Trials@uspto.gov
571-272-7822

Paper 32
Date: March 19, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

IPR2018-01512
Patent 9,565,213 B2

Before BRIAN J. McNAMARA, STACEY G. WHITE, and JOHN P. PINKERTON, *Administrative Patent Judges.*

McNAMARA, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 3[1]8(a)

I. BACKGROUND

On March 20, 2019, we instituted an *inter partes* review of claims 1–16 of U.S. Patent No. 9,565,213 B2 ("the '213 Patent"). Paper 8 ("Dec. to Inst."). Patent Owner filed a Patent Owner Response (Paper 15, "PO Resp."), Petitioner filed a Petitioner Reply (Paper 17, "Pet. Reply") and Patent Owner filed a Patent Owner Surreply (Paper 22, "PO Surreply"). A transcript of an oral hearing held on December 18, 2019 (Paper 31, "Hr'g Tr.") has been entered into the record. Patent Owner also filed a Motion to Exclude Evidence (Paper 24, "Mot. To Exclude"), Petitioner filed an Opposition to Patent Owner's Mot to Exclude (Paper 25,"Opp. to Mot. To Exclude") and Patent Owner filed a Reply to Petitioner's Opposition (Paper 29, "Reply To Opp. to Mot. To Exclude").

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. §318(a)(2018). We base our decision on the preponderance of the evidence. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d).

Having reviewed the arguments of the parties and the supporting evidence, we conclude that Petitioner has demonstrated by a preponderance of the evidence that the challenged claims are unpatentable.

II. THE '213 PATENT

The '213 patent discloses methods and systems for protecting a secured network. Ex. 1001, Abstract. Figure 1 of the '213 patent is reproduced below.

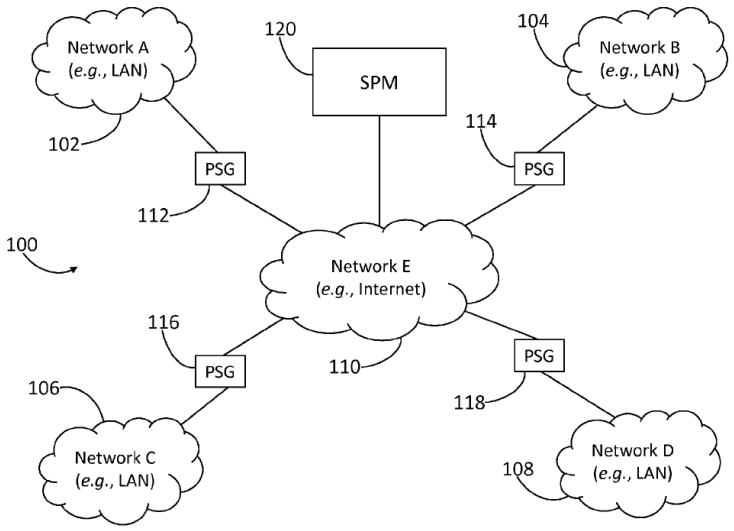


FIG. 1

Figure 1 of the ’213 patent illustrates a network environment that includes packet security gateways (PSGs) situated between networks and a security policy management (SPM) server that communicates dynamic security policies to the PSGs. *Id.* at 4:53–55, 4:66–5:3, Fig. 1. The PSGs perform packet transformation functions on received packets according to rules in a dynamic security policy in which “each rule may specify criteria and one or more packet transformation functions that should be performed for packets associated with the specific criteria.” *Id.* at 7:7–13. The patent explains that:

> The specified criteria may take the form of a five-tuple of values selected from packet header information, specifying a protocol type of the data section of the IP packet (e.g., TCP, UDP, ICMP, or any other protocol), one or more source IP addresses, one or more source port values, one or more destination IP addresses, and one or more destination ports.

Id. at 7:13–19, Fig. 3.

The ’213 patent describes packet transformation functions that forward packets into the network (e.g., Ex. 1001, 2:50–52), drop packets (*e.g., id*. at 2:57–59), or perform functions other than forwarding or dropping

the packets, (*e.g.*, *id.* at 1:49–51). For example, rules in a dynamic security policy may specify a transformation function that routes or switches packets to a network address corresponding to a monitoring device by encapsulating the packet with a header that corresponds to the network address of the monitoring device. *Id.* at 11:14–33. The monitoring device strips the header and copies the packets, or data within the packets, for subsequent review before forwarding the packets to the destination address. *Id.* at 11:22–33.

Various combinations of rules may implement services, such as a network threat awareness service in which a packet transformation function produces a digest or log of the packet, "e.g., associated network addresses, ports, protocol types, URIs, arrival times, packet sizes, directions, interface names, media access control (MAC) addresses, matching rule IDs, metadata associated with matching rules, enforced policy names, or the like." *Id.* at 11:36–54. Such packet logs can employ a logging standard, such as syslog, and be read by awareness application servers that perform transformations to produce awareness information that can be accessed by client applications. *Id.* at 11:54–60.

Figure 11 of the '213 patent is reproduced below.

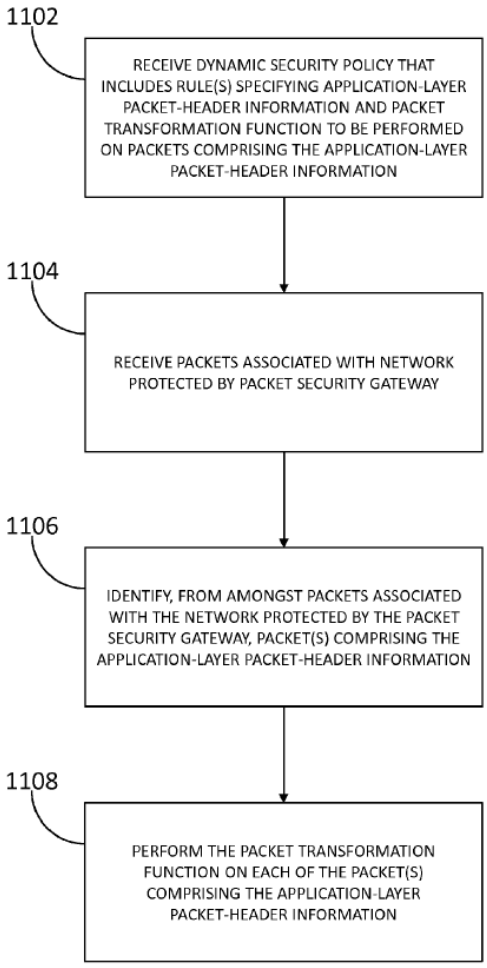


FIG. 11

Figure 11 of the ’213 patent “illustrates an exemplary method for protecting a secured network that includes identifying packets based on application-layer packet-header information.” Ex. 1001, 21:17–19. At step 1102, a plurality of PSGs (e.g., 112, 114, 116, and 118) associated with an SPM (120) receive a dynamic security policy that includes at least one rule (i.e., one or more rules) specifying application-layer packet-header information and a packet transformation function to be performed on packets comprising the application-layer packet-header information. *Id.* at 21:20–26. For example, one or more rules of the dynamic security policy received from the SPM may specify that: (1) the application-layer packet-header information

includes information that identifies one or more HTTP packets, and (2) the packet transformation function may accept or deny packets based on the specified application-layer packet-header information. *Id.* at 21:29–35.

At step 1104, a PSG receives packets from a computing device located in one of the protected networks. Ex. 1001, 21:35–43. At step 1106, the PSG identifies those packets associated with the protected network that comprise the specified application-layer packet-header information. *Id.* at 21:44–48. For example, if the rule specifies application-layer packet-header information that identifies one or more HTTP packets (e.g., one or more HTTP packets that comprise an HTTP GET method and/or an HTTP PUT method), the PSG may identify those packets as originating from and/or destined for a network address corresponding to URLs specified in the HTTP GET or HTTP PUT method call. *Id*. at 21:48–64.

At step 1108, the PSG performs the packet transformation function on each of the packets identified as comprising the specified application-layer packet-header information. Ex. 1001, 21:64–67. For example, the PSG may accept and forward the packets to their respective destinations or drop the packets. *Id.* at 21:67–22:6.

The method illustrated in Figure 12 of the ’213 patent is similar to that illustrated in Figure 11, except that instead of a dynamic security policy that performs a transformation function based on identifying application-layer packet-header information, the method illustrated in Figure 12 performs a transformation function that comprises a packet digest logging function based on specified packet identification criteria (e.g., application-layer packet-header information and/or a five-tuple specifying one or more transport-layer protocols, a range of source addresses, a range of source ports, a range of destination addresses, and a range of destination ports). *See*

Ex. 1001 22:7–23:18; *compare id.* at Fig. 11, *with id.* at Fig. 12. The packet digest logging function may generate a record comprising a subset of information for each identified packet, store the data temporarily at the PSG or send it to a different computing device, e.g., the SPMS, and may reformat the data according to a logging system standard. *Id.* at 22:60–23:18.

III. ILLUSTRATIVE CLAIM(S)

Independent claim 1, using the Petitioner's designation for each claim limitation as shown below, is illustrative.

1. **[1.1]** A method comprising:

receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information **[1.2]** and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information;

[1.3] receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;

[1.4] identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application layer packet-header information;

[1.5] performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises

[1.6] identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information;

[1.7] generating, for each of the one or more packets comprising the application-layer packet-header

information, a record comprising the subset of information specified by the packet digest logging function; and

[1.8] reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard; and

[1.9] routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function.

Id. at 25:14–55; *see* Petition ("Pet") 25–47 (including Petitioner's designation for each claim element).

Independent claim 10 generally parallels the language of independent claim 1, but recites that the dynamic security policy comprises at least one rule specifying "packet-identification criteria," instead of "application-layer packet-header information," and that the packet identifying criteria comprises a "Differentiated Service Code Point (DSCP) selector."

IV. GROUNDS OF INSTITUTION

A. Prior Art and Asserted Grounds

Petitioner asserts that the challenged claims would have been unpatentable on the following grounds:

Claims Challenged	35 U.S.C. §	References/Basis(s)
1–9	103(a)	ACNS[1], Kjendal[2]
10–16	103(a)	ACNS, Kjendal, Diffserv[3]

[1] Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5 (Ex. 1008)
[2] U.S. Patent No. 9,172,627 B2 (Ex. 1009)
[3] "An Architecture for Differentiated Services," Network Working Group Request for Comments 2475, The Internet Society, Dec. 1998 (Ex. 1011)

V. CLAIM CONSTRUCTION

The Petition has been accorded a filing date of August 20, 2018. Paper 6. For petitions accorded a filing date before November 13, 2018, we interpret claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs. LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016). In applying a broadest reasonable construction, claim terms generally are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). Any special definition for a claim term must be set forth in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

A. Dynamic Security Policy

In our Decision to Institute, we construed "dynamic security policy" to mean "any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria." *See* Dec. to Inst. 8–9. Petitioner agrees with our preliminary construction. Pet. Reply 1–3. Patent Owner's Response proposes that "dynamic security policy" be construed to mean "a non-static set of one or more rules." *See* PO Resp. 12–16. Patent Owner contends our preliminary construction alters the explicit language of the specification describing a dynamic security policy as one that *includes* any rule, message, etc. *Id.* at 13 (citing Ex. 1001, 2:58–63), PO Surreply 4–5. According to Patent Owner, a rule itself is not a dynamic security policy, but only part of a dynamic security policy. *Id.*

Patent Owner's proposed construction that a dynamic security policy be a *set of one or more* rules is inconsistent with its argument that a rule may not be a policy, as under Patent Owner's construction *one* rule may constitute a dynamic security policy. Our preliminary construction that *any* rule, message, etc., may be a dynamic security policy does not preclude a policy of more than one rule and is consistent with the Specification's description in the singular that "[a]s used herein" a dynamic security policy "includes any rule, message," etc. (*see* Ex. 1001 4:58–63) and "may include one or more rules" (*id.* at 6:11–12). Such a "dynamic security policy may utilize the combination of one or more rules to create policies for governing packets within a network environment or effectuating one or more services within a network environment." Ex. 1001, 8:34–37.

Patent Owner further argues that our construction removes any patentable weight from the word "dynamic" because it does not explicitly state that the policy is "non-static." PO Resp. 15–16. Patent Owner does not point to any use of the expression "non-static" in the '213 patent Specification. In some embodiments, a dynamic security policy may be constructed or revised manually off line and loaded into SPMS's memory by an administrator (Ex. 1001, 14:23–47); in other embodiments the SPMS may be configured to add, remove, or alter one or more dynamic security policies based on information received from devices within the network known to be associated with malicious traffic (*id*. at 14:48–15:37). As discussed above, however, the Specification explicitly states, "[a]s used herein, a dynamic security policy includes any rule message, instruction, file data structures, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria." *Id.* at 4:58–64. As our construction

is consistent with that language, we decline to adopt Patent Owner's construction and apply our preliminary construction in the Decision.

B. Monitoring Device

In our Decision to Institute, we preliminarily construed "monitoring device" to mean "a device configured to copy (or store) packets or data contained within them." *See* Dec. to Inst. 14–15. Petitioner agrees with our construction. Pet. Reply 3–4. Patent Owner contends that we should construe "monitoring device" according to its plain and ordinary meaning, which Patent Owner defines as "a device configured to monitor packets." PO Resp. 18–19; PO Surreply 5–6. Patent Owner's construction merely replaces the adjective "monitoring" with the infinitive form "to monitor"—it does not provide any context to the term "monitor." We further note that neither claim 1 nor claim 10 expressly states that the monitoring devices actually monitors, or in any way observes, the packets. Instead the claims merely state that packets are routed to a monitoring device, without reciting what, if anything, the monitoring device does with the packets.

We construe the recited "monitoring device" in view of the Specification. As we noted in the Decision to Institute, the '213 patent describes a packet transformation function as forwarding packets to a monitoring device in the context of a voice over internet protocol (VoIP) call, where the monitoring device copies or stores packets or data contained within the packets for subsequent review, e.g., by law enforcement. Dec. to Inst. 14–15 (citing Ex. 1001, 16:54–17:21). We also noted that the '213 Specification discusses similar functions performed by the monitoring device in the context of logging. *Id.* at 15 (citing Ex. 1001, 11:26–31). Patent Owner has not identified any other functions performed by the claimed monitoring device. Thus, for purposes of this Decision, consistent

with the Specification, we apply the construction adopted in the Decision to Institute and construe "monitoring device" to mean "a device configured to copy (or store) packets or data contained within them."

C. Packet

Neither party proposed a construction of "packet" prior to institution. Patent Owner's Response proposes that the term "packet" be construed to mean a packet at layer 2 (data link layer [L2]) or layer 3 (network layer [L3]) of the Open Systems Interconnection (OSI) seven layer model. *See* PO Resp. 9–12. Patent Owner states that, as agreed by Petitioner's expert Dr. Kevin Jeffay, packets received by the PSGs and identified on a packet-by-packet basis as including application-layer packet-header information in the '213 patent are not application-layer packets. *Id.* at 10–11 (citing Ex. 1004, Jeffay Decl. ¶ 51, including Dr. Jeffay's diagram depicting embedding of protocol data units during the transmission process). Patent Owner explains that, in one embodiment, the PSG is implemented in a network-layer transparent manner in which the PSG may send and receive traffic at the link layer using an interface not addressed at the network layer, and simultaneously perform the packet transformation function at the network layer. *Id.* at 11 (citing Ex. 1001, 3:4–9). Alternatively, the PSG includes a network interface having a network-layer addressable address. *Id.* (citing Ex. 1001, 3:10–13). Patent Owner further notes that the '213 patent explicitly states that packet transformation functions operate at the network layer, even when the PSG operates in a network-layer transparent manner. *Id.* at 11–12 (citing Ex. 1001, 6:38–41). Finally, Patent Owner argues that Petitioner's expert Dr. Jeffay agrees that the routing by the PSG on a packet-by-packet basis to a monitoring device refers to a process carried out by a

layer-3 network interconnection, such as a router. *Id.* at 12 (citing Ex. 1004, Jeffay Decl. ¶ 40).

Petitioner does not oppose Patent Owner's proposed construction—instead, as discussed further herein, Petitioner argues that the asserted prior art discloses receiving Layer 2 and Layer 3 packets. Pet. Reply 6–12.

We find Patent Owner's proposed construction of "packet" to be consistent with the use of the term in the context of the '213 patent. Thus, for purposes of this Decision, we construe "packet" to mean an L2 or L3 packet.

D. Rules

In our Decision to Institute, we construed "rule(s)" to mean "a condition or set of conditions that when satisfied cause a specific function to occur." Dec. to Inst. 9–10. Neither party disputes this construction, and we find, in light of the full record, that it is the broadest reasonable construction. Thus, we apply it in this Decision. Patent Owner notes that in our Decision to Institute, we stated the claim language is unclear as to whether (1) the dynamic security policy includes (i) a rule specifying criteria and (ii) a packet transformation function or (2) that the dynamic security policy includes rules specifying both the criteria and the packet transformation function. PO Resp. 16–17 (citing Dec. to Inst. 10). Patent Owner argues that the latter understanding comports with the claim language. We note that the Specification states "[e]ach rule may specify criteria and one or more packet transformation functions that should be performed for packets associated with the specified criteria." Ex. 1001, 7:10–13. It is not necessary, however, for us to resolve the issue for purposes of this Decision, as only those terms which are in controversy need to be construed and only

to the extent necessary to resolve the controversy. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc*., 200 F.3d 795, 803 (Fed. Cir. 1999).

E. Security Policy Management Server (SPMS)

In our Decision to Institute, we construed "security policy management server (SPMS)" to mean "a server configured to communicate a dynamic security policy to a packet gateway." Dec. to Inst. 10–11. Neither party disputes this construction, and we find, in light of the full record, that it is the broadest reasonable construction. Thus, we apply it in this Decision.

F. Packet Security Gateway (PSG)

In our Decision to Institute, we construed "packet security gateway (PSG)" to mean "a gateway computer configured to receive packets and perform a packet transformation function on the packets." Dec. to Inst. 11. Neither party disputes this construction, and we find, in light of the full record, that it is the broadest reasonable construction. Thus, we apply it in this Decision.

G. Packet Transformation Function

In our Decision to Institute, we construed packet transformation function" to mean "operations performed on a packet." Dec. to Inst. 11–13. Although Patent Owner maintains "packet transformation function" should be construed to mean "a function that transforms one or more packets from one state to another," Patent Owner states that it applied our construction for purposes of this proceeding. PO Resp. 18. As we stated in our Decision to Institute, Patent Owner's proposed construction is not meaningful because it uses a variation of the term "transform" to define "transformation." Dec. to Inst. 12–13. Our Decision to Institute also noted:

> the packet transformation function may perform a number of operations, such as: forwarding packets to the network or an IPsec stack; dropping packets or sending them to an infinite sink (e.g., *id.* [Ex. 1001] at 6:19–31); routing packets to a network address corresponding to a monitoring device whose address may be different from the packet's destination network address, and encapsulating packets with an IP header specifying the address corresponding to the monitoring device (*id*. at 11:14–26); and producing a digest or log of the packet information (*id.* at 11:45– 54).

Dec. to Inst. 13. In consideration of the above, we apply the construction articulated in the Decision to Institute, and for purposes of this Decision, we also construe "packet transformation function" to mean "operations performed on a packet."

H. Packet-By-Packet

Neither party proposed a construction of the term "packet-by-packet" until Patent Owner filed its Surreply. *See* PO Surreply 1–3. Prior to Institution, neither party explicitly discussed the term "packet-by-packet" as a distinguishing feature of the claims. As justification for its last minute construction proposal in its surreply, Patent Owner contends that it drafted its Patent Owner Response on the basis of deposition testimony by Petitioner's expert that "packet-by-packet" means "you're working a packet at a time." *Id.* at 1–2 (citing PO Resp. 25; Ex. 2009, Transcript of April 18, 2019 Deposition Testimony of Dr. Kevin Jeffay ("Jeffay Tr. I"), 48:8–16). According to Patent Owner, although Petitioner did not dispute its expert's testimony that "working a packet at a time" is the correct construction, Petitioner's Reply asserts that "packet-by-packet" encompasses analyzing "more than one packet at a time." *Id.* at 2 (citing Pet. Reply 6–9; Ex. 1020, Jeffay Reply Decl. ¶17).

It is unusual that the parties have proceeded so far in this proceeding before providing argument as to the construction of "packet-by-packet." Indeed, we are not convinced that we should construe "packet-by-packet" when the phrase used in claim 1 is "on a packet-by-packet basis." Neither "packet-by-packet" or "on a packet-by-packet basis" are defined in the Specification. It is unclear from the '213 patent whether "on a packet-by-packet basis" requires inspecting every single packet, even if the preceding packet indicates there is no application-layer packet-header information in the following expected packet. *See*, *e.g.*, Ex. 1001 21:44–22:5, 22:37–59. On the other hand, as packets may arrive out of order, it appears that some inspection of each packet may be necessary. In the context of claim 1, it appears that the inclusion of the term "on a packet-by-packet basis" means performing the transformation function only on those packets that comprise the application-layer packet-header information specified in a rule. For example, claim 1 recites "identifying" such packets "on a packet-by-packet basis," and then "performing . . . the packet transformation function" on such packets.

The construction "working a packet at a time" offers little insight into what "on a packet-by-packet basis" actually means. At this late stage of the proceeding, we address this issue to the extent necessary for this Decision in our substantive analysis of the claims, as explained below.

VI. ANALYSIS OF PRIOR ART CHALLENGES

A. Introduction

To prevail on its challenges, Petitioner must demonstrate by a preponderance of the evidence that the claims are unpatentable. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). "In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it

challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc*. 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify "with particularity . . . the evidence that supports the grounds for the challenge to each claim")). This burden never shifts to Patent Owner. *See Dynamic Drinkware, LLC. v. Nat'l Graphics, Inc*., 800 F.3d 1375, 1378 (Fed. Cir. 2015) (*citing Tech. Licensing Corp. v. Videotek, Inc*., 545 F.3d 1316, 1326–27 (Fed. Cir. 2008)) (discussing the burden of proof in *inter partes* review). Petitioner cannot satisfy its burden of proving obviousness by employing "mere conclusory statements," but "must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness." *In re Magnum Oil Tools Int'l, Ltd.,* 829 F.3d 1364, 1380 (Fed. Cir. 2016).

A claim is unpatentable under 35 U.S.C. § 103(a) 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." *KSR Int'l Co. v. Teleflex Inc*., 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Additionally, the obviousness inquiry typically requires an analysis of "whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring

"articulated reasoning with some rational underpinning to support the legal conclusion of obviousness")).

B. Claims 1–9 as Obvious Over ACNS in View of Kjendal

1. ACNS

a) Description of ACNS

The Cisco Application and Content Networking System (ACNS) is a "software solution" for "setting up and managing content delivery and content caching services in a centrally managed environment." Ex. 1008, 25, 1-1[4]. An ACNS device can be configured to operate in one of the following modes: (i) Content Distribution Manager, (ii) Content Engine; (iii) Content Router or (iv) IP/TV Program Manager. *Id.* at 1-2–1-3. All ACNS devices are shipped from the factory as Content Engines and must be reconfigured to operate in other modes. *Id.* at 2-14. Initial set-up requires (i) enabling a Content Distribution Manager using an interactive setup utility or device mode global configuration in the Command Line Interface (CLI), (ii) enabling a Content Engine as a centrally managed device, and, (iii) if content routing will be used to route requests, enabling a Content Router. *Id.* at 1-2, 2-3, 2-6–7, Fig. 2-1.

"The primary role of a Content Distribution Manager is to perform centralized content and device management . . . [T]he Content Distribution Manager manages both content acquisition and distribution and also manages policy setting and configurations on individual Content Engines." *Id.* at 1-2. "Through the Content Distribution Manager GUI [Graphical User Interface], the network administrator can specify what content is to be

[4] Consistent with the Petition, we number the pages of the exhibits using the pagination printed in the original document, rather than the sequential page number of the exhibit. Pet. 19.

distributed and to whom." *Id.* As discussed further below, Petitioner analogizes the Content Distribution Manager to the claimed security policy management server ("SPM server" or "SPMS"). Pet. 20.

An ACNS Content Engine is "an 'in-line' device between end users and the Internet" that intercepts end user content requests, enforces policies to assure security and budgetary objectives are met, and can be used to "[a]uthenticate, monitor, log, and control web access from end users to implement corporate policies regarding work environment and system security." Ex. 1008, 1–9. Among other tasks, upon receipt of a content request, an ACNS Content Engine "[p]asses the request through 'rules,' which might rewrite certain headers, redirect the request, or otherwise manipulate the request." *Id*. at 1-9–10. "Content Engines can be centrally managed through the Content Distribution Manager or locally as separate standalone content caches." *Id.* at 1-2. Petitioner analogizes the Content Engine to the claimed packet security gateway ("PSG"). Pet. 21.

Content Routers "redirect client requests for content to the closest Content Engine containing the content" using "the Domain Name System (DNS) to ensure that the Content Router receives all requests for content." Ex. 1008, 1-2.

IP/TV Program Managers are used by a system administrator "to set up and manage IP/TV scheduled or on-demand programs, channels, recording, and file transfers among IP/TV Servers." *Id.* at 1-3.

Petitioner contends that ACNS Content Engines perform packet transformation functions, citing the description of Configuring Caching Services so that a Content Engine need not retrieve the same data multiple times. Pet. 23 (citing Ex. 1008, 8-1). According to Petitioner, based on the user's HTTP request packet for information, ACNS determines whether the

system is configured to allow the specific HTTP request method in the request packet, whether the system already has the information cached, and generating a log entry for the request. *Id.* (citing Ex. 1008, 8-23–24, disclosing that Content Engines accept or reject HTTP requests depending on whether the HTTP method is supported and that in HTTP 1.1 some request methods (e.g., GET, HEAD, or POST) are supported by default, a list of unsupported methods is maintained, and methods can be added to a list of supported methods the Creating New HTTP Method for Content Engine window).

ACNS also discloses that administrators can maintain in various formats transaction logs of the date and time of a request, the URL requested, whether there was a cache hit or miss, the type of request, the number of bytes transferred, and the source IP address. *See* Ex. 1008, 19-1. Content Engines can send for logging only transactions associated with HTTP request authentication failures, or send all the transactions. *Id.* at 19–21.

b) Public Availability of ACNS

Patent Owner contends Petitioner failed to demonstrate that ACNS constitutes a printed publication accessible to the public for purposes of qualifying as a prior art reference. *See* PO Resp. 19–22.

With its Petition, Petitioner submitted the Declaration of Eli Fuchs, who identifies himself as Senior Product Line Manager, Cisco Service Provider Video for Cisco Systems. *See* Ex. 1012 ("Fuchs Decl.") ¶ 1. Mr. Fuchs testified that in 2006 he was a Senior Engineering Manager in the product development team and worked on the team that created the ACNS system that is the subject of the ACNS Guide, i.e., the ACNS reference in this proceeding. *Id.* ¶ 3. Mr. Fuchs further testified that in 2007, he became

Senior Business Development Manager, Service Provider Video for Cisco Systems, where his responsibilities included sales support and interacting with customers in various ways. *Id.* ¶ 4. Mr. Fuchs also states that since 2011, he has been Senior Product Line Manager, service provider video, for Cisco Systems and in that role, he continues to work in the product areas that include content networking systems, such as the ACNS System. *Id.* According to Mr. Fuchs:

> As the current Senior Product Line Manager, Service Provider Video, and as past Senior Business Development Manager, Service Provider Video and Senior Development Manager for products including the ACNS product, I have personal knowledge concerning the records, documents, manuals, and guides relating to Cisco products that are made, kept, and disseminated by Cisco Systems, including records, documents, manuals, and guides relating to the ACNS System.

Id. ¶ 6. Mr. Fuchs testified that the ACNS System was available for purchase in the U.S. as least as early as 2008 and, consistent with its U.S. copyright notice date, the ACNS reference was developed by that time and provided to all customers purchasing the ACNS System through Cisco's website at www.cisco.com. *Id.* ¶¶ 7–8. Mr. Fuchs further stated that the ACNS software Guide proffered as Exhibit 1008 was generally available in the U.S. at least as early as 2008. *Id.* at ¶ 8.

Mr. Fuchs further states that release notes on Cisco's websites demonstrate that the ACNS reference was distributed prior to March 20, 2008. *Id.* ¶¶ 9–10, 13. As discussed below, we are persuaded that Mr. Fuchs's reference to March 20, 2008, and release notes on Cisco's website lacks context. During his deposition, Mr. Fuchs recalled seeing the March 20, 2008 date of the release notes on cisco.com, but it became clear that Mr. Fuchs had not attached the release notes to Exhibit 1008. Ex. 2021,

Transcript of Deposition of Eli Fuchs ("Fuchs Tr.") 34:3–38:10. Subsequent to Mr. Fuchs's deposition, Petitioner filed a Supplemental Declaration by Mr. Fuchs, accompanied by Exhibit 1028 ("Release Notes"), Exhibit 1029, and Exhibit 1030 (collectively, "ACNS Document History"). Mr. Fuchs testified he had inadvertently omitted Release Notes and ACNS Document History from his initial declaration. Ex. 1027 ("Fuchs Supp. Decl.") ¶ 3.

In his initial declaration, Mr. Fuchs notes that the intended audience for the ACNS reference was "a network administrator or similarly-positioned person at the customer who managed the network of the customer's enterprise computer systems." Ex. 1012 Fuchs Decl. ¶¶ 12–13. However, Mr. Fuchs also states that the ACNS reference was available to anyone on Cisco's website after its release in March 2008 and was not treated as confidential. *Id.* ¶ 15.

Patent Owner argues that Exhibit 1008 in this proceeding does not include a publication date, and Mr. Fuchs Declaration testimony is not based on the personal knowledge concerning the publication of ACNS, but on the results of a database search using the Google search engine. PO Resp. 20–21 (citing Ex. 2021, Fuchs Tr.24:20–25:19. Patent Owner also argues that the ACNS reference is no longer available at the Cisco website. *Id.* at 21 (citing Ex. 2004, Goodrich Decl. ¶ 63, testifying "the link that should have led me to the Ex. 1008 instead led me to an End-of-Life retirement notification. Accordingly, I was not able to access Ex. 1008 as of July 3, 2019." (footnote omitted)).

Although Exhibit 1008 does not provide a specific publication date, it bears a copyright notice dated 2006. Ex. 1008, 2. In his Supplemental Declaration, Mr. Fuchs states that Release Notes referenced in his first declaration (Ex. 1012, Fuchs Decl. ¶ 9), but inadvertently omitted from

Exhibit 1008 and now filed as Exhibit 1028, are dated May 12, 2006, i.e., well before March 20, 2008. Ex. 1027, Fuchs Supp. Decl. ¶ 3. Mr. Fuchs states he confirmed the Release Notes in Exhibit 1028 are those he referenced in his first declaration by checking the Internet Archives. *Id.* Mr. Fuchs notes that the Release Notes corroborate the availability of the ACNS Guide (Ex. 1008) at least as early as March 20, 2008, because the May 12, 2006 Release Notes state "[t]he most current Cisco documentation for the released products [ACNS] is available at Cisco.com" and the Release Notes instruct administrators who configure, monitor and manage device that run ACNS 5.5.1 software to "consult the ACNS Guide for information on 'creating rules patterns and configuring rule actions' in using the ACNS software." *Id.* at ¶¶ 4–5. We further note that the Release Notes are dated May 12, 2006 for ACNS Release 5.5.1-b7.

As discussed further in Section VII of this Decision, Patent Owner has objected to Mr. Fuchs's Supplemental Declaration and moved to exclude it as untimely and prejudicial and as a vehicle to circumvent Petitioner's service of supplemental evidence in response to Patent Owner's objections.

Patent Owner argues that Petitioner offers no explanation how Release Notes from May 12, 2006, in Exhibit 1028 corroborate the purported March 20, 2008 publication date of ACNS. We note, however that the summary of release notes in Exhibit 1029 also shows release notes for AACNS Release 5.5.1-b.7 dated May 12, 2006 (Ex. 1029, 4) and their latest update as of March 20, 2008 (*id.* at 1).

We agree that Mr. Fuchs's statement that "the earliest version number for the ACNS Software Release 5.5.1, was updated on March 20, 2008" is confusing. *See,* Ex. 1012, Fuchs Decl. ¶¶ 7, 8, 13. However, Exhibit 1008 concerns Release 5.5. *See also*, Ex. 1008, 28 (Related Documentation).

Nevertheless, Petitioner's statement and Mr. Fuchs's testimony that the ACNS Guide in Exhibit 1008 was available as early as March 20, 2008 does not preclude ACNS being available earlier.

We do not exclude Exhibits 1027–1029, but we do not rely on Mr. Fuchs's Supplemental Declaration or on Exhibits 1028–1030 in order to decide this issue. Notwithstanding the confusion resulting from Mr. Fuchs's testimony concerning March 20, 2008 and the omission of the Release Notes and ACNS Document History from his initial declaration, Mr. Fuchs testimony in his initial declaration concerning that date is consistent with Cisco having made ACNS available to the public well before the critical date of the '213 patent.

The issue before us is not the exact date Exhibit 1008 was accessible to the public, but whether ACNS was accessible to the public such that it serves as a prior art reference. Although Mr. Fuchs testified that he conducted a search using the Google search engine to locate the ACNS documentation and could not could not testify as to the exact date ACNS was available to the public, he also testified "I do know it's the general practice at Cisco that in order to release a product, you have to release documentation with it," that customers would be provided with product documentation, and that such documentation would generally be available online. Ex. 2021, Fuchs Tr. 25:15–26:12. Thus, even if he could not recall the exact dates, Mr. Fuchs testified to his extensive role in the production of ACNS and from his personal knowledge that the ACNS product was generally available in 2008. Ex. 1012, Fuchs Decl. ¶ 6. We are persuaded that the totality of the circumstances supports Mr. Fuchs's testimony that these documents were publically available. Cisco produced the ACNS Configuration Guide for Centrally Managed Deployments in Exhibit 1008,

the additional documentation referenced therein, and Release Notes for software updates for the ACNS product, for the use of its customers. This purpose would have been frustrated unless ACNS and its associated documentation were made available to the public. Thus, Mr. Fuchs original testimony is sufficient for us to find ACNS was accessible to the public.

Although we need not rely on Mr. Fuchs' Supplemental Declaration or on Exhibits 1028–1030, the circumstances surrounding the ACNS documentation are consistent with Exhibit 1008 having been available to the public at least as early as the March 20, 2008, i.e., the date identified in Mr. Fuchs' initial declaration (Ex. 1012, Fuchs Decl. ¶ 9). The 2006 copyright notice in the ACNS Guide for software version 5.5 proffered as Exhibit 1008 and the May 12, 2006 Release Notes for software version 5.5.1-b7 proffered as Exhibit 1028 are consistent with each other. Exhibit 1029 merely illustrates that the May 12, 2006 Release Notes would have been available to the public not later than March 20, 2008. Patent Owner does not dispute that these dates are all well before the critical date of the '213 patent.

2. Kjendal

Petitioner states that Kjendal "relates to monitoring traffic for analysis and security by sending copies of certain, identified packets to a monitoring or logging device, based on policies provided to the device." Pet. 24 (citing Ex. 1009, Abstract). Kjendal discloses a system in which network policies are defined and regulated through an administrator controlled network policy server device that transmits established policies to network interface devices known as packet forwarding devices. Ex. 1009, 2:59–66. Kjendal discloses, either selectively or on a regular basis, mirroring one or more packets or portions of packets to a destination other than the original intended destination as part of determining the application associated with a flow or

session being established. *Id.* at 7:43–60. Kjendal also discloses dynamic mirroring is not limited to facilitating the identification of computer applications running on a network. *Id.* at 8:59–61.

3. Overview of Claim 1

We begin by reviewing the relationship of the limitations of method claim 1, as identified by Petitioner.

Claim limitation 1.1 recites a packet security gateway receiving a dynamic security policy that comprises a rule specifying application-layer packet-header information and a packet transformation function.

Claim limitation 1.2 defines the packet transformation function as comprising a packet digest logging function to be performed on certain packets, i.e., those packets comprising application-layer packet-header information.

Claim limitation 1.3 recites receiving packets associated with the protected network.

Claim limitation 1.4 recites identifying from the packets received in limitation 1.3, on a packet-by-packet basis, those packets that comprise the application-layer packet-header information recited in the rule of claim limitation 1.1.

Claim limitation 1.5 recites performing, on a packet-by-packet basis, the packet transformation function recited in claim limitation 1.2 (i.e., the packet digest logging function) on each of the packets identified in claim limitation 1.4, i.e. those packets identified as comprising the application-layer packet-header information in the rule of claim limitation 1.1.

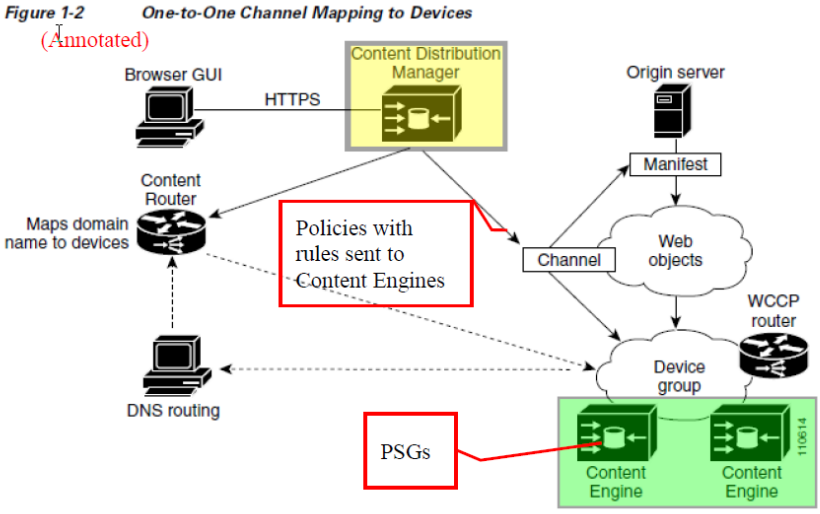
Claim limitations 1.6, 1.7, and 1.8 recite steps carried out in performing the packet transformation function recited in claim limitation 1.5. Specifically, claim limitation 1.6 recites identifying a subset of

information specified by the packet digest logging function (defined in claim limitation 1.2) for each of the packets comprising the application-layer packet-header information (i.e., those packets identified in claim limitation 1.4); claim limitation 1.7 recites generating a record for each of those packets comprising the application-layer header-information (i.e., those packets identified in claim element 1.4) of the subset of information specified by the packet digest logging function (claim limitation 1.6); and claim limitation 1.8 recites reformatting the subset of information (claim element 1.6) in accordance with a packet logging standard.

Claim element 1.9 recites the packet security gateway routing on a packet-by-packet basis the packets comprising the application-layer packet-header information (i.e., the packets identified in claim limitation 1.4) to a monitoring device in response to performing the packet transformation function (claim limitations 1.2, 1.5–1.8)

4. Claim Limitation 1.1

Claim 1 is drawn to a method. Petitioner identifies as claim element 1.1 the limitation that recites "receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information." Pet. 25. Petitioner's annotated version of Figure 1–2 of ACNS is reproduced below:



Pet. 26. Figure 1-2 depicts ACNS's content acquisition and distribution architecture. Ex. 1008, 1-11. Petitioner's annotated drawing identifies the ACNS Content Distribution Manager as corresponding to the claimed SPM transmitting policies with rules to Content Engines that correspond to the claimed PSGs. Pet. 26–27.

First, Petitioner contends that ACNS discloses at least two examples of "rules specifying application packet-layer information" that are part of a dynamic security policy provisioned to the Content Engines. *Id.* at 28. Citing the description in ACNS of Content Engines identifying HTTP packets and request methods associated with those packets and the ability to modify acceptable request methods, Petitioner contends that the rule is "dynamic." *Id.*at 28 (citing Ex. 1008, 8-23; Ex. 1004 ¶¶ 155–157).

Second, Petitioner cites the use of the ACNS Content Distribution Manager GUI to set up Internet Content Adaption Protocol (ICAP) rules for packet identification and field substitution as evidence in ACNS of rules specifying application-layer packet-header information in a dynamic policy provisioned by the Content Distribution Manager to the Content Engines. *Id.* at 29–30. Petitioner notes that, in ACNS, Content Engines can use ICAP

based servers to implement rules to identify specific HTTP application-layer packets and examine, filter, and modify fields with a substitution string, or re-route the HTTP packet, i.e. to transform application-layer packets. *Id.* (citing Ex. 1008, 16-13–23; Ex. 1004 Jeffay Dec. ¶ 158).

Patent Owner contends that: (i) ACNS does not disclose the claimed PSG (PO Resp. 23–24), (ii) ACNS does not disclose receiving dynamic security policies (*id.* at 24–28), and (iii) the policies in ACNS are not dynamic security policies (*id.* at 28–31).

We have construed packet security gateway (PSG) to mean "a gateway computer configured to receive packets and perform a packet transformation function on the packets." *See* § V.F. That construction is not disputed by the parties. In support of its first contention as to claim limitation 1.1, Patent Owner argues ACNS's "Content Engine cannot be a packet security gateway because the Content Engine does not inspect packets and does not perform any security analysis on packets." Pet. 23 (citing Ex. 2021, Fuchs Tr. 15:2–19 (testifying that the Content Engine does not perform any security analysis on a request and does not look at individual packets within a request)); *see also*, Ex. 2004, Goodrich Decl. ¶ 107.

Patent Owner's argument that ACNS does not perform security analysis is unpersuasive. After his deposition, Mr. Fuchs corrected this testimony, stating that upon reviewing ACNS, he recognized that the Content Engine can perform security analysis. Ex. 1027, Fuchs Supp. Decl. ¶ 6. As discussed above, we do not rely on Mr. Fuchs' testimony itself. However, notwithstanding Patent Owner's argument that given his position, Mr. Fuchs's revision of his deposition testimony is not credible (PO Surreply 12–13), Mr. Fuchs points to specific passages in ACNS indicate

that ACNS can perform security analysis. Ex. 1027, Fuchs Suppl. Decl. ¶ 6 (citing Ex. 1008, 1-9). Although Mr. Fuchs did not alter his deposition testimony that ACNS does not look at individual packets within a request, he did not know if in transaction logging, ACNS records information about individual packets in the transaction. Ex. 2021, Fuchs Tr. 15:16–19, 18:19–19:2

In further support of its argument that ACNS does not disclose the claimed PSG, Patent Owner cites the testimony of Petitioner's expert, Dr. Kevin Jeffay, that ACNS Content Engines are not capable of inspecting a payload of a packet for malware. PO Resp. 24 (citing Ex. 2020, Transcript of June 5, 2019 Deposition Testimony of Dr. Kevin Jeffay ("Jeffay Tr. II") 68:8–69:16); *see also* PO Surreply 13–14. Petitioner points out that this testimony is not particularly relevant because it concerns whether ACNS discloses searching application-layer packets, but Dr. Jeffay also testified the ACNS Content Engine looks to the packet header of an HTTP packet that can be embedded in a Layer 2 or Layer 3 packet to determine whether the HTTP packet is using a supported method. Pet. Reply 10–11 (citing Ex. 1020, Jeffay Reply Decl. ¶ 61). Although Dr. Jeffay acknowledges that "it [ACNS] doesn't allow you to, for example, directly inspect the payloads to see is there malware in a payload," he also states "ACNS will allow you to provide security functions related to -- associated with users or with content in the form of request methods or URLs." Ex. 2020, Jeffay Tr. II 67:10–15. Citing Kjendal, Dr. Jeffay explains

> given that you've determined that you don't want to support a particular method or you don't want a user to access particular content, combining Kjendal . . . would provide a facility where an ACNS user could then do analysis of the actual content of messages that have been flagged by the ACNS system by

> mirroring those packets to a monitoring device that could then do a further analysis of those packets and, in particular, do things like look at the payloads.

Id. at 67:16–68:3. Petitioner further notes that ACNS operates on packets because it can identify an HTTP request from the request information in the first packet and determine that each subsequent packet that is part of the same request is an HTTP packet. Pet. Reply 7–8.

Petitioner also argues that ACNS looks at each packet on a packet-by-packet basis using ICAP, as well as HTTP. *Id.* at 8. We agree that Petitioner has demonstrated ACNS acts on packets. We address the parties' competing contentions about "on a packet-by-packet basis" claim limitations in our discussion of claim limitations 1.2, 1.4 and 1.5.

Patent Owner next argues that ACNS does not disclose the Content Distribution Manager sending policies to a Content Engine, but instead the CDM is used "to directly alter a policy already being enforced thereon." PO Resp. 26. Patent Owner cites two such examples: (i) when an administrator manually adds an HTTP request method to a plurality of plurality of request methods previously configured in the Content Engine and (ii) when the administrator modifies one of the previously configured request methods. *Id.* (citing Ex. 1008, 8-24; Ex. 2004, Goodrich Decl. ¶¶ 109–114). According to Patent Owner, although ACNS allows an administrator to modify a policy implemented on a Content Engine, ACNS does not teach that Content Engines receive policies from a CDM. On this basis, Patent Owner contends that the record does not support Petitioner's contentions that ACNS discloses step-by-step instructions for generating a policy on the CDM. *Id.* at 27. Patent Owner's arguments are not persuasive. As Petitioner points out, the CDM provides a graphical user interface that the

administrator uses to configure a Content Engine, e.g., by adding new HTTP request methods to the list of those supported by the ACNS product. Pet. Reply 11. We agree with Petitioner that this constitutes the Content Engine receiving a dynamic security policy. *Id.*

Patent Owner further argues that ACNS's policies are not dynamic security policies because Petitioner's overly broad construction of "dynamic security policy" fails to give patentable weight to "dynamic." PO Resp. 28–31. According to Patent Owner, the set of rules used by the Content Engine in ACNS "is not a dynamic security policy because the rules must be manually added or modified by a user operating a GUI or a command line interface." *Id.* at 30. We are not persuaded by this argument. Our construction of "dynamic security policy" is not limited to policies that update automatically. *See* § V.A.

5. Claim Limitation 1.2

Petitioner identifies as claim element 1.2 the limitation that recites "a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information."

Petitioner cites ACNS as teaching packet transformation functions that include logging all packets or only some packets and, through a user interface, allowing a user to choose to log and to configure ACNS transaction logging functionality with a single policy to be sent from the Content Distribution Manager to one or more Content Engines. Pet. 31–34. Patent Owner argues that "transaction logs [in ACNS] are not logs of individual packets identified as having application-layer packet-header information." PO Resp. 31–32 (citing the language "performing . . . on a

packet-by-packet basis . . .” from claim limitation 1.5 (alteration in original)).

Petitioner states that “ACNS generally teaches packet transformation functions that can be logged only on packets that are identified by application-layer packet-header information,” but acknowledges that “ACNS does not explicitly state that its packet digest logging functions are performed on packets based on their meeting criteria in the two application-layer packet-header rules discussed above in element [1.1],” i.e., application-layer packet-header information identified by the HTTP request method or ICAP rules. Pet. 30–31 (citing Ex. 1004, Jeffay Decl. ¶ 165), 35; *see also* PO Resp. 33–34.

Instead, Petitioner cites Kjendal as disclosing “a system where application-layer packet-header information is used to determine what should be logged, noting that Kjendal teaches packets may be mirrored (i.e., sent to a network logger) based on dynamic rules specifying application-layer packet-header information, such as identification of application types. *Id.* at 31 (citing Ex. 1004, Jeffay Decl. ¶¶ 164–167), 35 (citing Ex. 1009, 10:23–33).

Petitioner argues that, recognizing ACNS discloses an administrator can perform real time transaction logging by sending only logs of HTTP authentication failures to the syslog server rather than logs of all transactions, a person of ordinary skill would understand that an administrator could selectively log other types of transaction information, as taught by Kjendal. Pet. 36–37. Thus, according to Petitioner, “given the teachings of Kjendal and ACNS, it would have been obvious to a POSA to implement the ACNS system such that the logging function logs packets based on application-layer packet-header rules.” *Id.* at 31.

Agreeing that "packet" in the context of the '213 patent means Layer 2 or Layer 3 packets, Patent Owner contends that ACNS concerns a content delivery network and does not concern Layer 2 or Layer 3 packets. Hr'g Tr. 29:18–30:13. As discussed further below, Petitioner does not deny ACNS is concerned with content delivery analysis, but argues that both the '213 patent and ACNS discuss HTTP requests and a GET method, e.g., as in claim 5, that reference to the request method is not mutually exclusive to looking at a network layer packet for security purposes, and that security analysis can be done on a packet-by-packet basis. *Id.* at 52:13–53:26. We address the packet-by-packet limitations further in our discussions of claim limitations 1.4 and 1.5.

According to Patent Owner, "simply sending a copy of a packet to a device called a 'network logger' is not a packed digest logging function." PO Resp. 34. As to Petitioner's reliance on Kjendal, Patent Owner responds that "mirroring a packet is **not** a packet digest logging function, regardless of where the mirrored packet is sent." *Id.* Patent Owner explains that sending a copy of a packet to a network logger is not the claimed packet digest logging function because that requires "identifying a subset of information," (claim limitation 1.6) "generating . . . a record comprising the subset of information," (claim limitation 1.7) and "reformatting . . . the subset of information," (claim limitation 1.8). *Id.* We address these individual claim elements separately below. Much of Patent Owner's discussion of Kjendal focuses on its contentions that, based on the differences between ACNS and Kjendal, a person of ordinary skill would not have been motivated to combine their teachings. *See id.* at 35–41. Therefore, we address Patent Owner's contentions in our discussion of the motivation to combine the teachings of ACNS and Kjendal.

a) Motivation to Combine the Teachings of ACNS and Kjendal

Noting that port-mirroring was deployed routinely on Cisco router systems, Petitioner contends that a person of ordinary skill would have found it obvious and straightforward to incorporate the specific packet monitoring teachings of Kjendal with the teachings of ACNS, including ACNS's teaching of selecting on a packet-by-packet basis those packets comprising selected application-layer packet-header information. Pet. 25.

Emphasizing its argument that ACNS concerns transaction logging, as opposed to logging individually identified packets, Patent Owner argues that the claimed packet transformation function "involves generating a record of each packet that includes a subset of the packet's information (*i.e.*, a packet digest) . . . and reformatting the subset of information in accordance with a logging system standard." PO Resp. 2–3. Patent Owner states that transaction logging in ACNS is a fundamentally different technique from that in Kjendal. *Id.* at 37. Stating that "ACNS never applies a security policy on individual in-transit packets," Patent Owner further argues that a person of ordinary skill would not have been motivated to combine the teachings of ACNS and Kjendal "because ACNS is concerned with analyzing at rest content (e.g., reassembled application layer messages) and not in-transit network traffic flow techniques taught by Kjendal and Diffserv." *Id.* at 3.

Noting that "[e]ach transaction in ACNS is typically spread over multiple packets," Patent Owner contends that transaction logging in ACNS does not log information about each packet, but "instead logs information about the transaction as a whole." *Id.* at 38. According to Patent Owner, a person of ordinary skill would have had no reason to combine the teachings

of Kjendal with ACNS because the combination does not address any known problem with transaction logging in ACNS. *Id.* at 40 (noting that ACNS "does not even mention a need to log individual packets to satisfy its security concerns."). Patent Owner states that, in contrast to ACNS, Kjendal's technique mirrors packets based on identifying criteria associated with traffic flow that would not identify a transaction. *Id.* at 39. According to Patent Owner, combining transaction logging in ACNS with traffic flow analysis of Kjendal to log only those packets that are of particular interest would change the operating principles of ACNS, requiring undue experimentation and producing unpredictable results. *Id.* at 30–41.

Petitioner responds that the flaw in Patent Owner's arguments concerning lack of motivation to combine the teachings of ACNS and Kjendal stems from a mischaracterization of ACNS as not teaching logging on a packet-by-packet basis. Pet. Reply 17. Petitioner cites HTTP transactions in ACNS that often fit within a single packet, arguing that in such circumstances logging information relating to a transaction is the same as logging information about a packet. *Id.*

Petitioner further argues that even where a transaction spans multiple packets, "the system may analyze the packets containing the transaction one at a time and in isolation, and would create a log from information extracted from the various packets in the group." *Id.* (citing Ex. 1020, Jeffay Reply Decl. ¶ 40 (referring to testimony in ¶¶ 33–34 of Ex. 1020, Jeffay Reply Decl. and in Ex. 1004, Jeffay Decl., ¶ 155, that a person of ordinary skill would have understood an application may recognize a packet as an HTTP packet based on the request method in the first line of the application-layer packet-header)).

Noting it is undesirable to overwhelm a syslog server by logging all packets, Petitioner states that ACNS logs only HTTP authentication failures and argues a person of ordinary skill would have been motivated to combine the teachings of ACNS and Kjendal because Kjendal teaches that problems associated with logging all packets can be addressed by selectively logging packets based on other types of information. *Id.* at 18. Accordingly, based on Petitioner's arguments and evidence, we find that ACNS and Kjendal "both log based on packets" and incorporating the teachings of Kjendal into ACNS does not change the principles on which ACNS operates. *Id.*

6. Claim Limitation 1.3

Petitioner identifies as claim element 1.3 the limitation that recites "receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway." Pet. 37. Petitioner cites the transmission of streaming media, as illustrated in Fig. 9-1 of ACNS, as disclosing Content Engines analogous to the claimed PSGs that receive packets associated with a network behind and protected by the Content Engines. *Id.* at 37–38. Petitioner states that ACNS also teaches "that Content Engines may be used as a proxy for a streaming server or broadcast server to replicate contents for multiple recipients." *Id.* at 38–39 (citing Ex. 1008 9–27, Fig. 9–12). Petitioner also cites ACNS as disclosing the ability of a user to view Content Engine statistics, including the number of packets sent and received. *Id.* at 39 (citing Ex. 1008, 21-14–18; Ex. 1004, Jeffay Decl. ¶ 171).

Patent Owner does not respond explicitly to Petitioner's contentions concerning claim limitation 1.3. We agree with Petitioner that ACNS's Content Engine would have been viewed as the claimed PSG and ACNS

discloses the PSG receiving packets associated with the network protected by the PSG.

7. Claim Limitations 1.4 and 1.5

We address claim limitations 1.4 and 1.5 together, as they both recite operations that are performed on a packet-by-packet basis. A significant dispute between the parties concerns the scope of the "packet-by-packet" limitation and whether it is disclosed by the references.

Petitioner identifies as claim limitation 1.4 the limitation that recites "identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application-layer packet-header information." Pet. 39.

Petitioner identifies as claim limitation 1.5 the limitation that recites "performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises." Pet. 41. As discussed above, claim limitation 1.2 defines the packet transformation function as a packet digest logging function. Thus, claim limitation 1.4 concerns the PSG identifying packets that comprise application-layer packet-header information and claim limitation 1.5 concerns the PSG carrying out the packet digest logging function on a packet-by-packet basis on those packets identified as comprising application-layer packet-header information.

a) Claim Limitation 1.4

As to claim limitation 1.4, the Petition cites ACNS as disclosing Content Engines examining the application-layer packet-headers of HTTP

packets to determine if the HTTP request method is supported by the Content Engine. Pet. 39–40. Alternatively, Petitioner contends that a Content Engine examines packet-header information through configuration of its ICAP protocol server functionality. *Id.* at 40. Patent Owner argues that Petitioner failed to demonstrate ACNS identifies packets with application layer packet information on a packet-by-packet basis. PO Resp. 41–46. Patent Owner argues that Dr. Jeffay acknowledged in his deposition that "ACNS is not capable of inspecting the payload of [Layer 2 or Layer 3] packets." *Id.* at 44 (citing Jeffay Tr. I 68:16–69:16). Petitioner contends that Patent Owner misstates Dr. Jeffay's testimony, noting that Dr. Jeffay's testimony concerned application-layer packets, not Layer 2 or Layer 3 packets. Pet. Reply 15 (citing Ex. 2020, Jeffay Tr. I, 65:19–69:16). Emphasizing that "his testimony is that ACNS does not disclose the ability to search payloads of application-layer packets," Petitioner states that "ACNS can analyze the packet headers of application-layer packets that are embedded within the payloads of Layer 2 or Layer 3 packets during communication." *Id.* (citing Ex. 1020, Jeffay Reply Decl. ¶¶ 32–33).

(1) Examining HTTP Packets

As an initial matter, Patent Owner argues a Content Engine, as described by ACNS, is a web proxy that must cache content and, for a web proxy to work, it must reassemble messages to send the request to an origin server and cannot work on a packet-by-packet basis. Hr' g Tr. 30:12–31:6.

ACNS states "Content Engines in an ACNS network save bandwidth and protect networks by acting as forward proxies that authenticate, filter, and cache all traffic between an organization's internal network and the Internet." Ex. 1008, 1-1; *see also* Pet. 47–48 (Petitioner's discussion of claim 2, citing the description in ACNS of the Content Engine as a "forward

proxy which receives requests from users and may either respond to the request with cached content, or forward the request to an outside server to obtain the content." (Ex. 1008, 8-23)).

According to Patent Owner in the '213 patent, "[b]ecause the packet identification criteria can include IP packet header and application-layer packet header information, the PSG is able to filter L2 or L3 (IP) packets on a packet-by-packet basis while the packets are in transit . . . . rather than reassembling application-layer messages." PO Resp. 5. Patent Owner states: "identify[ing] packets in real time, as they are being received in-transit . . . differentiates the PSGs of the '213 Patent from prior art content proxies, such as those disclosed in ACNS, which teaches applying rules to reassembled, at rest, application layer messages rather than in-transit packets." *Id.* at 2. As discussed below, Patent Owner does not cite sufficient evidence supporting its assertions limiting the '213 patent to real time identification of packets in transit.

Patent Owner cites the testimony of Petitioner's expert Dr. Jeffay acknowledging "[a] POSA would understand that a rule requiring [identifying] packe- header information . . . must first identify, on a packet-by-packet basis, each packet comprising [] application-layer packet header information." *Id.* at 42 (quoting Ex. 1004, Jeffay Decl. ¶ 173; citing Ex. 2009 Jeffay Tr. I 48:8–16) (alteratio9n in original). According to Patent Owner, ACNS does not include packet filtering rules that identify packets with specified application-layer packet-header information on a packet-by-packet basis because ACNS must reassemble payloads of packets of HTTP (web) communications flows before determining whether or not a web object should be cached or a request should be logged. *Id.* at 42. Noting Petitioner's reference to the disclosure in ACNS Chapter 8 as teaching

examining application-layer packet-header information of HTTP packets to determine whether a request method is supported by the Content Engine, Patent Owner states that ACNS must reassemble the L2 and/or L3 packets received by the Content Engine to identify the request method, because such requests are often spread over several L2 and/or L3 packets. *Id.* at 43 (citing Ex. 2004, Goodrich Decl. ¶ 128). Patent Owner emphasizes that "ACNS cannot identify application-layer packet header information in an HTTP request without reassembling the packets that make up the request because ACNS cannot inspect the payload of an L2 or L3 packet." *Id.* at 44; *see* § VI.B.3.

Petitioner points out that ACNS never mentions reassembly. Pet. Reply 6–7 (citing Ex. 1020, Jeffay Reply Decl. ¶33), Hr'g Tr. 11:5–7. Petitioner argues Patent Owner is wrong because ACNS does not have to operate that away and can identify application-layer packet-header information without reassembling application-layer packets. *Id.*; Pet. Reply 14. Petitioner notes that an application layer packet to be transmitted over the Internet is embedded in a TCP packet that in turn is embedded in a network layer packet, and that any packet smaller than 1500 bytes can be transmitted as one packet. Hr'g Tr. 11:14–21. Petitioner also notes the acknowledgment by Patent Owner's expert that many requests, such as HTTP GET or HTTP PUT are small enough to fit in a single packet. Pet. Reply 7 (citing Ex. 1026, Deposition Transcript of Dr. Goodrich ("Goodrich Tr.") 27:20–29:8). According to Petitioner, in those cases, ACNS necessarily operates on a packet-by-packet basis. *Id.* (citing. Ex. 1020, Jeffay Reply Decl. ¶ 32). Petitioner's arguments demonstrate that under certain circumstances, for example in short GET and PUT HTTP requests, ACNS effectively processes individual packets. Petitioner contends that

ACNS' disclosure of this embodiment is a sufficient teaching for purposes of finding obviousness. Hr'g Tr. 12:26–13:4.

Patent Owner also argues that ACNS is concerned with transactions and that a transaction cannot fit in one packet because a web proxy looks at the back and forth communications not just between it and the origin server, but also between the web proxy and the information it gets from the client it services. Hr'g Tr. 29:20–30:27. Petitioner notes, however, that claim 5 refers to HTTP requests and a GET method just as ACNS does.*Id.* at 52:13–53:21 (arguing that in ACNS, even if reassembly is required for content delivery analysis, reassembly is not required for security analysis). We do not construe claim 1 to be limited to the features recited in claim 5, but we do not exclude such features from claim 1.

Petitioner further argues that even where an HTTP request spans multiple packets, ACNS still teaches operating on packets on a packet-by-packet basis, e.g., where an application may recognize a packet as being an HTTP packet based on the request method in the first line of the application header. *Id.* at 7 (citing Ex. 1004, Jeffay Decl. ¶ 155; Ex. 1020, Jeffay Reply Decl. ¶ 33); Hr'g Tr. 13:17–15:2. Petitioner relies on Dr. Jeffay's testimony that when an HTTP request is made, the ACNS system can identify the request from the request information in the first packet and determine on a packet-by-packet basis that each subsequent packet that is part of the same request is an HTTP packet. *Id.* at 7–8 (citing Ex. 1004, Jeffay Decl. ¶ 155; Ex. 1020 Jeffay Reply Decl. ¶ 33; Ex. 1008, 8-23–8-24); *see also*, Hr'g Tr. 16:5–25, 17:1–18:8 (discussing implications of claims 4 and 5).

Patent Owner contends that Petitioner is wrong because ACNS must reassemble the L2 and/or L3 packets to identify an HTTP request. PO Surreply 8–10. According to Patent Owner, "ACNS cannot look at

individual packets as they come across the wire for application-layer packet header information, as required by the 'packet-by-packet' basis claim element." *Id.* at 9–10 (citing PO Resp. 41–45).

Patent Owner also argues that its TIG produc, which it purports implements the '213 patent, involves a tradeoff that forgoes deeper inspection of the application layer in favor of implementing rules on a packet-by-packet basis. PO Surreply 2 (citing Ex. 2004, Goodrich Decl. ¶ 165, Ex. 2007, 6 (Gartner article on security technology); Ex. 2006, 7–8 (Enterprise Strategy Group paper on cyberthreat technology)). We first note that Patent Owner's citation does not provide any technical analysis to support Patent Owner's assertion. More importantly, Patent Owner does not cite to any such statement in the '213 patent.

Patent Owner's approach to the term "packet-by-packet" appears to require an inspection of each L2 or L3 packet "as packets come across the wire" (*id.*) or are "in-transit" (PO Resp. 5). There is no such language in the claims. Patent Owner does not identify any disclosure in the '213 patent Specification that states explicitly the PSG's identification on a packet-by-packet basis of those packets comprising the application-layer packet-header information is performed on isolated packets "in transit" or as "they come across the wire."

As we noted in IPR2018-01386, the issue before us is not whether the reference discloses the exact steps claimed, but instead what it would have taught or suggested to one of ordinary skill in the art. *Cisco Sys., Inc. v. Centripetal Networks, Inc.*, IPR2018-01386, Paper 31 at 26 (PTAB Jan. 23, 2020)(Final Written Decision), noting that Petitioner did not rely on the Narayanaswamy reference to disclose packet-by-packet analysis, but to

disclose inspecting application-layer packet-header information (citing -01386 Pet. Reply 10–11).

As claim 1 does not recite limitations that define the meaning of "on a packet-by-packet basis," we turn to the Specification's description of Figure 11, which states that "[a]t step 1106, the packet security gateway may identify from amongst the packets associated with the network protected by the packet security gateway, and on a packet by packet basis, one or more packets comprising the application-layer packet-header information." Ex. 1001, 21:44–48. The Specification further states that the rule(s) specifying the application-layer packet-header information may identify one or more HTTP packets, e.g. one or more HTTP packets comprising an HTTP GET method call and/or an HTTP PUT method call. *Id.* at 21:50–53. In addition "identifying the packets . . . may include the packet security gateway determining the packets are among the HTTP packets identified by the rule(s)." *Id.* at 21:56–60. For example, "the HTTP GET method call and/or the HTTP PUT method call may specify one or more URIs and packet security gateway 112 may determine that the packet(s) originated and/or are destined for a network address corresponding to the URIs." *Id.* at 21:60–64. The '213 Specification provides no further description about how the identification is carried out.

Petitioner points out that the ACNS system can recognize a request is an HTTP request based on the first packet and make a determination about whether each subsequent packet is part of the same request. *See* Ex. 1020, Jeffay Reply Decl. ¶ 60. In that case, the content engine is identifying on a packet-by-packet basis those packets comprising the application-layer packet-header information from among the packets associated with the network protected by the content engine.

According to Patent Owner, by "opinin[ing] that the term 'packet-by-packet' must be read broadly enough to 'analyze more than one packet at a time,'" Dr. Jeffay misunderstands or mischaracterizes a tradeoff made by Patent Owner that foregoes performing deeper inspection of the application layer in favor of implementing rules on a packet-by-packet basis. PO Surreply 2–3 (quoting Ex. 1020, Jeffay Reply Decl. ¶ 17). Patent Owner does not identify a discussion of any such tradeoff in the '213 patent. Patent Owner contends that the challenged claims are patentable over ACNS "because ACNS discloses analyz[ing] more than one packet at a time, rather than received packets that include specified application layer packet-header information on a packet-by-packet basis or logging packets on a packet-by-packet basis." *Id.* at 3 (alteration in original).

Patent Owner's reference to paragraph 17 of Dr. Jeffay's Reply Declaration neglects to consider the full context of the testimony, i.e., that "the packet-by-packet analysis recited in the claims of the '213 Patent is not limited to Dr. Goodrich's view that each packet must be read in complete isolation." Ex. 1020, Jeffay Reply Decl. ¶ 10. According to Dr. Jeffay, "the '213 Patent contemplates that an HTTP request may be [sic] span multiple Layer 2 and Layer 3 packets and that the packet-by-packet analysis may be accomplished by identifying the application-layer packet-header information in one or more packets 'amongst' the packets that comprise the HTTP request." *Id.* at ¶ 11 (noting that dependent claim 4 of the '213 patent recites "the application-layer packet-header-information identifies one or more hypertext transfer protocol (HTTP) packets" and "the one or more packets comprising the application-layer packet-header information are ***amongst*** the one or more HTTP packets.").

We do not limit claim 1 to features recited in claim 4, but we do not exclude these features from claim 1. Dr. Jeffay testifies that a person of ordinary skill would have recognized that only certain packets contain the application-layer header information and that the application-layer header-information can be used to identify all of the HTTP packets that make up the HTTP request to which the transformation function will be applied. *Id.* Thus, according to Dr. Jeffay the claimed packet-by-packet analysis can involve looking at more the one packet at a time. *Id.* Dr. Jeffay addresses packet logging in paragraph 13 of his Reply Declaration in a similar way.

Dr. Jeffay notes a person of ordinary skill would not interpret packet-by-packet as Dr. Goodrich argues because in cases where headers in an HTTP message are large enough to span multiple lower layer packets, the limited capability of the technology in the '213 patent would fail to identify packets having certain application-layer packet-header information, i.e., it could only identify packets based on application layer packet headers in the first packet of a lower layer protocol. *Id.* ¶ 15. In paragraph 16 of his Reply Declaration, Dr. Jeffay states that "[i]f the headers [in an HTTP message] continue into the second packet of a lower layer protocol, the technology of the '213 patent cannot analyze those headers based on examining the second packet alone" or determine whether the contents of the second packet are HTTP headers or HTTP payload data. *Id.* at 16. It is this problem that led Dr. Jeffay to state in Paragraph 17 of his Reply Declaration that is addressed by "analyz[ing] more than one packet at time," while still operating on a packet-by-packet basis, i.e. "[t]he ability to analyze a packet by comparing it to other packets in a flow or to analyze groups of packets can account for the circumstances where application-layer packet-headers span multiple packets." *Id.* ¶ 17.

Dr. Jeffay's explanation is persuasive in the context of claim limitation 1.4 and the corresponding description on the Specification. The '213 patent Specification does not state that the packets are examined "in transit" or "as they come across the wire." Furthermore, the '213 patent does not state that each and every L2/L3 packet is examined to determine the presence of application-layer packet-header information, only that a determination is made for each packet. Claim limitation 1.1 recites "at least one rule specifying application-layer packet-header information." Claim limitation 1.4 recites identifying "on a packet-by-packet basis one or more packets comprising the application-layer header-information." As claim 1 does not recite how the identification is performed, claim 1 is not limited to identifying the application-layer packet-header information by individual packet inspection. Identifying the presence of application-layer packet header information in each packet is sufficient.

(2) ICAP Analysis

Alternatively, as to claim limitation 1.4, Petitioner notes that ACNS describes ICAP as an open standards protocol that can be used, typically at the edge of a network to adapt content to improve the value of the content, e.g., by virus scanning, content translation, content filtering, content insertion. Pet. 29, 40 (citing Ex. 1008, 16–1; Ex. 1004, Jeffay Decl. ¶ 158). Petitioner cites the disclosure in ACNS that a Content Engine examines packet-header information using ICAP rules to identify packets and the rule actions to apply. *Id.* at 40 (citing Ex. 1008, 16-5–25). According to Petitioner, such rules include identifying packets using application-layer packet-header information such as URL and Request Method. *Id.* (citing Ex. 1008, 16-16–18; Ex. 1004, Jeffay Decl. ¶ 160); *id.* at 29 (citing Ex. 1008 16-13–23, Ex. 1004, Jeffay Decl. ¶ 158).

According to Patent Owner, the Content Engines in ACNS are concerned with content management and not applying rules to individual packets. PO Resp. 46 (citing Ex. 2004 Goodrich Decl. ¶ 67; Ex. 1008, 1-2 (stating "[t]he primary role of a Content Engine in the ACNS network is to serve client requests for content."). Patent Owner argues that Petitioner's expert acknowledges the ACNS ICAP server rule actions are applied to content requests or content responses and not individual packets, i.e., not on a packet-by-packet basis, and that Petitioner's Reply does not rebut Patent Owner's argument. *Id.* at 45–46 (citing Ex. 2020, Jeffay Tr. II, 58:4–11); PO Surreply 10.

We have addressed Petitioner's and Patent Owner's packet-by-packet arguments above in the context of examining individual packets and do not find them persuasive. Those arguments are no more or less persuasive in the context of ICAP rules. Petitioner notes that ACNS teaches implementing ICAP to match a header filed pattern within an HTTP header, noting that ACNS refers to matching patterns of "request-line" and "user-agent" fields of an HTTP packet. Pet. 29 (citing Ex. 1010, 26 (HTTP/1.1 memo). Petitioner further notes that ACNS teaches modifying these fields with a substitution string to re-route or otherwise modify the HTTP packet, thus allowing the ACNS implementing ICAP rules to identify and transform packets based on application-layer packet-header information. *Id.* at 29–30 (citing Ex. 1004, Jeffay Decl. ¶ 158). Thus, we are persuaded that Petitioner has demonstrated ACNS ICAP implementation also discloses claim limitation 1.4.

b) Claim Limitation 1.5

Claim limitation 1.5 recites that the PSG performs, on a packet-by-packet basis, the transformation function (defined in claim element 1.2 as a

comprising a packet digest logging function) on each of the packets comprising the application-layer packet-header information (i.e., the packets identified in claim limitation 1.4). The features of the packet logging function are recited more explicitly in claim elements 1.6–1.8, discussed separately below. As to the claimed transformation function, i.e., the packet logging function recited in claim limitation 1.2 discussed above, Petitioner relies on Kjendal to teach it was known that packets may be mirrored, i.e., sent to a network logger, based on dynamic rules specifying application-layer packet-header information. Pet. 35.

As to claim limitation 1.5, Petitioner cites ACNS as performing packet transformations, e.g., (i) allowing or denying packets based on included HTTP request methods, and (ii) a packet digest logging function to notify the Content Engine to extract and log defined information from the packet header. Pet. 41 (citing Ex. 1008, 8-23, 19-1– 5). Petitioner states that a person of ordinary skill would understand that the ACNS system performs such transformations on a packet-by-packet basis to avoid skipping packets and thereby avoid invalid packets or refusing valid ones. *Id*. (citing Ex. 1004, Jeffay Decl. ¶ 177).

Petitioner contends that ACNS performs logging on a packet-by-packet basis, with sample log entries that apply to a single packet. Pet. Reply 8 (citing Ex. 1020, Jeffay Reply Decl. ¶34; Ex. 1008, 19-1 ("Squid" log entry for 1100 byte transaction), 19-2 (Apache-Style Transaction Logging for a 632 byte transaction, less that the size of one packet). Petitioner contends that the log entry is for a single packet, demonstrating ACNS teaches logging on a packet-by-packet basis. *Id*. Patent Owner argues Petitioner is "fabricating a sample log entry for a transaction Petitioner alleges can fit in a single packet," but Petitioner has not shown its

sample log entry is found in ACNS. PO Surreply 7 (citing Pet. Reply 8). We note, however, that sample the Squid log entry cited by Petitioner is found at Exhibit 1008, 19-1 and the sample Apache-Style transaction log entry is found at Exhibit 1008, 19-2.

Patent Owner argues Petitioner's assertion is "untenable" and that the transaction log entry does not mean the packet transformation is performed on a packet-by-packet basis "given that the very next transaction would very likely be split over multiple packets that must be reassembled." PO Surreply 7 (citing PO Resp. 43–44). As discussed above, we are not persuaded by Patent Owner's reassembly arguments in the context of identifying packets comprising the application-layer packet-header information.

In the context of packet logging, Petitioner argues that even where a transaction spans multiple packets, such as a 3,436 byte transaction identified by Patent Owner as another sample log entry, a person of ordinary skill would have understood that to generate the Squid-type log entry packets can be analyzed individually to determine the properties of the complete transaction and, after analysis of individual packets, each packet can be dropped, forwarded, or logged as appropriate and the log may contain information about the entire transaction. *Id.* at 9 (citing Ex. 1020, Jeffay Reply Dec. ¶¶ 34–35).

Patent Owner argues that "transaction logs in ACNS are not logs of individual packets identified as having application layer packet-header information." PO Surreply 6. Patent Owner contends that a person of ordinary skill "would understand the transaction logging functionality of ACNS to log transactions between the Content Engine and its clients that meet criteria set up by a user using the GUI shown on [Exhibit 1008] 19-10 and 19-11, as opposed to logging information about ***each packet*** that

includes application-layer packet-header information." *Id.* at 6–7 (citing Ex. 2004, Goodrich Decl. ¶¶ 116-124, Ex. 2020 (Jeffay Tr. II, 33:1–11), PO Resp. 32 (arguing "ACNS teaches creating a record of each **transaction** requested by the Content Engine.").

> Based on the antecedents in claim 1, Petitioner correctly argues:
>
> the claim says that you're performing the logging transformation function on the packets that have the specific application layer of packet header information, not as Patent Owner says in its surreply that you would log each packet that has any application layer of packet header information

Hr'g Tr. 19:1–6. Petitioner adds "I don't need a log for every packet that's part of the request that might have application layer header information. I see the specific application layer header info that I want, and I create one log based on that." *Id.* at 19:17–19, *see also, id.* at 20:1–18. The issue before us is whether it would have been obvious to create a packet digest log for those packets that comprise the identified application-layer packet-header information. As we discussed in our analysis of claim limitation 1.2, Petitioner cites Kjendal for the proposition that a person of ordinary skill would have understood the utility of selectively logging packets. *See* § VI.B.5. Thus, we are persuaded that Petitioner has demonstrated the combined teachings of ACNS and Kjendal disclose the features recited in claim limitation 1.5.

Petitioner also states that the ACNS implementation of ICAP demonstrates performing a packet transformation function. Pet. 41. Patent Owner argues that the implementation of ICAP rules by ACNS does not operate on a packet-by-packet basis. PO Surreply 10–11. We addressed this issue our analysis of claim element 1.4 above and found Petitioner's arguments persuasive. We agreed with Petitioner that ACNS teaches

modifying HTTP header fields with a substitution string to re-route or otherwise modify the HTTP packet, thus allowing the ACNS implementing ICAP rules to identify and transform packets based on application-layer packet header information. *Id.* at 29–30 (citing Ex. 1004, Jeffay Decl. ¶ 158). Thus, we are persuaded by Petitioner's argument that ACNS teaches claim limitation 1.5.

8. Claim Limitation 1.6

Petitioner identifies as claim element 1.6 the limitation that recites "identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application layer packet-header information." Pet. 42. Petitioner cites ACNS as disclosing the existence of multiple information logging formats that may include a subset of information from the application-layer packet-header. *Id*. (citing Ex. 1008, 19-1, discussing a "Squid" log entry). Petitioner asserts that a person of ordinary skill would have known that such information as the URL an HTTP method are found in the header of an HTTP application-layer packet and that any subset of the information from the packet could be logged. *Id*. (citing Ex. 1004, Jeffay Decl. ¶181).

Patent Owner contends that Petitioner's citations of ACNS does not suggest the claimed limitation because ACNS logs transactions, rather than packets. PO Resp. 47–48. Petitioner emphasizes its earlier arguments that ACNS teaches logging packets and that in combination, Kjendal discloses a system where application-layer packet header information is used to determine what should be logged. Pet. Reply 13 (citing Ex. 1020, Jeffay Reply Decl. ¶71). For example, Dr. Jeffay testifies that because the Squid entry illustrated in ACNS (Ex. 1008, 19-1) concerns a transaction that fits within a single packet, at least in this case ACNS teaches logging packets.

Ex. 1020, Jeffay Reply Decl. ¶83. Dr. Jeffay also repeats his opinion concerning transactions that span multiple packets, arguing that the mere fact a transaction spans multiple packets does not preclude performing a packet digest logging function. *Id.* ¶ 84.

Patent Owner further argues that Petitioner failed to demonstrate the claimed feature of identifying a subset of information specified by the packet digest logging function for each of the packets. PO Resp. 48–49. Patent Owner emphasizes that implementing the packet digest logging function as recited in claim element 1.6 permits tailoring the packet digest logging function to match the condition in the rule, enhancing the ability of the '213 patent to produce awareness information. *Id.* at 49 (citing Ex. 2004, Goodrich Decl. ¶ 135 (testifying the ACNS Guide lacks the ability to log packet information with the level of granularity and specificity enable by the techniques claimed in the '213 patent). We agree with Dr. Jeffay, however, that claim elements 1.6 recites no particular level of granularity or specificity and are persuaded by Petitioner's arguments that the combined teachings of ACNS and Kjendal disclose claim element 1.6.

9. Claim Limitation 1.7

Petitioner identifies as claim element 1.7 the limitation that recites, "generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function." Pet. 43. Petitioner cites the "squid" log entry in ACNS as the default format for transaction logging in the Content Engine. *See id.* at 43–44, (citing Ex. 1008, 19-1). ACNS states that typical transaction log fields include "the date and time when a request was made, the URL that was requested, whether it was a cache hit or a cache miss, the type of request, the number of

bytes transferred, and the source IP address." Ex. 1008, 19-1. Petitioner notes that the ACNS system identifies and extracts application packet information and combines information not found therein to generate an internal record before writing it in the specified format. Pet. 44 (citing Ex. 1008, 19-1–5).

Patent Owner's arguments concerning claim element 1.7 are similar to those Patent Owner advances concerning claim element 1.6. i.e., that ACNS concerns transaction logging, as distinguished from packet logging (PO Resp. 50–51), and we find them unpersuasive for the same reasons we are persuaded by Petitioner's arguments concerning claim element 1.6.

10. Claim Limitations 1.8 and 1.9

Petitioner identifies as claim element 1.8 the limitation that recites "reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard." Pet. 44.

Petitioner identifies as claim element 1.9 the limitation that recites "routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function." Pet. 45.

As to claim element 1.8, Petitioner notes that "ACNS also teaches that the subset of information, already formatted in one log format, may be reformatted into syslog format." *Id.* at 44 (citing Ex. 1004 ¶¶ 186–187, Ex. 1008, 19-19–21). As to claim element 1.9, Petitioner cites Kjendal as teaching routing identified packets to a monitoring device based on rules by mirroring selected packets to a wide variety of logger devices that perform

analysis, identification, and decryption based on application-layer packet-header information. *Id.* at 45–46.

Patent Owner does not address claim element 1.8 explicitly. As to claim element 1.9, Patent Owner contends techniques are directed to mirroring packet flow rather than routing on a packet-by-packet basis to a monitoring device in response to performing a packet transformation function. PO Resp. 52. Patent Owner contends Petitioner fails to show that Kjendal routes packets in response to an operation performed on the packets. *Id.*

We addressed this issue in the context of claim element 1.2. In addition, Petitioner quotes our Decision to Institute in IPR2018-01386, where we noted Kjendal performs selective mirroring for efficiency and stated "Kjendal' s selective mirroring suggests examining packets and executing a transformation function that forward packets and mirrors only certain packets depending on their characteristics." Pet. Reply 16–17 (citing IPR2018-01386, Paper 8 at 31). Consistent with our analysis in our Decision to Institute in IPR2018-01386 cited by Petitioner, we agree with Petitioner that claim element 1.9 is taught by Kjendal.

11. Objective Considerations

Before determining whether a claim is obvious in light of the prior art, we consider any relevant evidence of secondary considerations of non-obviousness. *See Graham*, 383 U.S. at 17. Notwithstanding what the teachings of the prior art would have suggested to one of ordinary skill in the art at the time of the invention, the totality of the evidence submitted, including objective evidence of non-obviousness, may lead to a conclusion that the challenged claims would not have been obvious to one of ordinary skill. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). Patent

Owner presents evidence of three such considerations: (1) long-felt but unmet need, (PO Resp. 59–64) (2) industry praise (*id.* at 65–66), and (3) commercial success/licensing (*id*. at 66–68).

"In order to accord substantial weight to secondary considerations in an obviousness analysis, the evidence of secondary considerations must have a nexus to the claims, i.e., there must be a legally and factually sufficient connection between the evidence and the patented invention." *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (internal quotations omitted). A nexus is presumed when "the patentee shows that the asserted objective evidence is tied to a specific product and that product 'embodies the claimed features, and is coextensive with them.'" *Id.* (quoting *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). If the product is not coextensive with the claims at issue—for example, if the patented invention is only a component of the product—the patentee is not entitled to a presumption of nexus. *See id.* (citing *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)).

a) Long Felt Unresolved Need and the Failure of Others

Patent Owner points to a U.S. Naval Research Laboratory presentation by Stanley Chincheck as evidence of a long felt, unresolved need recognized as early as 2010 to improve signature based network security systems. PO Resp. 60–62 (citing Ex. 2013, 5–6; Ex. 2004, Goodrich Decl. ¶ 160), PO Surreply 19–22. Patent Owner's expert, Dr. Goodrich, refers to the limitations of signature based systems, but does not specifically connect the teachings of the references to signature based systems or explain why the techniques in these references would be less

effective than that claimed in the '213 patent. Ex. 2004, Goodrich Decl. ¶ 160. In addition, the Chincheck presentation does not comment on any specific approach or technology, including that discussed in the '213 patent. Ex. 2013, 3. Thus, even if the Chincheck presentation indicates a need existed to improve certain types of signature based systems, it provides no evidence that the '213 patent addresses that need, or that the approach in the cited references failed to do so.

Patent Owner cites statements in a May 2018 paper titled "Centripetal Networks Threat Intelligence Gateway" by Tony Palmer, a paper Patent Owner commissioned from the Enterprise Strategy Group (ESG), concerning its CleanINTERNET intelligence-led managed security service using its RuleGATE enforcement point. PO Resp. 61–64 (citing Ex. 2006). Although we do not dismiss the ESG paper out of hand because it was commissioned by Patent Owner, we also cannot overlook the potential implications arising from this fact.

Patent Owner notes ESG's assertion that Patent Owner's "**goal is nothing less that the transformation of CTI (cyber threat intelligence) into protective action at scale**" and that Patent Owner "**does this by converting indicators to rules that drive actions** across a risk spectrum, i.e., **logging, content capture, mirroring, redirection**, shielding, and advanced threat detection." *Id.* at 63 (quoting Ex. 2006, 7). According to Patent Owner, ESG's description of Patent Owner's solution is tied to the inventions in the '213 patent that are directed to receiving a dynamic security policy, as distinguished from prior art security policies by its automatic updating when new CTI is received. *Id.* at 63 (citing Ex. 2004, Goodrich Decl. ¶ 163), PO Surreply 22. We note, however, as discussed above, the '213 patent does not limit a dynamic security policy to one that is

updated automatically, as the '213 patent describes an administrator updating the dynamic security policy manually. Ex. 1001, 14:23–47.

As Petitioner notes, Patent Owner's expert, Dr. Goodrich acknowledges that the ESG paper does not disclose whether the products it discusses embody the claims of the '213 patent. Pet. Reply 21 (citing Ex. 1021, Deposition Transcript of Dr. Michael Goodrich ("Goodrich Tr.") 24:12–30:7).

In view of the above, Patent Owner does not establish a sufficient nexus between the invention claimed in the '213 patent and the purported long felt, unmet need.

b) Industry Praise

Patent Owner cites the ESG Paper (Ex. 2006) as well as a Gartner article (Ex. 2007) and an American Banker article (Ex. 2011) as evidence of industry praise. PO Resp. 65–66. Similar to its long-felt need contentions, however, Patent Owner does not provide sufficient analysis or explanation to establish the requisite nexus. Patent Owner provides no analysis demonstrating that any of its product is coextensive with the challenged claims, so no presumption of nexus is applied. *See Fox Factory*, 944 F.3d at 1373–74. Additionally, the cited praise of Patent Owner's products is not linked sufficiently to the challenged claims, due in part to Patent Owner's failure to address lauded features with no relationship to the claims.

For example, Patent Owner cites the ESG Paper as describing Patent Owner's TIG (Threat Intelligence Gateway) as having the "highest performance network filter that ESG has tested or seen in action to date." PO Resp. 65 (citing Ex. 2006, 8). Patent Owner also cites the ESG Paper as stating patent Owner's TIG processed over 140 Gbps of network traffic at wire speed, and distributing, ingesting, synthesizing into a network policy,

and enforcing over five million complex network filtering rules with each complex filtering rule containing at least a dozen unique fields. *Id.* (citing Ex. 2006, 7; Ex. 2004, Goodrich Decl. ¶167). Patent Owner does not associate this information with the limitations of the challenged claims. Patent Owner does not address whether they are part of the claimed invention or, if not, their relative contribution to the industry praise compared to any actual features of the claimed invention.

Regarding the Gartner article, Patent Owner notes that Gartner praises Patent Owner's product's "ability to instantly detect and prevent malicious connections based on millions of threat indicators at 10-gigabit speeds," as having "the largest number of third-party threat intelligence service integrations," and using "5 million indicators simultaneously." PO Resp. 65–66 (citing Ex. 2007, 5). Again, insufficient analysis is presented to address how these features relate to the challenged claims. Patent Owner's reference to the American Banker article similarly suffers from a lack of explanation. *Id.* at 66 (citing Ex. 2011, 14; Ex. 2004, Goodrich Decl. ¶ 168)

Patent Owner's sole nexus explanation is a conclusory assertion that "the salutary benefits of Centripetal' s TIG [threat interface gateway] are made possible in large part by the '213 patent's dynamic security policies, which are automatically managed and distributed by the claimed SPM, as well as its network layer packet-by-packet rule enforcement, packet digest logging function and packet transformation function for routing packets to a monitoring device." PO Resp. 66 (citing Ex. 2004, Goodrich Decl. ¶169). Dr. Goodrich's testimony cited in support of this statement is merely a near-verbatim copy of this conclusory statement with no additional explanation. *See* Ex. 2004, Goodrich Decl. ¶ 169; 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the

opinion is based is entitled to little or no weight."). As a result, we find that Patent Owner has not established a sufficient nexus between the cited industry praise and the invention of the challenged claims.

c) Commercial Success and Licensing

Patent Owner contends that the commercial success of its RuleGATE product as well as a license to the '213 Patent taken by Keysight Technologies are compelling secondary considerations of non-obviousness. PO Resp. 66–68. Jonathan Rogers, Patent Owner's Vice President of Operations and COO, testified that Patent Owner's RuleGATE system has been sold to customers and that RuleGATE embodies the '213 patent, although the record includes no technical analysis to support his testimony that RuleGATE embodies the '213 patent. Ex. 2016, Rogers Decl. ¶¶ 3–6.

Petitioner responds that Patent Owner does not provide an element by element analysis to support Mr. Rogers' claim. Pet. Reply 22–23. Patent Owner argues that no such element by element analysis is required and that, given Mr. Rogers' testimony, which Petitioner failed to cross-examine, nexus is presumed. PO Surreply 23.

Although Patent Owner argues it was incumbent on Petitioner to put forth evidence to rebut the presumption, we are not persuaded that Mr. Roger's bald assertion, without any factual basis, constitutes adequate evidence of nexus. Mr. Rogers states he is familiar with Patent Owner's licensing practices and assists in licensing Patent Owner's patented technologies, but he provides no foundation for his assertion that RuleGATE embodies the 213 patent. Mr. Rogers does not state he has any personal knowledge of the '213 patent or its claims; he does not state what aspects of RuleGATE embody the claims of the '213 patent; he does not state whether he draws on any personal technical background for his testimony; and he

does not state whether his assertion is based on a legal assessment of counsel. Indeed, Mr. Rogers does not provide any basis for his assertion that RuleGATE does, in fact, embody the claims of the '213 patent. As an employee of Patent Owner, Mr. Rogers' testimony, without foundation or corroboration of any kind, is unreliable.

"Whether a product is coextensive with the patented invention, and therefore whether a presumption of nexus is appropriate in a given case, is a question of fact." *Fox Factory,* 944 F.3d at 1373. Although the patentee is not required to prove perfect coextensiveness, the patentee is required to demonstrate the product is essentially the claimed invention. *Id.* at 1374. As Patent Owner has provided insufficient factual evidence to demonstrate RuleGATE is the claimed invention, we do not apply a presumption of nexus in this case.

As additional evidence of commercial success, Patent Owner cites a "worldwide, royalty-bearing, non-transferable, irrevocable, nonterminable, nonexclusive license to Centripetal's worldwide patent portfolio," including the '213 patent, taken by Keysight Technologies to settle a patent infringement suit. PO Resp. 67–68 (citing Ex. 2012, 83). Petitioner points out that Keysight was sued on the '213 patent and ten other patents. Pet. Reply 24. Patent Owner provides no information about the relevant details of this license—e.g., how many patents comprise the portfolio, or the relative contribution of the '213 patent to the value of the license—such that we could discern whether Keysight took the license "out of recognition and acceptance of the subject matter claimed" in the '213 patent. *See In re GPAC Inc*., 57 F.3d 1573, 1580 (Fed. Cir. 1995). As such, we find that Patent Owner has not provided sufficient evidence to establish the requisite nexus between the Keysight license and the '213 Patent. *See id*.

12. Conclusion as to Obviousness of Claim 1

Having reviewed the arguments and evidence presented by the parties, we find that Petitioner has demonstrated a person of ordinary skill would have been motivated to combine the teachings of ACNS and Kjendal and that the combined teachings of ACNS and Kjendal disclose all the limitations of claim 1 to a person of ordinary skill. Thus, we conclude that Petitioner has shown by a preponderance of the evidence that claim 1 is unpatentable as obvious under 35 U.S.C. 103 over the combined teachings of ACNS and Kjendal.

C. Claims 2–9 as Obvious Over ACNS in View of Kjendal

1. Claim 2

Claim 2 depends from claim 1 and recites "the at least one rule indicates performing an accept packet transformation function on the packets comprising the application-layer packet-header information, and wherein the performing the packet transformation function comprises forwarding, by the packet security gateway, the each of the one or more packets comprising the application-layer packet-header information toward its respective destination." Noting that ACNS Content Engines accept (or reject) an HTTP request depending upon whether the HTTP request is supported, Petitioner argues that a person of ordinary skill would understand that the HTTP packet will be accepted based on HTTP (application layer) request method (packet header) information and forwarded to its destination. Pet. 47–48 (citing Ex. 1008, 8-23, Ex. 1004, Jeffay Decl. ¶¶ 199–201). Petitioner also notes that ACNS discloses the Content Engine may function as a forward proxy that receives user requests and either responds to the request of forwards the request to an outside server to obtain the requested content. *Id.* (citing Ex. 1008, 1-3).

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim.

Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 2 and that a person of ordinary skill would have had reason to combine the teachings of these references. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 2 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS and Kjendal.

2. Claim 3

Claim 3 depends from claim 1 and recites "the at least one rule indicates performing a deny packet transformation function on the packets comprising the application layer packet-header information, and wherein the performing the packet transformation function on comprises dropping, by the packet security gateway, the each of the one or more packets comprising the application-layer packet header information." Petitioner notes that, in a manner similar to HTTP packet acceptance discussed with respect to claim 2, ACNS a person of ordinary skill would understand that an ACNS Content Engine could reject an HTTP packet based on the Request Method. Pet. 49.

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim.

Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 3 and that a person of ordinary skill would have had reason to combine the teachings of these references. The

additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 3 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS and Kjendal.

3. Claim 4

Claim 4 depends from claim 1 and recites "the application-layer packet-header information identifies one or more hypertext transfer protocol (HTTP) packets, and wherein identifying the one or more packets comprising the application-layer packet-header information comprises determining by the packet security gateway that the one or more packets comprising the application-layer packet-header information are amongst the one or more HTTP packets." Petitioner notes that, as discussed above, ACNS Content Engines can accept or reject an HTTP request depending upon whether the HTTP request method is supported. Pet. 50.

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim.

Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 4 and that a person of ordinary skill would have had reason to combine the teachings of these references. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 4 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS and Kjendal.

4. Claim 5

Claim 5 depends from claim 4 and recites "the one or more HTTP packets comprise an HTTP GET method call, and wherein determining that the one or more packets comprising the application-layer packet-header information are amongst the one or more HTTP packets comprises determining that the one or more packets comprising the application-layer packet-header information are associated with the HTTP GET method call." As Petitioner points out ACNS discloses the HTTP GET method call among rule criteria and that the logging system identifies the Request Method (including GET) in order to create a corresponding log entry. Pet. 51.

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim.

Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 5 and that a person of ordinary skill would have had reason to combine the teachings of these references. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 5 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS and Kjendal.

5. Claim 6

Claim 6 depends from claim 5 and recites "the HTTP GET method call specifies a uniform resource identifier (URI), and wherein determining that the one or more packets comprising the application-layer packet-header information are associated with the HTTP GET method call comprises determining that the one or more packets comprising the application-layer

packet-header information originated from or are destined for a network address corresponding to the URI." Petitioner notes that "ACNS teaches implementing URL filtering for HTTP packets containing a Request Method, such as GET, based on the URI contained within the HTTP (application-layer) packet-header." Pet. 52 (citing Ex. 1008, 16-2525–33, Ex. 1004, Jeffay Decl. ¶215). Petitioner also cites the "squid" log format example in which the log comprises a "peerhost" field to demonstrate whether the packet is being forwarded to the URI or another address. *Id*. at 53 (citing Ex. 1008, 19-1–8; Ex. 1004, Jeffay Decl. ¶ 218).

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim.

Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 6 and that a person of ordinary skill would have had reason to combine the teachings of these references. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 6 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS and Kjendal.

6. Claim 7

Claim 7 depends from claim 4 and recites "the one or more HTTP packets comprise an HTTP PUT method call, and wherein determining that the one or more packets comprising the application-layer packet-header information are amongst the one or more HTTP packets comprises determining that the one or more packets comprising the application-layer packet-header information are associated with the HTTP PUT method call."

Petitioner notes that the HTTP 1.1 specification discussed in ACNS includes eight Request Methods, including PUT. Pet. 54.

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim.

Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 7 and that a person of ordinary skill would have had reason to combine the teachings of these references. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 7 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS and Kjendal.

7. Claim 8

Claim 8 depends from claim 7 and recites "the HTTP PUT method call specifies a uniform resource identifier (URI), and wherein determining that the one or more packets comprising the application-layer packet-header information are associated with the HTTP PUT method call comprises determining that the one or more packets comprising the application-layer packet-header information originated from or are destined for a network address corresponding to the URI." Petitioner argues that ACNS discloses this feature for the same reasons as those discussed with respect to claims 6 and 7. Pet. 54–55.

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim.

Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS and Kjendal

teaches the features recited in claim 8 and that a person of ordinary skill would have had reason to combine the teachings of these references. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 8 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS and Kjendal.

8. Claim 9

Claim 9 depends from claim 1 and recites "the at least one rule comprises a five-tuple specifying one or more transport-layer protocols, a range of source addresses, a range of source ports, a range of destination addresses, and a range of destination ports, and wherein identifying the one or more packets comprising the application-layer packet-header information comprises determining by the packet security gateway that each of the one or more packets comprising the application-layer packet-header information corresponds to at least one of the one or more transport-layer protocols, has a source address within the range of source addresses, a source port within the range of source ports, a destination address within the range of destination addresses, and a destination port within the range of destination ports." Petitioner notes that the five-tuple of protocol, source address, destination address, source port, and destination port as identification criteria is well known. Pet. 55–56 (citing Ex. 1004, Jeffay Decl. ¶¶ 231–232). Petitioner cites Chapter 17 of ACNS as teaching filtering packets using Access Control Lists based on all five-tuple elements. *Id.* at 56 (citing Ex. 1008, Table 17-4).

Patent Owner does not explicitly respond to Petitioner's contentions beyond its arguments as to the independent claim.

Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS and Kjendal teaches the features recited in claim 9 and that a person of ordinary skill would have had reason to combine the teachings of these references. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 9 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS and Kjendal.

D. Claim 10 as Obvious Over ACNS in View of Kjenda, and Diffserv

1. Diffserv

Petitioner describes differentiated services as allowing a system to give certain packets priority over others. Pet. 59 (citing Ex. 1004, Jeffay Decl. ¶¶ 68–71). According to Petitioner, "Diffserv is a flexible standard for marking each network packet with a priority value within the DSCP [Differential Service Code Point] field." *Id.* (citing Ex. 1011, §§ 2, 2.31). Petitioner cites the description in ACNS of implementing differentiated services that utilize a DSCP selector, and a differentiated management services screen referring to Quality of Service (QoS), noting that ACNS uses DSCP values carried in packet headers to enable Content Engines to classify packets bases on quality of service differentiation. *Id.* at 59–61. Petitioner contends that a person of ordinary skill would have recognized DSCP based packet filtering packet as an obvious variant, as filtering can be based on any network packet filed. *Id.* at 61–62. Petitioner also notes that Kjendal teaches mirroring with network services including QoS. *Id.* at 62 (citing Ex. 1009, 2:14–16, 3:1–7).

2. Claim 10

As Petitioner notes, claim 10 is similar to claim 1, except that where claim 1 recites the dynamic security policy comprises at least one rule specifying application-layer packet-header information, claim 10 broadly recites that the rule includes packet-identification criteria. Pet. 62. Claim 10 also recites that the packet-identification criteria comprises a Differential Service Code Point (DSCP) selector (identified by Petitioner as claim element 10-3). Petitioner cites Diffserv as disclosing a system that may select packets in a traffic stream based on the content of some portion of the packet header, specifically the DSCP information. *Id.* at 63. Petitioner further notes that ACNS contemplates a combination with Diffserv because ACNS teaches the presence of the DSCP field in packets and implementing QoS based on the DSCP field. *Id.* at 66 (citing Ex. 1008, 17-1–8; Ex. 1004, Jeffay Decl. ¶ 263). Thus, Petitioner argues that the combination of ACNS, Kjendal, and Diffserv teaches the claimed elements of claim 10, including classifier rules that include the claimed packet-identification criteria. *Id.* at 63.

As to claim 10 limitations designated 10.1 and 10.2, Patent Owner argues that the combination of ACNS in view of Kjendal and Diffserv does not discloses receiving a dynamic security policy from a security policy management server for the same reasons Patent Owner argued with respect to claim 1. PO Resp. 54. As we disused in our analysis of claim 1, we are persuaded that Petitioner has demonstrated the combination of Kjendal and ACNS discloses these limitations.

Patent Owner also argues that Petitioner has not demonstrated Diffserv discloses receiving a dynamic security policy with a rule that includes a DSCP selector as the packet identification criteria. *Id.* at 54–56.

Patent Owner contends that, to the extent Diffserv discloses utilizing DSCP data, that data is used to classify packets prior to applying a security policy and not as packet-identification criteria specified by a dynamic security policy. *Id.* at 55 (citing Ex. 2004, Goodrich Decl. ¶¶151–153). Patent Owner adds that "the combination with Diffserv is unsupported and does not reach the claimed subject matter because the 'rule' that Diffserv's '[p]acket classifiers' would still not be packet-identification criteria in a received dynamic security policy." *Id.* (alteration in original)

Noting Patent Owner's apparent acknowledgement that ACNS and Diffserv disclose the use of DSCP data, Petitioner argues a person of ordinary skill would have understood ACNS to teach packets are classified and marked with a DSCP. Pet. Reply 19 (citing Ex. 1020, Jeffay Reply Decl. ¶¶ 980–92). We find persuasive Petitioner's argument that a person of ordinary skill would have recognized DSCP can be used as part of a security measure to identify packets to check for malicious traffic and take action on those packets, given that ACNS Content Engines are in line devices between end users and the Internet and can perform virus scanning. *Id.* at 19–20 (citing Ex. 1020, Jeffay Reply Decl.¶ 92). As Petitioner points out, ACNS contemplates a combination with Diffserv because ACNS teaches the presence of the DSCP field in packets and implementing QoS based on the DSCP field. Pet. 66 (citing Ex. 1008, 17-1–8; Ex. 1004, Jeffay Decl. ¶ 263). Thus, we are persuaded that Petitioner has demonstrated a person of ordinary skill would have had reason to combine the teachings of ACNS, Kjendal, and Diffserv. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness.

In consideration of the above, we find that Petitioner has demonstrated by a preponderance of the evidence that claim 10 is

unpatentable under 35 U.S.C. § 103(a) over the combination of ACNS, Kjendal, and Diffserv.

E. Claims 11–16 as Obvious Over ACNS in View of Kjendal and Diffserv

1. Claim 11

Claim 11 depends from claim 1 and further recites "the subset of information comprises at least one of a portion of data from the packet, a source address of the packet, a source port of the packet, a destination address of the packet, a destination port of the packet, a transport-protocol type of the packet, a uniform resource identifier (URI) from the packet, an arrival time of the packet, a size of the packet, a flow direction of the packet, an identifier of an interface of the packet security gateway that received the packet, or one or more media access control (MAC) addresses associated with the packet." Petitioner cites ACNS as disclosing a Content Engine that may identify several of the claimed criteria from individual packets including that date and time a request was made, the URL that was requested, the number of bytes transferred and the source IP address. Pet. 69–70. Petitioner cites Diffserv as teaching specific information that should be gathered for a log record, including the date/time the packet was received and the destination and IP address. *Id.* at 70.

Patent Owner does not respond explicitly to Petitioner's contentions concerning claim 11. Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS, Kjendal, and Diffserv teaches the features recited in claim 11 and that a person of ordinary skill would have had reason to combine the teachings of these references. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-

obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 9 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS, Kjendal, and Diffserv.

2. Claim 12

Claim 12 depends from claim 10 and further recites "temporarily storing data in a memory of the packet security gateway, the data comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria; and utilizing, by the packet security gateway, the data to generate a message comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria." Noting that ACNS discloses real time transaction logging and an example of a real-time syslog message sent from the transaction logging module (Content Engine) to the remote syslog host, Petitioner argues that ACNS teaches the message is generated and thus temporarily stored in memory at the Content Engine (analogous to the claimed PSG) as an obvious step before sending messages. Pet. 71 (citing Ex. 1008, 19-19; Ex. 1004, Jeffay Decl., ¶ 290).

Patent Owner does not respond explicitly to Petitioner's contentions concerning claim 12. Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS, Kjendal, and Diffserv teaches the features recited in claim 12 and that a person of ordinary skill would have had reason to combine the teachings of these references. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a

preponderance of the evidence claim 12 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS, Kjendal, and Diffserv.

3. Claim 13

Claim 13 depends from claim 12 and recites "communicating, by the packet security gateway and to the security policy management server, the message comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet identification criteria." Noting that ACNS provides instruction for configuring the destination of the syslog messages, Petitioner contends that a person of ordinary skill would understand that one likely location for the syslog server that receives log messages is the Content Distribution Module (corresponding to the claimed SPM). Pet. 72 (citing Ex. 1008, 19-20–21; Ex. 1004, Jeffay Decl. ¶ 294).

Patent Owner does not respond explicitly to Petitioner's contentions concerning claim 13. Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS, Kjendal, and Diffserv teaches the features recited in claim 13 and that a person of ordinary skill would have had reason to combine the teachings of these references. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 13 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS, Kjendal, and Diffserv.

4. Claim 14

Claim 14 depends from claim 10 and recites "reformatting the subset of information specified by the packet digest logging function in accordance with the logging system standard comprises reformatting the subset of information specified by the packet digest logging function in accordance with a syslog logging system standard."

Noting that the '213 patent acknowledges logging can be implements using a known standard, e.g., Syslog, Petitioner cites ACNS as reformatting information into the syslog system standard. Pet. 73.

Patent Owner does not respond explicitly to Petitioner's contentions concerning claim 14. Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS, Kjendal, and Diffserv teaches the features recited in claim 14 and that a person of ordinary skill would have had reason to combine the teachings of these references. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 14 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS, Kjendal, and Diffserv.

5. Claim 15

Claim 15 depends from claim 10 and recites "the packet-identification criteria comprises a five-tuple specifying one or more transport-layer protocols, a range of source addresses, a range of source ports, a range of destination addresses, and a range of destination ports, and wherein identifying the one or more packets corresponding to the packet-identification criteria comprises determining by the packet security gateway

that each of the one or more packets corresponding to the packet-identification criteria corresponds to at least one of the one or more transport-layer protocols, has a source address within the range of source addresses, a source port within the range of source ports, a destination address within the range of destination addresses, and a destination port within the range of destination ports."

Petitioner notes that, except for referring to the packet identification of the rule, claim 15 is functionally equivalent to claim 9 discussed above. Pet. 73–74. Petitioner argues that the references disclose the elements of claim 15 for the same reason they disclose the elements of claim 9. *Id.*

Patent Owner does not respond explicitly to Petitioner's contentions concerning claim 15. Having reviewed the arguments and evidence of record, we find that Petitioner has demonstrated that the combination of ACNS, Kjendal, and Diffserv teaches the features recited in claim 15 and that a person of ordinary skill would have had reason to combine the teachings of these references. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 15 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS, Kjendal, and Diffserv.

6. Claim 16

Claim 16 depends from claim 10 and recites "the packet-identification criteria comprises application-layer packet-header information, and wherein identifying the one or more packets corresponding to the packet-identification criteria comprises determining by the packet security gateway that each of the one or more packets corresponding to the packet-

identification criteria comprises at least a portion of the application-layer packet-header information." Petitioner contends that the analysis discussed above in the context of claim elements 1.1 and 1.4 applies equally to claim 16. Pet. 74–75. We have addressed these limitations in the Decision and agree with Petitioner that the same analysis applies to claim 16. The additional limitations in this claim do not affect our analysis that objective considerations do not establish non-obviousness. Thus, we conclude Petitioner has demonstrated by a preponderance of the evidence claim 16 is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of ACNS, Kjendal, and Diffserv.

VII. MOTION TO EXCLUDE

Patent Owner moves to exclude Exhibits 1004, 1008, 1010–1012, 1015, 1017, 1020–1023, and 1025–1030. Mot. To Exclude 1. Patent Owner's Motion to Exclude does not discuss Exhibits 1015 and 1017. Patent Owner objected to Exhibits 1015 and 1017 as irrelevant. Paper 10 (Patent Owner's Objections I"), 4. As this Decision does not rely on Exhibits 1015 and 1017, we dismiss as moot Patent Owner's Motion to Exclude Exhibits 1015 and 1017.

We next turn to Patent Owner's Motion to Exclude Exhibit 1012, i.e., the Declaration of Eli Fuchs, and Ex. 1027, i.e., the Supplemental Declaration of Eli Fuchs, relied upon by Petitioner to support the public accessibility of the ACNS Guide filed as Exhibit 1008.

Patent Owner objected to the Fuchs Declaration (Ex. 1012) as hearsay, but provided no further explanation of its objection. Paper 10 Patent Owner cross-examined Mr. Fuchs concerning his testimony before filing its Patent Owner Response. *See generally* Ex. 2021, Fuchs Tr. Other than a broad statement that Petitioner did not serve supplemental evidence,

Patent Owner's Motion to Exclude does not further explain the basis for its hearsay objection to Exhibit 1012. Mot. To Exclude 1. In the absence of such justification, we deny Patent Owner's Motion to Exclude Exhibit 1012.

Patent Owner objected to Mr. Fuchs's Supplemental Declaration (Ex. 1027) as untimely Supplemental Information under 37 C.F.R. § 42.104(b) and 37 C.F.R. § 42.23(b), under FRE 401 and FRE 402 as irrelevant because it exceeds the proper scope of Petitioner's Reply, under FRE 403 as creating prejudice to Patent Owner arising from Patent Owner's inability to respond, under FRE 702 as conclusory and lacking facts supporting Mr. Fuchs's opinions, under FRE 602 as not based on Mr. Fuchs's personal knowledge of the subject of his testimony, and under FRE 801 as hearsay not subject to a hearsay exception under FRE 802 or FRE 803. Paper 19 ("PO's Objections II") 8–9. Patent Owner also contends that Petitioner filed Exhibit 1027 as a means to circumvent the requirement to provide supplemental evidence in response to Patent Owner's objections, i.e., as a vehicle to introduce Exhibits 1028 and 1029 as evidence of public accessibility. Reply to Opp. to Mot to Exclude 6.

We agree with Petitioner that Mr. Fuchs Supplemental Declaration did not exceed the scope of Petitioner's Reply because it was responsive to arguments raised in the Patent Owner Response concerning the public accessibility of ACNS. Opp. to Mot. To Exclude 9 (citing PO Resp. 19–22). As discussed in Section VI.B.1.b of this Decision, Mr. Fuchs's omission of Release Notes and ACNS Documentation History (*see* Exs. 1028, 1029) from Ex. 1008 first became apparent during his deposition, and was a subject of the Patent Owner Response. PO Resp. 19–22. We are not persuaded that Patent Owner has been prejudiced by this Supplemental Declaration. For example, there is no evidence that Patent Owner sought to

depose Mr. Fuchs concerning his Supplemental Declaration before Patent Owner filed its Patent Owner Surreply.

We also are not persuaded that Mr. Fuchs's testimony constitutes opinion testimony. Most, if not all of Mr. Fuch's testimony concerns facts relating to Cisco's software documentation and the content of the ACNS Guide. As to his personal knowledge and the facts associated with his testimony, Mr. Fuchs' Supplemental Declaration refers to the purported publication dates of the same Release Notes discussed in his initial Declaration (Ex. 1012, Fuchs Decl. ¶ 9). *See* Ex. 1027, Fuchs sup. Decl. ¶ 3. Patent Owner cross-examined Mr. Fuchs on those issues based on the testimony in his initial declaration. *See* § VI.B.1.b.. As to hearsay, Mr. Fuchs's testified that he personally viewed the Cisco web site and that he had personal knowledge of Cisco's document policies and that Cisco did not release products without making product documentation available. *See, id.* The totality of circumstances and the probity of the information in the documents indicate that Mr. Fuchs's Supplemental Declaration (Exhibit 1027) and Exhibits 1028, 1029, and 1030 fall within the ambit of residual exception to hearsay under FRE 807.

Patent Owner objected to Exhibit 1008 on the basis that Petitioner failed to establish its public accessibility as a printed publication, asserting its date is hearsay and the document was not authenticated. PO's Objections I, 2. We addressed the issue of public accessibility of ACNS earlier in this Decision and determined that Petitioner has demonstrated ACNS to have been accessible to the public. *See* § VI.B.1.b. We also find that Mr. Fuchs' initial declaration and the circumstances previously discussed provide sufficient evidence of authenticity. Therefore, we deny Patent Owner's Motion to Exclude Exhibit 1008.

Patent Owner moves to exclude Exhibits 1010, 1011, 1022–1023, 1025, and 1028–1030 as unauthenticated. This Decision does not rely on Exhibits 1010 (Hypertext Transfer Protocol – HTTP/1/1), Exhibit 1022 (Office of Naval Research Broad Agency Announcement), 1023 (Wikipedia List of HTTP Header Fields), and 1025 (Syslog Protocol RFC5425). Therefore, we dismiss as moot Patent Owner's Motion to Exclude Exhibits 1010, 1022, 1023, and 1025 as unauthenticated and turn to the remaining exhibits that are the subject of Patent Owner's Motion to Exclude as unauthenticated, i.e., Exhibit 1011 (Diffserv) and Exhibit 1028 (Release Notes), Exhibit 1029 and Exhibit 1030 (collectively, "ACNS Document History").

Patent Owner argues it timely objected to these Exhibits and Petitioner failed to serve Supplemental Evidence in response to Patent Owner's objections. Mot. To Exclude 1. Patent Owner further argues we should exclude Exhibits 1011 and 1028 under Federal Rule of Evidence (FRE) 901 "because Petitioner failed to produce any evidence to support a finding that Exhibits [] 1011 and []1028 [] are in fact what Petitioner claims they are." *Id.* We find that Petitioner has met its burden as to authentication. FRE 901(b)(4) provides the following example of "evidence that satisfies the requirement" of authenticating or identifying evidence: "The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances."

Petitioner notes that, in fact, it produced the requisite evidence in paragraphs 129–136 of Dr. Jeffay's initial declaration, where he testified about his personal knowledge of Exhibit 1011 and how others could obtain a copy. Opp. to Mot. To Exclude 5 (citing Ex. 1004, Jeffay Decl. ¶¶ 129–136). Dr. Jeffay stated he had personal knowledge of the Diffserve

Specification, that he has been aware of its public accessibility since December 1998, when he first encountered it as the final Diffserv Specification (RFC 2475), that RFC documents do not change, but are updated through errata, and that he is aware of other professionals in possession of Diffserv, and that Diffserv is available on the Internet at a specific address. Ex. 1004 ¶¶ 129–132. Petitioner also notes document characteristics indicative of its authenticity, including its appearance and contents. In consideration of Dr. Jeffay's testimony and the distinguishing characteristics of the document, we deny Patent Owner's Motion to Exclude Exhibit 1011.

We addressed the issues concerning Ex. 1028 in our earlier discussion of discussion of the public accessibility of ACNS. *See* § VI.B.1.b. We noted the existence of some issues arising from testimony given by Mr. Fuchs in his initial declaration, his supplemental declaration and on cross-examination, we found the characteristics of the ACNS (Ex. 1008) and Release Notes (Ex. 1028) and the consistency of their copyright notices and software versions to be sufficient evidence that the documents are what they purport to be. *Id.* We address Exhibits 1029 and 1030 in Section VI.B.1.b and find sufficient evidence that they are what they purport to be as well. *Id.* Thus, we deny Patent Owner's Motion to Exclude Exhibits 1028–1030.

Patent Owner also moves to exclude Exhibit 1004, the Jeffay Declaration, and Exhibit 1020, the Jeffay Reply Declaration. Mot. To Exclude. 1. Patent Owner objected to Ex. 1004 on the basis that Dr. Jeffays's opinions are conclusory, irrelevant, and do not disclose underlying facts or data in support of his opinions. Paper 10, 1. Neither Patent Owner's objections nor Patent Owner's Motion to Exclude presents any argument

supporting these objections. Patent Owner's Motion is thus denied as to Exhibit 1004.

Patent Owner raised a similar list of objections to the testimony by Dr. Jeffay in his Reply Declaration (Exhibit 1020). *See* Paper 19, 1–3. Patent Owner argues we should exclude Ex. 1027 because Exhibit 1020 purports to authenticate references filed with the Petition that should have been the subject of supplement evidence. Mot. To Exclude 3. Patent Owner's Motion to Exclude does not identify any such references specifically. *Id.* Patent Owner also argues that Dr. Jeffay's Reply Declaration should be excluded because Petitioner is not permitted to introduce new evidence and arguments I its Reply in order to make the *prima facie* case that it should have made in its Petition. *Id.* at 3. Patent Owner's Motion to Exclude does not identify any such arguments. We agree with Petitioner that the subject matter of Dr. Jeffay's Reply Declaration is responsive to matters raised in the Patent Owner Response and Dr. Goodrich's Declaration in support of Patent Owner's response. Opp. to Mot. To Exclude 14–15. Therefore, we deny Patent Owner's Mot. to Exclude Ex. 1020.

Patent Owner objected to Ex. 1021, the deposition transcript of Dr. Goodrich in IPR2018-01386 on the grounds that Petitioner is prejudiced because of its inability to respond to untimely evidence, and because Petitioner uses citations out of context. Paper 19, 3–4. Patent Owner's Motion to Exclude does not discuss Exhibit 1021 explicitly. Patent Owner is not prejudiced, as it had ample opportunity to obtain a declaration from its own expert, Dr. Goodrich, before filing its Patent Owner surreply. In addition, the only subject matter from Exhibit 1021 in this Decision concerns arguments made by Patent Owner that are almost a verbatim repetition of arguments Patent Owner made unsuccessfully in IPR2018-

01386 concerning objective considerations. *See* § VI.B.11. Therefore, we deny Patent Owner's Motion to Exclude Ex. 1021.

Patent Owner also moved to exclude Exhibit 1026, the transcript of Dr. Goodrich's August 29, 2019 deposition in this proceeding. Patent Owner generally objected to Exhibit 1026 as not relevant because it exceeds the scope of Petitioner's Reply and uses citations out of context, but cites no specific testimony. Paper 19, 7. As neither Patent Owner's objections, nor its Motion to Exclude cite any specific testimony or present any argument, Patent Owner's Motion to Exclude Exhibit 1026 is denied.

In consideration of the above, we dismiss Patent Owner's Motion to Exclude Exhibits 1010, 1015, 1017, 1022, 1023, and 1025. We deny Patent Owner's Motion to Exclude Exhibits 1004, 1008, 1011, 1012, 1020–1021, and 1026–1030.

VIII. CONCLUSION[5]

In consideration of the above, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claims 1–9 are unpatentable under 35 U.S.C. § 103(a) over ACNS and Kjendal and that claims 10–16 are unpatentable under 35 § U.S.C.§ 103(a) over ACND, Kjendal, and Diffserv.

[5] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this 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).

In summary:

Claims	35 U.S.C. §	Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1-9	103(a)	ACNS, Kjendal	1–9	
10–16	103(a)	ACNS, Kjendal, Diffserv	10–16	
Overall Outcome			1–16	

IX. ORDER

Inconsideration of the above, it is

ORDERED that claims 1–16 are unpatentable;

FURTHER ORDERED that Patent Owner's Motion to Exclude Exhibits 1010, 1015, 1017, 1022, 1023, and 1025 is DISMISSED;

FURTHER ORDRED that Patent Owner's Motion to Exclude Exhibits 1004, 1008, 1011–1012, 1020–1021, and 1026–1030 is DENIED and

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

FOR PETITIONER:

Daniel McDonald
Jeffrey Blake
Kathleen Ott
Michael Wagner
Christopher Davis
MERCHANT & GOULD P.C.
dmcdonald@merchantgould.com
jblake@merchantgould.com
kott@merchantgould.com
mwagner@merchantgould.com
cdavis@merchantgould.com

FOR PATENT OWNER:

James Hannah
Jeffrey Price
Michael Lee
KRAMER LEVIN NAFTALIS & FRANKEL
jhannah@kramerlevin.com
jprice@kramerlevin.com
mhlee@kramerlevin.com

Bradley Wright
BANNER & WITCOFF LTD.
bwright@bannerwitcoff.com