, 6A; Ex. 1005, 12:58–13:18, Fig. 4; Ex. 1003 ¶¶ 160–162), 42. Petitioner, relying on testimony of Dr. Jakobsson, contends a person of ordinary skill in the art would have applied Stone's parallel data transfer to the switch fabric of Nortel for the benefit of increasing the speed of transmitting a subscriber's data packets to the appropriate service cards. Pet. 43–46 (citing Ex. 1005, 11:59–61; Ex. 1003 ¶¶ 192–199). Dr. Jakobsson testifies that a person of ordinary skill in the art would have been motivated to transfer data packets in parallel between Nortel's switch fabric and packet service cards in order to increase the operating speed and efficiency of the system. Ex. 1003 ¶¶ 190–192 (citing Ex. 1012, 8; Ex. 1005, 11:59–61).

We credit Dr. Jakobsson's testimony and determine the Petition and supporting evidence articulates a reason with a rational underpinning that a person of ordinary skill in the art would have applied Stone's teaching of transferring data packets in parallel, to transfer data packets in parallel between Nortel's switch fabric and packet service cards, for the benefit of increasing speed as taught by Stone. We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Nortel and Stone would have rendered claims 2 and 14 obvious.

Claim 3 recites "parallel transmitting of the identified data packets to a plurality of applications configured on one of the identified application processing modules." Claim 15 recites a similar limitation. Petitioner, relying on testimony of Dr. Jakobsson, contends it would have been obvious to a person of ordinary skill in the art to apply Stone's parallel data transmission to Nortel's ISN, such that the processor interface in a single packet service card transmits data packets in parallel to each of the processor groups in cases where a single subscriber's data packets must be processed according to multiple processing rules. Pet. 39–40 (citing Ex. 1003 ¶¶ 166–169); 46–49 (citing Ex. 1004, 9:20–22, 20:7–8, 20:15–16, 22:31–32; Ex. 1012, 9–12; Ex. 1003 ¶¶ 202–209). Petitioner also contends that a person of ordinary skill in the art would have utilized parallel data transfer in Nortel's system for the reasons given in the discussion of motivation with respect to claims 2 and 14, namely, increasing speed and efficiency. Pet. 46; *see id.* at 47 ("It would have been obvious to a POSA that parallel data transfer of the data packets to each processing group in the packet service card would best accomplish the necessary processing, because parallel data transfer was well-known in the art to provide faster data throughput compared to serial data."). We agree with Petitioner and determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Nortel and Stone teach the additional limitations of claims 3 and 15 and would have rendered claims 3 and 15 obvious.

Claim 4 recites "the plurality of applications includes a monitoring application and a network data processing application." Petitioner contends Nortel teaches monitoring applications for the reasons discussed for claim 17. Pet. 40. Petitioner contends Nortel teaches network data processing applications in teaching policies and processing rules relating to priority in usage of buffer and bandwidth, traffic steering, and rules for accepting or dropping certain types of network traffic. *Id.* at 40–41 (citing Ex. 1004, 14:32–15:1, 23:24–27; Ex. 1003 ¶¶ 173–175). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Nortel and Stone teach the additional limitation of claim 4 and would have rendered claim 4 obvious.

Claim 5 recites "the monitoring application includes an intrusion detection application." Petitioner contends Nortel teaches this limitation in teaching firewall policies and processing rules, for the reasons discussed for claim 10. Pet. 41 (citing Ex. 1003 ¶¶ 176–177). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Nortel and Stone teach the additional limitation of claim 5 and would have rendered claim 5 obvious.

Claim 6 recites "the network data processing application includes at least one of a URL filter, a content filter, a firewall, and an intrusion prevention application." Petitioner contends Nortel teaches this limitation in teaching firewall policies and processing rules, for the reasons discussed for claim 10. Pet. 41 (citing Ex. 1003 ¶¶ 178–181). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Nortel and Stone teach the additional limitation of claim 6 and would have rendered claim 6 obvious.

Claim 7 recites "the plurality of applications includes a plurality of monitoring applications for monitoring data flows at a plurality of protocol layers." Petitioner contends Nortel discloses this limitation for the reasons discussed for claim 17. Pet. 42 (citing Ex. 1003 ¶¶ 182–183). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Nortel and Stone teach the additional limitation of claim 7 and would have rendered claim 7 obvious.

Claim 8 recites "the plurality of monitoring applications includes at least one intrusion detection application for detecting intrusions at a portion of the plurality of protocol layers." Petitioner contends Nortel discloses this limitation for the reasons discussed for claim 17. Pet. 42 (citing Ex. 1003 ¶¶ 184–185). We determine that the Petition and supporting evidence adequately show by a preponderance of the evidence that the combination of Nortel and Stone teach the additional limitation of claim 8 and would have rendered claim 8 obvious.

D. Asserted Obviousness over Alles and Lin: Claims 1, 9–13, and 16–19

1. Alles (Ex. 1006)

Alles relates to a system and method for providing desired service policies to subscribers accessing the Internet. Ex. 1006, 1:8–12. An ISN enables the provision of desired service policies to each subscriber. *Id.* at Abstract. The desired service policies for each subscriber are provided as an input. *Id.* The desired service policies are translated into processing rules. Each processing rule contains a classifier and associated action. *Id.* A classifier generally identifies the application data flows to which the action is applied to provide the desired service policies. *Id.* Each data bit group is classified to associate with a subscriber, and only the processing rules corresponding to the subscriber are applied to the data bit group, to provide the desired services. *Id.*

2. Lin (Ex. 1007)

Lin relates to a system and method for assigning packet data to one of several processors provided in a data switch. Ex. 1007, 1:15–18. A content addressable memory (CAM) having a search field, a mask and an output for each CAM location is used to determine a processor for processing IP packets, with each IP packet being received as a sequence of cells. *Id.* at Abstract. IP packets may be assigned to a processor (group) based on an examination of the header data, potentially including IP header and other higher layer protocols headers. *Id.* The search field of a CAM location is pre-stored with header data, and the bit positions to be searched in the location are specified by using a mask. *Id.* The output of the location identifies the processor group for executing packets with headers matching the search field, with only the bits specified by the mask being compared. *Id.* When a first cell of an IP packet is received, the header data is provided as an input to the CAM, and the output identifies the processor (group) for executing the IP packet. *Id.*

3. Claims 1, 9–13, and 16–19

Claim 1 recites "a plurality of application processing hardware modules, each configured with an application for processing data packets." Claim 13 recites a similar limitation. Petitioner contends Alles teaches these limitations in teaching a plurality of packet service cards, with each packet service card including a plurality of processor groups, and each processor group configured to process data using processing rules. Pet. 51–55 (citing Ex. 1006, Figs. 3, 4, 3:24–26, 9:44–58, 10:31–35, 10:57–65, 11:7–9, 11:15–

23, 11:46–51, 11:59–67; Ex. 1003 ¶¶ 219–223), 62. Petitioner, relying on testimony of Dr. Jakobsson, contends that the processing rules of Alles implement policies relating to firewalls, security, anti-spoofing, virtual private networks, encryption, and traffic steering, and that these functions were well-known in the art to be performed by applications. Pet. 53–55 (citing Ex. 1006, Fig. 5A, 7:51–60, 7:62–8:3; Ex. 1003 ¶¶ 224–227).

We agree with Petitioner and rely on Alles's teaching of a processor group configured with processing rules to provide service policies such as security functions, and Dr. Jakobsson's testimony that a person of ordinary skill in the art would have understood that security functions are provided by software applications, both of which are cited above, to determine that Alles, in view of the knowledge of a person of ordinary skill in the art, teaches "a plurality of application processing hardware modules, each configured with an application for processing data packets" as recited in claim 1 and in the similar limitation of claim 13.

Claim 1 recites "a subscriber profile for identifying data packets associated with the subscriber profile in a stream of data packets." Claim 13 recites the same limitation. Petitioner contends that this limitation is taught by the combination of Alles and Lin. Pet. 56, 62. Petitioner, relying on testimony of Dr. Jakobsson, contends Alles teaches identifying incoming data packets using IP addresses, and associating the data packets with a subscriber. Pet 56 (citing Ex. 1006, 2:44–55, 2:64–3:5, 4:43–56, 55:46–55, 6:16–21, 7:62–8:3, 8:53–9:25, 10:36–50; Ex. 1003 ¶¶ 231–232). Petitioner, relying on testimony of Dr. Jakobsson, contends Lin teaches storing an IP address in a CAM, and examining the IP address of an incoming data packet to identify a subscriber. Pet. 56 (citing Ex. 1007, Abstract, 2:51–67, 4:48–

60, 10:6–20, 10:49–65, 11:21–52; Ex. 1003 ¶¶ 233–234).

Patent Owner contends that the combination of Alles and Lin does not teach the claimed "subscriber profile" because, according to Patent Owner, the classifiers of Alles and Lin do not identify incoming data packets and are not stored in CAM. PO Resp. 54–58 (citing Ex. 1007, 2:51–59, 6:40–55, 9:57–62, 9:66–10:1, 10:49–65, 11:53–56; Ex. 1006, 7:64–66; Ex. 2006 ¶¶ 106–108, 115–117, 127). Patent Owner contends that the classifiers of Alles and Lin are part of processing rules applied by packet service cards, which are separate from CAMs. *Id.* at 58–60 (citing Ex. 1007, 7:22–24; Ex. 1006, 12:26–31; Ex. 2006 ¶ 127). Patent Owner contends that Dr. Jakobsson's testimony regarding the classifier and service policy taught by the combination of Alles and Lin is not supported by the disclosures of Alles and Lin. *Id.* at 60–62 (citing Ex. 1006, 2:47–48, 7:62–63, 11:49–51; Ex. 1007, 17:65–67; Ex. 2007, 85:2–6, 119:22–120:6; Ex. 2006 ¶¶ 114–130).

Alles teaches that a classifier specifies a data flow and any corresponding conditions, and that the data flow may be uniquely identified using, inter alia, the destination IP address. Ex. 1006, 7:64–8:2. Lin teaches examining the header of an IP packet to determine the specific subscriber related to the IP packet by matching a destination IP address of the packet with that of a destination IP address stored in CAM. Ex. 1007, 2:36–38, 10:49–65, 11:8–10, 11:29–30. We are not persuaded by Patent Owner's contention that the data for destination IP addresses stored in the classifiers of Alles are not the same as the data for the destination IP addresses stored in the CAM of Lin. Storing an IP destination address of a specific subscriber in CAM in order to identify data packets having a matching destination IP address is sufficient to meet the claim language "a subscriber profile for identifying data packets associated with the subscriber profile in a stream of data packets."

Also, we are not persuaded by Patent Owner's contention that Dr. Jakobsson's testimony is not supported by the disclosures of Alles and Lin. We determine that Dr. Jakobsson's testimony that the classifiers of Alles and the CAM of Lin use a destination IP address to identify a subscriber is supported by the cited portions of these references. Ex. 1003 ¶¶ 230–237 (citing Ex. 1006, 2:47–54, 4:43–56, 5:46–55, 6:16–21, 7:64–8:2, 8:53–9:25, 10:44–50, 12:27–29; Ex. 1007, Abstract, 2:51–67, 4:48–60, 10:6–20, 10:49–65, 11:27–30, 11:35–52, 11:58–60).

We rely on Alles's teaching of an IP address that associates a data packet with a subscriber; Lin's teaching of using an IP address associated with a subscriber and stored in CAM to examine the IP address of a received data packet and identify the subscriber, and creditDr. Jakobsson's testimony, all of which are cited above, in determining that the combination of Alles and Lin teaches "a subscriber profile for identifying data packets associated with the subscriber profile in a stream of data packets."

Claim 13 recites "a security policy for determining a portion of the identified data packets to be processed by each of the applications." Petitioner contends Alles teaches this limitation in teaching each processing rule contains a classifier and an associated action, the classifier identifies data packets to which the associated action is applied, and the switch fabric forwards the data packets to designated processor groups for processing in accordance with the classifiers and actions specified by the processing rules. Pet. 62–63 (citing Ex. 1006, 2:45–51, 7:63–8:3; Ex. 1003 ¶¶ 267–268). We agree with Petitioner's showing that Alles teaches this limitation.

Claim 1 recites

> a network processing module for identifying one or more of the plurality of application processing modules for processing the identified data packets based on an association of the application configured on each application processing module with the subscriber profile and for transmitting the identified data packets in at least one of series and parallel to the identified application processing modules based on the security policy.

Claim 13 recites a similar limitation. Petitioner, relying on the testimony of Dr. Jakobsson, contends the combination of Alles and Lin teaches these limitations in teaching switch fabric 340 for identifying one or more packet service cards 350-A, 350-B for processing the identified data packets (Ex. 1006; Fig. 3, 4:43–49, 5:34–37, 9:6–9, 10:24–50) by using the CAM to identify the processors providing the service policies for the subscriber's data packets, and forwarding the identified data packets to the identified processors (Ex. 1007, Abstract, 2:51–67, 10:6–20, 10:49–65). Pet. 57–59 (citing Ex. 1006, Fig. 3, 10:24–50; Ex. 1007, Abstract, 10:6–20, 10:49–65; Ex. 1003 ¶¶ 239–248), 63.

Patent Owner contends that the combination of Alles and Lin does not teach these limitations because Petitioner argues that the identification of the processor is based on the subscriber, not the application. PO Resp. 46–49 (citing Pet. 57; Ex. 1007, Figs. 2A, 2B, 2:54–59, 4:21–26, 10:16–21, 10:49–61; Ex. 2006 ¶¶ 105–108). We are not persuaded by Patent Owner's contention that the combination of Alles and Lin does not teach identifying a processor "based on an association of the application configured on each application processing module with the subscriber profile" as claimed. Lin discloses a node that uses CAM to assign each IP packet associated with a subscriber to a processor designed to provide the service policies desired by the subscriber. Ex. 1007, 2:28–35. Lin teaches that the CAM stores an IP destination address associated with the subscriber, and stores data identifying a processor capable of providing the desired service policies to the associated subscriber. *Id.* at 2:36–43, 2:51–59. In other words, associating an IP destination address that identifies a subscriber with a processor group that applies processing rules capable of providing the subscriber's desired service policies meets the limitation "identifying one or more of the plurality of application processing modules for processing the identified data packets based on an association of the application configured on each application processing module with the subscriber profile" as recited in claim 1 and the corresponding recitation of claim 13.

Patent Owner contends that Alles teaches adding service policies to processors after a data flow begins, which means that a CAM cannot identify a processor based on an association of the service policy configured on the processor with the subscriber profile. PO Resp. 49–51 (citing Ex. 1006, 8:11–37; Ex. 2006 ¶¶ 109–111). We are not persuaded by Patent Owner's contention that Alles teaches adding service policies to processors after a data flow begins. Contrary to Patent Owner's contention, Alles teaches generating a rule for a subscriber dynamically after an IP address is allocated to a subscriber, not adding service policies to processors after a data flow begins. Ex. 1006, 8:18–30. Further, Alles also teaches generating processing rules up-front. *Id.* at 8:11–12. Because Alles teaches that the processing rules are generated up-front at least some of the time, it is irrelevant that Alles may also disclose other modes of generating processing rules. *See Unwired Planet, LLC*, 841 F.3d at 1002.

Patent Owner contends that Petitioner alleges that processing rules are applications, not service policies. PO Resp. 51–52 (citing Pet. 53). We are not persuaded by this contention. Petitioner contends that Alles discloses that processing rules implement service policies relating to, inter alia, security and encryption, and that these functions were well-known in the art to be performed by applications. Pet. 54 (citing Ex. 1006, Fig. 5A, 7:51–60, 7:62–8:3; Ex. 1012, 4, 6; Ex. 1013, 4; Ex. 1014, 3; Ex. 1003 ¶¶ 224–226). Petitioner contends that a person of ordinary skill in the art would have understood that Alles discloses software instructions to perform specific functions, such as a corresponding action for each rule as shown in Figure 5A of Alles. *Id.* at 55 (citing Ex. 1006, Fig. 5A; Ex. 1003 ¶¶ 228–229). We agree with Petitioner and determine that the processing rules of Alles which include service policies teach "applications" within the meaning of claims 1 and 13.

Dr. Jakobsson testifies that the identification of the packet service card to which the data packet is forwarded is based on (a) the subscriber to whom the data relates, and (b) an association of the application configured on each application processing module with the subscriber profile. Ex. 1003 ¶¶ 239– 240. Dr. Jakobsson testifies that

> by using the CAM to identify the processors capable of providing the service policies for the subscribers associated with the incoming data, the switch fabric 340 identifies "one or more of the plurality of application processing modules for processing the identified data packets based on an association of the application configured on each application processing module with the subscriber profile."

Id. ¶ 241. We credit Dr. Jakobsson's testimony and determine that the combination of Alles and Lin teaches this limitation.

Petitioner, relying on testimony of Dr. Jakobsson, contends that a person of ordinary skill in the art would have modified the ISN of Alles to include the CAM of Lin, for the benefit of quickly and efficiently routing data packets to appropriate processor groups as taught by Lin. Pet. 66–68 (citing Ex. 1003 ¶¶ 293–295). Petitioner also contends that combining the ISN of Alles with the CAM of the ISN of Lin is the combination of known elements according to known methods that yields predictable results. *Id.* at 69 (citing Ex. 1003 ¶ 298). We agree with Petitioner and credit Dr. Jakobsson's testimony cited above in determining that the Petition and supporting evidence provides a reason with a rational underpinning for adding the CAM of Lin to the ISN of Alles.

Petitioner, relying on testimony of Dr. Jakobsson, contends that it would have been obvious to a person of ordinary skill in the art that the processing rules of Alles comprise applications, because a person of ordinary skill would have understood the term "application" to include software or instructions to perform specific functions on a computer, such as the security functions of Alles. Pet. 69–70 (citing Ex. 1003 ¶¶ 299–306). We credit Dr. Jakobsson's testimony and determine the Petition and supporting evidence shows that a person of ordinary skill in the art would have understood the processing rules taught by Alles comprise software instructions to perform specific functions, such as security related anti-virus functions, and that a person of ordinary skill would have considered the software instructions to perform security related functions to be applications.

For the reasons given above, we determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles and Lin would have rendered claims 1 and 13 obvious.

Claim 9 recites "wherein transmitting the identified packets in series to the applications includes transmitting the identified data packets to be processed by a first application before being processed by a second application." Claim 11 recites a similar limitation. Petitioner contends these limitations are taught by Lin's teaching of assigning processing rules for one subscriber to one packet service card, and Alles's teaching of applying processing rules in an order to ensure predictable and desirable service policies. Pet. 60–61 (citing Ex. 1007, 7:32–38; Ex. 1006, 9:26–28; Ex. 1003 ¶¶ 250–252). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles and Lin would have rendered claims 9 and 11 obvious.

Claim 10 recites "the second application is selected from a list consisting of an anti-virus application, a URL filter, a content filter, a firewall, an intrusion prevention service, and a database protection application." Claim 12 recites a similar limitation. Petitioner contends these limitations are taught by Alles's teaching of rules for firewall parameters, and that a person of ordinary skill in the art would have understood that the processing rules of Alles are implemented through applications. Pet. 61 (citing Ex. 1007, 7:51–60; Ex. 1003 ¶¶ 254–256). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles and Lin would have rendered claims 10 and 12 obvious.

Claim 16 recites "wherein the plurality of applications includes a monitoring application and a network data processing application, wherein the monitoring application includes an intrusion detection application and wherein the network data processing application includes at least one of a

URL filter, a content filter, a firewall, and an intrusion prevention application." Petitioner contends the combination of Alles and Lin teaches this limitation for the reasons discussed for claim 10. Pet. 63–64. Petitioner also contends Alles teaches this limitation in teaching a virtual private network with encryption and tunneling, which is intrusion prevention. *Id.* (citing Ex. 1006, 7:56–57; Ex. 1003 ¶¶ 272–278). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles and Lin would have rendered claim 16 obvious.

Claim 17 recites "wherein the plurality of applications includes a plurality of monitoring applications for monitoring data flows at a plurality of protocol layers, wherein the plurality of monitoring applications includes at least one intrusion detection application for detecting intrusions at a portion of the plurality of protocol layers." Petitioner contends Alles teaches this limitation in teaching processing rules for monitoring application layer protocols such as SMTP and TELNET, and transport layer protocols such as TCP and UDP. Pet. 64 (citing Ex. 1006, 12:24–64, Fig. 5; Ex. 1014, 8–10; Ex. 1003 ¶¶ 281–287). Petitioner also contends that Alles teaches this limitation in teaching service policies and processing rules that perform intrusion detection, such as rules relating to firewall parameters. Pet. 65 (citing Ex. 1006, 7:51–60; Ex. 1003 ¶ 286). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles and Lin would have rendered claim 17 obvious.

Claim 18 recites "transmitting the identified data packets to be processed by a first application before being processed by a second application that is selected from a list consisting of an anti-virus application, a URL filter, a content filter, a firewall, an intrusion prevention service, and a database protection application." Claim 19 recites a similar limitation. Petitioner contends that "transmitting the identified data packets to be processed by a first application before being processed by a second application" is taught by the combination of Alles and Lin for the reasons discussed for claim 9. Pet. 65–66. Petitioner contends an "application that is selected from a list consisting of an anti-virus application, a URL filter, a content filter, a firewall, an intrusion prevention service, and a database protection application" is taught by the combination of Alles and Lin for the reasons discussed for claim 10. *Id.* We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles and Lin would have rendered claims 18 and 19 obvious.

E. Asserted Obviousness over Alles, Lin, and Stone: Claims 2–8, 14, and 15

Claim 2 recites "transmitting the identified packets in parallel to the applications includes parallel transmitting of the identified data packets to each of the identified application processor modules." Claim 14 recites a similar limitation. Petitioner, relying on testimony of Dr. Jakobsson, contends the cited art renders these limitations obvious because it would have been obvious to a person of ordinary skill in the art to apply Stone's teaching of parallel transmission to Alles's ISN, such that the switch fabric transmits data packets in parallel to the packet service cards. Pet. 70–71 (citing Ex. 1006, Fig. 3; Ex. 1005, 12:58–13:18, Fig. 4), 76. Petitioner, relying on testimony of Dr. Jakobsson, contends a person of ordinary skill in the art would have applied Stone's parallel data transfer to the combined teachings of Alles and Lin for the benefit of increasing the speed of transmitting a subscriber's data packets to the appropriate service cards. Pet. 71–72, 77–80 (citing Ex. 1003 ¶¶ 312, 339–347).

We credit Dr. Jakobsson's testimony cited above and determine the Petition and supporting evidence articulates a reason with a rational underpinning that a person of ordinary skill in the art would have applied Stone's teaching of transferring data packets in parallel, to transfer data packets in parallel between Alles's switch fabric and packet service cards, for the benefit of increasing speed as taught by Stone. We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles, Lin, and Stone would have rendered claims 2 and 14 obvious.

Claim 3 recites "parallel transmitting of the identified data packets to a plurality of applications configured on one of the identified application processing modules." Claim 15 recites a similar limitation. Petitioner, relying on testimony of Dr. Jakobsson, contends it would have been obvious to a person of ordinary skill in the art to implement the processor interface in a packet service card taught by the combination of Alles and Lin to transmit packets in parallel to each of the processor groups in the packet service card, as taught by Stone, for the benefit of more rapidly processing a user's data with multiple service policy requirements. Pet. 72–73, 80–83 (citing Ex. 1003 ¶¶ 318, 350–356). We agree with Petitioner for the reasons given by Petitioner and determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles, Lin, and Stone would have rendered claims 3 and 15 obvious.

Claim 4 recites "the plurality of applications includes a monitoring application and a network data processing application." Petitioner contends

Alles teaches monitoring applications for the reasons discussed in claim 17. Pet. 74. Petitioner contends Alles teaches network data processing applications in teaching policies and processing rules relating to priority in usage of buffer and bandwidth, traffic steering, and rules for accepting or dropping certain types of network traffic. *Id.* (citing Ex. 1006, 7:59–64, 12:59–64; Ex. 1003 ¶¶ 322–323). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles, Lin, and Stone would have rendered claim 4 obvious.

Claim 5 recites "the monitoring application includes an intrusion detection application." Petitioner contends Alles teaches this limitation in teaching firewall policies and processing rules. Pet. 74–75 (citing Ex. 1006, 7:51–60; Ex. 1003 ¶¶ 223–229). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles, Lin, and Stone would have rendered claim 5 obvious.

Claim 6 recites "the network data processing application includes at least one of a URL filter, a content filter, a firewall, and an intrusion prevention application." Petitioner, relying on testimony of Dr. Jakobsson, contends Alles teaches this limitation in teaching firewall policies and processing rules. Pet. 75 (citing Ex. 1003 ¶¶ 327–330). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles, Lin, and Stone would have rendered claim 6 obvious.

Claim 7 recites "the plurality of applications includes a plurality of monitoring applications for monitoring data flows at a plurality of protocol layers." Petitioner, relying on testimony of Dr. Jakobsson, contends Alles teaches this limitation in disclosing monitoring applications for monitoring data flows at a plurality of protocol layers. Pet. 75 (citing Ex. 1003 ¶¶ 331–332; Pet. 64–65). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles, Lin, and Stone would have rendered claim 7 obvious.

Claim 8 recites "the plurality of monitoring applications includes at least one intrusion detection application for detecting intrusions at a portion of the plurality of protocol layers." Petitioner, relying on testimony of Dr. Jakobsson, contends Alles teaches this limitation in disclosing firewall policies used to detect intrusions. Pet. 75–76 (citing Ex. 1003 ¶¶ 333–334; Pet. 74–75). We determine that the Petition and supporting evidence show by a preponderance of the evidence that the combination of Alles, Lin, and Stone would have rendered claim 8 obvious.

III. CONCLUSION

We determine that claims 1–19 of the '696 patent are unpatentable.

IV. ORDER

Accordingly, it is

ORDERED that claims 1–19 of U.S. Patent No. 9,525,696 B2 are unpatentable;

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

In summary:

Claims	**35 U.S.C. §**	**Reference(s)/Basis**	**Claims Shown Unpatentable**	**Claims Not Shown Unpatentable**
1, 9–13, 16–19	103	Nortel	1, 9–13, 16–19	
2–8, 14, 15	103	Nortel, Stone	2–8, 14, 15	
1, 9–13, 16–19	103	Alles, Lin	1, 9–13, 16–19	
2–8, 14, 15	103	Alles, Lin, Stone	2–8, 14, 15	
Overall Outcome			1–19	

PETITIONER:

Jeremy Lang
Donald Daybell
ORRICK, HERRINGTON & SUTCLIFFE LLP
ptabdocketjjl2@orrick.com
d2dptabdocket@orrick.com

Brian Chang
WEIL, GOTSHAL & MANGES LLP
brian.chang@weil.com

PATENT OWNER:

Chad Walters
Kurt Pankratz
Bryan Parrish
BAKER BOTTS LLP
chad.walters@bakerbotts.com
kurt.pankratz@bakerbotts.com
bryan.parrish@bakerbotts.com