UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,

Petitioner,

- vs. -

CENTRIPETAL NETWORKS, INC.,

Patent Owner

Case No.: IPR2018-01512
U.S. Patent No. 9,565,213

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases **Page(s)**

Other

PETITIONER'S AMENDED EXHIBIT LIST

EX1001	U.S. Patent No. 9,565,213 (the '213 Patent)
EX1002	Prosecution History of the '213 Patent
EX1003	CV of Dr. Kevin Jeffay
EX1004	Declaration of Dr. Kevin Jeffay dated August 15, 2018
EX1005	Patent Owner's Opening *Markman* Brief in Related Litigation, *Centripetal Networks, Inc. v. Keysight Tech. Inc.*, Case 2:17-cv-00383-HCM-LRL ("*Keysight* lawsuit"), Doc. 106 (filed April 20, 2018)
EX1006	Patent Owner's Rebuttal *Markman* Brief in *Keysight* lawsuit, Doc. 117 (filed May 3, 2018)
EX1007	Parties' Joint Claim Construction Chart in *Keysight* lawsuit, Doc. 124, Ex. 1 (Filed May 11, 2018)
EX1008	Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5 ("ACNS")
EX1009	U.S. Patent No. 9,172,627 ("Kjendal")
EX1010	Hypertext Transfer Protocol (HTTP) 1.1 Specification, as defined in RFC 2616 (the "HTTP 1.1 Specification")
EX1011	"An Architecture for Differentiated Services," also known as the Diffserv architecture, as defined in RFC 2475 ("Diffserv")
EX1012	Declaration of Eli Fuchs, Dated July 2, 2018
EX1013	INTENTIONALLY NOT USED
EX1014	INTENTIONALLY NOT USED
EX1015	Dictionary.com definition of "monitor" found at http://www.dictionary.com/browse/monitor (visited June 7, 2018)
EX1016	Excerpts from File History of European Pat. App. No. 15722292.8
EX1017	"The Internet Standards Process – Revision 3," as defined in RFC 2026, (the "RFC Specification")

EX1018	U.S. Patent Pub. No. 2004/0114518 ("MacFaden")
EX1019	U.S. Patent No. 8,156,206 ("Kiley")
EX1020	Declaration of Kevin Jeffay, Ph.D. in Support of Petitioner's Reply to Patent Owner Response
EX1021	Transcript of Deposition of Michael Goodrich in IPR2018-01386, dated July 17, 2019
EX1022	Broad Agency Announcement 10-004 from the Department of the Navy, Science & Technology Division
EX1023	Wikipedia Page on "List of HTTP Header Fields"
EX1024	INTENTIONALLY LEFT BLANK
EX1025	Request for Comment (RFC) 5424
EX1026	Transcript of Deposition of Michael Goodrich in IPR2018-01512, dated August 29, 2019
EX1027	Supplemental Declaration of Eli Fuchs, Dated October 7, 2019
EX1028	Release Notes for Cisco ACNS Software, Release 5.5.1, dated May 12, 2006 ("Release Notes")
EX1029	Results of Internet Archive Search for Release Notes for Cisco ACNS Software, Release 5.5.1
EX1030	Results of Internet Archive Search for Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5
EX1031	Declaration of Jeffrey D. Blake, Dated October 7, 2019

I. INTRODUCTION

Patent Owner's ("PO") Response (Paper 15) commits three significant errors in its discussion of the claims of the '213 Patent. First, PO argues for a narrowing construction of "dynamic security policy" contrary to its own specification in an effort to sidestep the ACNS prior art reference. Second, PO misrepresents both ACNS and Kjendal (and Petitioner's positions) in arguing the prior art fails to teach identifying or logging packets on a "packet-by-packet" basis. Finally, PO's objective indicia argument is a house of cards having no nexus to the patent claims or evidentiary support. The claims should be found unpatentable.

II. CLAIM CONSTRUCTION

A. "Packet"

Petitioner agrees that the term "packet" refers to a link layer (Layer 2) packet or a network layer (Layer 3) packet. *See* EX1020, ¶¶22-23; EX2009 at 46:10-47:11. Petitioner and Dr. Jeffay applied this construction of "packet" throughout the submissions in this proceeding. *See* EX1020, ¶23.

B. "Dynamic Security Policy"

PO seeks to narrow the construction of "dynamic security policy." Paper 15 at 12-16. The Board properly construed "dynamic security policy," noting it "follows exactly the disclosure in the '213 Patent." Paper 8 at 8-9 (citing EX1001, Col. 4:58-63); EX1020, ¶¶24-25. Thus, PO already acted as its own lexicographer. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1316 (Fed. Cir. 2005) (en banc) ("the

inventor's intention, as expressed in the specification, is regarded as dispositive" of a claim construction).

PO's semantic argument that the specification used "includes" instead of "means" does not allow PO to ignore its definition, especially under the "broadest reasonable interpretation" standard. *Cuozzo Speed Techs., L.L.C. v. Lee*, 136 S. Ct. 2051, 2142 (2016). *See* Paper 15 at 13. This is too little, too late. PO prefaced its definition with the phrase "as used herein," signaling an explicit definition. EX1001, Col. 4:58-63. "Includes," moreover, would only support broadening the phrase, not narrowing it as PO proposes.

PO's proposed construction is inconsistent with the specification and confusing. First, PO argues that a dynamic security policy must be a "non-static **set** of one or more rules." Paper 15 at 14-15 (emphasis in original). The term "set" adds nothing, as the specification frequently refers to the dynamic security policy as having "one or more rules" without using the word "set." *See* EX1001, Cols. 8:4-9:9. The phrase "any rule" in the Board's construction can include "one or more rules." EX1020, ¶¶24-25. Thus, it is not necessary to add "set" to the construction.

Further, PO would narrow the construction of "dynamic security policy" by adding the limitation that the rules in the policy must be "non-static," even though the specification states that the dynamic security policy "includes ***any*** rule… that specifies criteria… and identifies a packet transformation function to be performed."

EX1001, Col. 4:58-63. The phrase "any rule" includes both static and non-static rules. EX1020, ¶¶24-25. Further, as the Board noted, the '213 Patent describes the "dynamic security policy" as being created either manually or automatically. Paper 8 at 7; EX1001, Cols. 14:41-47, 14:56-15:5.

Moreover, PO does not show how its construction would change the outcome of the invalidity analysis. As shown below, it does not.

C. "Monitoring Device"

The Board properly construed the term "monitoring device" to mean a "device configured to copy (or store) packets or data contained within them." Paper 8 at 14-15. PO seeks to narrow the Board's construction because "it fails to give patentable weight to the term 'monitoring.'" Paper 15 at 18-19. That is incorrect. The "copy[ing] or stor[ing] packets or data contained within them" for subsequent review is consistent with the standard definition of monitoring. EX1004, ¶¶121-123; EX1015.

III. ACNS WAS PUBLICLY AVAILABLE

ACNS was publicly available before the priority date (April 16, 2014) of the '213 Patent. PO largely ignores the declaration of Eli Fuchs that establishes the public availability of ACNS. *See* EX1012. Mr. Fuchs testified in his declaration that the ACNS product was on-sale at least by 2008 (*see* EX1012 at ¶¶8-10) and that "all customers who purchased the ACNS product which is the subject of ACNS

opted either to subscribe to a mailing list by which they would be notified (such as by email) of the links to ACNS on the www.cisco.com website, or to otherwise be provided or informed of the availability of that ACNS." *Id.* at ¶11. Mr. Fuchs also explained that "[p]roviding customers with access to the ACNS Guide was important to the users' ability to use the ACNS System." *Id.* at ¶¶12-13. Further, Mr. Fuchs' deposition testimony was unequivocal that customers who purchased the ACNS product were provided a copy of ACNS. EX2021 at 25:20-26:20.

ACNS itself corroborates Mr. Fuchs' testimony. As Mr. Fuchs noted in his declaration, ACNS states that it was intended for "network administrators and content managers." EX1008 at 25; EX1012 at ¶¶12-13. Further, ACNS has a section on "Obtaining Documentation" that states that "Cisco documentation [such as ACNS] and additional literature are available at Cisco.com." EX1008 at 28. ANCS also provides the path that could be used to find it on the website: "You can access the most current Cisco documentation at this URL: http://www.cisco.com/techsupport." *Id.* In addition, ACNS explains that Cisco product documentation, including ACNS, was accessible to customers through a "Product Documentation DVD" or the "the Product Documentation Store in the Cisco Marketplace at this URL: http://www.cisco.com/go/marketplace/". *Id.* at 29.

Mr. Fuchs' declaration also referenced Cisco Release Notes that further corroborate the public accessibility of ACNS. Those Release Notes were

inadvertently left out of Exhibit 1008, but they have now been filed as Exhibit 1028, and a supplemental declaration from Mr. Fuchs indicates these are the Release Notes referenced in his original declaration. *See* EX1027. The Release Notes support the public accessibility of ACNS by explaining that "[t]he most current Cisco documentation for released products is available at Cisco.com." EX1028 at 1. Notably, the Release Notes, which state that they were intended for network administrators using the ACNS product, specifically reference that ACNS was publicly accessible to those administrators: "For more information on creating rule patterns and configuring rule actions, see Chapter 16, 'Configuring Request Processing Services' in the *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments*, Release 5.5 [i.e., ACNS]". *Id.* at 2, 6. The Release Notes also list ACNS as among the "Software Documentation" available to administrators using the ACNS product. *Id.* at 47. These statements in the Release Notes further confirm that ACNS was available to customers (i.e. administrators) at least as early as March 20, 2008. *See* EX1029 (webpage from the Internet Archive showing the Release Notes on Cisco website by March 20, 2008); EX1031.

PO misleadingly cites from the deposition of Mr. Fuchs to argue that he was not aware of when ACNS was publicly available and that his declaration is "solely based on a Google search." That is not correct. Mr. Fuchs testified that the basis for the dates provided in his declaration was ACNS and the Release Notes (along

with his own recollections). EX2021 at 34:3-36:14. The deposition testimony cited by PO involved a question about when ACNS was "first available," and Mr. Fuchs testified that he does not "recall exact dates" but the Google search heled him identify the documentation that corroborates his recollection that ACNS was available at least by March 2008. EX2021 at 24:20-25:19, 34:3-36:14; EX1020, ¶29. Indeed, a search of the Internet Archive located ACNS on the www.cisco.com website as of February 6, 2009 – five years before the priority for the '213 Patent – which further corroborates Mr. Fuchs' testimony. *See* EX1030, EX1031.

IV. CLAIMS 1-16 ARE UNPATENTABLE

A. The System Disclosed in ACNS Acts on a Packet-By-Packet Basis

A fatal flaw underlying many of PO's arguments in its Response is the misplaced claim that the system disclosed in ACNS does not act on a packet-by-packet basis. *See, e.g.*, Paper 15 at 31-35, 42-51. PO is wrong when it argues that "ACNS does not identify packets on a packet-by-packet basis." *Id.* at 42-46. PO is also incorrect that ACNS discloses transaction logging and not logging on a packet-by-packet basis. *Id.* at 31-35, 46-51.

With respect to the identification of packets, PO focuses on the fact that ACNS discusses an "HTTP request" and concludes from this that "ACNS must reassemble L2 and/or L3 packets received by the Content Engine to identify the request method." Paper 15 at 43-44. That is wrong, as ACNS never mentions reassembly.

EX1020, ¶33. Instead, ACNS discloses that its software could analyze application-layer packet-header information in an HTTP packet on a packet-by-packet basis to determine whether the packet is an HTTP packet and whether the HTTP method in the request is supported. *Id.* at ¶¶32-33. For example, in many instances, an HTTP request (such as an HTTP GET or HTTP PUT method call) will be small enough that it can fit inside a ***single*** packet, as Dr. Goodrich admitted in his deposition. *Id.* at ¶32; EX1026 at 27:20-29:8. The '213 Patent also admits as much where claim 5 recites that "***one*** or more ***packets*** comprise an HTTP GET method call" and Claim 7 recites that "***one*** or more ***packets*** comprise an HTTP PUT method call". EX1001, Col. 26:12-13, 26:29-30 (emphasis added in both). Where an HTTP request fits inside a single packet, ACNS necessarily operates on a packet-by-packet basis. EX1020, ¶32.

Further, even where an HTTP request spans multiple packets, ACNS still teaches operating on packets on a packet-by-packet basis. EX1020, ¶33. As Dr. Jeffay explained in his original declaration, an application may recognize a packet as being an HTTP packet based on the request method in the first line of the application-layer packet header. EX1004, ¶155, citing HTTP 1.1 Specification (EX1010); EX1020, ¶33. When an HTTP requests is made, the system disclosed in ACNS can identify that the request is an HTTP request from the request method information in the first packet. EX1004, ¶155, citing EX1008 at 8-23 – 8-24;

EX1020, ¶33. The system would also be able to determine on a packet-by-packet basis that each subsequent packet that is part of the same request is an HTTP packet. *See* EX1020, ¶33. The same would be true if the ACNS product was using ICAP instead of HTTP. *See* EX1008 at 19-1 – 19-5; EX1020, ¶33. Thus, ACNS discloses that the ACNS product looks at each packet on a packet-by-packet basis.

With respect to the logging of packets, ACNS teaches that the logging is performed on a packet-by-packet basis. EX1020, ¶¶34-35. PO acknowledges that the ANCS Guide discloses logging. Paper 15 at 31-35. However, PO argues that the logging is performed on complete transactions, and not on a packet-by-packet basis. *Id.* Again, PO is mistaken. ACNS discloses sample log entries that apply to a single packet, which demonstrates that the ACNS product is capable of logging on a packet-by-packet basis. EX1020, ¶34. For example, ACNS contains a sample "squid" log entry for a transaction whose length is 1,100 bytes, as reproduced below:

1012429341.115 100 172.16.100.152 TCP_REFRESH_MISS/304 1100 GET
http://www.cisco.com/images/homepage/news.gif - DIRECT/www.cisco.com -

Example of Squid Log Entry for a Single Packet (Annotated)

EX1008 at 19-1; *see also id.* at 19-2 (example of "Apache-Style Transaction Logging" for a transaction that is 632 bytes in length – less than the size of one packet). This is smaller than the size of a packet excluding HTTP headers. EX1020, ¶34. Thus, this log entry is for a single packet, and it shows that that ACNS teaches logging on a packet-by-packet basis. *Id.*

PO focuses its analysis on another example log entry in ACNS where the entry reflects a 3,436 byte transaction, which indicates that the transaction spans multiple packets. Paper 15 at 32-33, 47-48. However, the fact that the transaction may have spanned multiple packets does not rule out packet-by-packet logging. EX1020, ¶¶34-35. A POSA would have understood that in order to generate Squid-type log entries, packets can be processed in a packet-by-packet manner without reassembling them. *Id.*, ¶34. The packets could be analyzed individually to determine the properties of the complete transaction, such as its length. *Id.* After the analysis of the individual packets, each packet can be forwarded, dropped, or logged as appropriate, and the log entry may contain information about the complete transaction. *Id.*

B. The Board Correctly Found that the Combination of ACNS and Kjendal Renders Claims 1-9 Obvious.

1. The combination of ACNS and Kjendal teaches receiving a dynamic security policy from a SPMSr (Element [1.1]).

Element [1.1] relates to the packet security gateway ("PSG") receiving a dynamic security policy from the security policy management server ("SPMS"). EX1001, Col. 25:15-18. The Board correctly found that element [1.1] is taught by the combination of ACNS and Kjendal. Paper 8 at 19-23; EX1020, ¶¶56-65. PO disputes that element [1.1] is taught by the art for three reasons, each of which fail to withstand scrutiny.

First, PO argues that the Content Engine in ACNS is not a PSG because the Content Engine "does not inspect packets and does not perform any security analysis on packet[s]." Paper 15 at 23-24. With respect to inspection of packets, Section IV.A above clearly explains that ACNS operates on packets. EX1020, ¶¶56-57. With respect to performing security analysis, the Board already rejected this argument from PO because "ACNS explicitly states that one of the tasks of the Content Engine is 'to implement corporate policies regarding the work environment and ***system security***.'" Paper 8 at 20 (emphasis added), citing EX1008 at 1-9. PO relies on deposition testimony from Mr. Fuchs that the Content Engine does not perform security analysis in practice (*see* Paper 15 at 23), but that testimony cannot negate what is stated in ACNS and what a POSA would understand from the disclosures of ACNS. EX1020, ¶58. Moreover, Mr. Fuchs issued a supplemental declaration acknowledging that ACNS discloses that it performs security analysis, and he overlooked that disclosure during his deposition. EX1027.

PO also argues that "Dr. Jeffay confirmed that the Content Engines are not capable of inspecting the payload of a packet for malware." Paper 15 at 24. This testimony is not relevant because it relates to whether ACNS discloses searching the payloads of HTTP (i.e. application-layer) packets. EX1020, ¶61; EX2020 at 65:19-69:16. As Dr. Jeffay explains, his opinion is that the Content Engine looks to the packet header of an HTTP packet (which can be embedded within a Layer 2 or Layer

3 packet) to determine whether they HTTP packet is using a supported method, and he did not provide an opinion about the Content Engine inspecting the payload of an HTTP packet. Thus, his testimony is consistent with the Content Engine acting as the claimed PSG. EX1020, ¶61.

Second, PO argues that the Content Engine (i.e., the PSG) does not receive a dynamic security policy from the Content Distribution Manager (i.e., the SPMS). Paper 15 at 24-28. The Board already considered and rejected this argument. Paper 8 at 20-22. As the Board noted, the Content Distribution Manager Graphical User Interface ("GUI") is used by the administrator to access the Content Distribution Manager and configure the Content Engine, such as to configure a Content Engine to work with a "WCCP enabled router." *Id.*, quoting EX1008 at 2-12 – 2-13. This constitutes the Content Engine receiving a dynamic security policy from the Content Distribution Manager. EX1020, ¶¶62-63. The command-line interface also can be used by an administrator to add new HTTP request methods to the list of those supported by the ACNS product, which a POSA would understand to be the provision of a new dynamic security policy to the Content Engine. EX1008 at C-6; EX1020, ¶64.

Third, PO asserts that the policies provisioned to the Content Engine in ACNS are not "dynamic security policies" because the policies are "static." Paper 15 at 28-31. This is an attempt by PO to change the construction of the term "dynamic

security policy," and the Board should deny it for the reasons explained in Section II.B above, including the fact that the '213 Patent specification discloses that the dynamic security policies can be changed either manually or automatically. EX1020, ¶65; EX1001, Cols. 14:41-47, 14:56-15:5. Moreover, as noted by the Board, the disclosures in ACNS qualify as a dynamic security policy even under Dr. Goodrich's narrower construction because the rules are "dynamic" in that they allow the ability to modify the acceptable HTTP request methods. EX1008 at 8-23 – 8-24; Paper 8 at 19-20.

2. The combination of ACNS and Kjendal teaches the claimed packet digest logging function (Element [1.2]).

ACNS and Kjendal, in combination, teach the packet digest logging function of element [1.2]. Paper 1 at 30-37; EX1020, ¶¶66-73. The Board agreed with this conclusion, and PO provides no reason to change. Paper 8 at 23-25.

PO begins its analysis of element [1.2] by repeating its argument that ACNS discloses transaction logging and does not teach logging packets on a packet-by-packet basis. Paper 15 at 31-35. This is incorrect for the reasons explained above in Section IV.A, namely that an HTTP "transaction" often can fit inside a ***single*** packet, and thus a log entry for a transaction is the same as a log entry for a packet. EX1020, ¶¶67-69. Indeed, ACNS provides at least two examples of log entries that would fit into a single packet because the number of bytes in the transaction is less than the 1,500 bytes that Dr. Goodrich states is the maximum amount of information

that can be embedded in one packet. *See* EX1008 at 19-1 (Squid log entry with 1,100 bytes), 19-2 (Apache log entry with 632 bytes). Moreover, even in the situation where a HTTP transaction spans multiple packets, the system may analyze the packets containing the transaction one at a time and in isolation, and the system would create a packet digest or log from information extracted from the various packets in the group. EX1020, ¶70. Thus, even in the case of the 3,436 byte transaction cited by PO, the fact that the transaction may have spanned multiple packets does not prevent a packet digest logging function from being performed. *Id.*

Further, PO argues that ACNS does not teach logging packets having the specified application-layer packet-header information. Paper 15 at 33-35. This misstates Petitioner's position on the combined teachings of ACNS and Kjendal. In the combination, Kjendal discloses a system where application-layer packet-header information is used to determine what should be logged. EX1020, ¶71. That teaching would be applied to ACNS. *Id.*

With respect to Kjendal, PO argues that "mirroring a packet is **not** a packet digest logging function." Paper 15 at 34. This focuses on the wrong teaching, as Kjendal discloses that the packet is sent to a network logger – i.e., it is logged – after the mirroring takes place. EX1009, Col. 10:46-58, 29:60-30:16; EX1020, ¶72. PO argues that Kjendal does not teach that the network logger discloses the "identifying," "generating" and "reformatting" steps required by the packet digest

logging function. Paper 15 at 34-35. But those steps are disclosed by ACNS. EX1020, ¶73.

3. ACNS Discloses Identifying Packets with Application-layer Packet-Header Information on a Packet-By-Packet Basis (Element [1.4]).

ANCS discloses element [1.4], which relates to the PSG identifying, on a packet-by-packet basis, packets associated with a protected network that comprise certain application-layer packet-header information. Paper 1 at 39-40; EX1020, ¶¶74-81. PO again repeats its argument that ACNS does not act on a packet-by-packet basis, and it asserts that ACNS must "reassemble the payloads of the packets of HTTP (web) communications flows" to identify the request method of an HTTP request. Paper 15 at 41-46. That is incorrect for the reasons set forth above in Section IV.A, which explain that ACNS discloses a system that identifies packets containing the application-layer packet-header information (e.g., the HTTP request method or ICAP) on a packet-by-packet basis – regardless of whether the request is embedded in a single Layer 2 or Layer 3 packet, or multiple such packets. *See* EX1008 at 8-23 – 8-24, 16-1, 16-15 – 16-25; EX1020, ¶¶77-81. Contrary to PO's arguments, ACNS can identify packets with the application-layer packet-header information without performing reassembly of the application-layer packets. Indeed, ACNS never mentions reassembly. *Id.*

PO incorrectly argues that Dr. Jeffay stated during his deposition that "ACNS is not capable of inspecting the payload of [Layer 2 or Layer 3] packets." Paper 15 at 44. That misstates his testimony. In the testimony cited by PO, Dr. Jeffay stated that he was discussing application-layer packets – not Layer 2 or Layer 3 packets. EX2020 at 65:19-69:16. Thus, his testimony is that ACNS does not disclose the ability to search the payloads of application-layer packets. *Id.* Instead, 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. EX1020, ¶¶32-33.

4. ACNS teaches the identifying limitation of Element [1.6], and the combination of ACNS and Kjendal teaches the generating limitation of Element [1.7].

ACNS teaches element [1.6], which relates to identifying a subset of information specified by the packet digest logging function. Paper 1 at 42-43. The combination of ACNS and Kjendal teaches element [1.7], which relates to generating a record comprising the subset of information from element [1.6]. *Id.* at 43-44.

PO responds to Petitioner's analysis of elements [1.6] and [1.7] by again arguing that ACNS discloses transaction logging and not logging of packets – and thus there can be no packet digest logging function. Paper 15 at 46-51. This argument fails for the reasons discussed above in Paragraphs IV.A. EX1020, ¶¶82-86. Further, with respect to element [1.6], PO asserts that ACNS does not provide

"the level of granularity and specificity" to describe how the packet digest logging function specifies the subset of information to be logged. Paper 15 at 48-49. Yet, the claims of the '213 Patent do not recite any particular level of granularity or specificity required by the packet digest logging function. EX1020, ¶85. Moreover, the examples on pages 19-1 – 19-22 of ACNS provide enough guidance for a POSA to understand that the system is able to log information about individual packets. *Id.*

5. The Combination of ACNS and Kjendal teaches the claimed routing limitation (Element [1.9]).

1. Kjendal teaches element [1.9], which relates to routing one or more packets corresponding to the application-layer packet-header information from the PSG to a monitoring device based in response to a packet transformation function. Paper 1 at 45-47; EX1020, ¶¶87-88. PO's Response does not question that Kjendal teaches routing packets to a monitoring device. Paper 15 at 51-53. Instead, PO argues for the first time that Kjendal does not teach routing packets to a monitoring device "in response to applying the packet transformation function." *Id.* The Board already addressed this argument in IPR2018-01386, another *inter partes* review proceeding relating to the '213 Patent, which is instructive. In that proceeding, the Board found that Kjendal teaches element [1.9] and cited a passage from Kjendal that states "[t]he mirroring may be done selectively rather than simply on a regular basis, which would be inefficient." IPR2018-01386, Paper 8 at 31 (citing EX1009, Col. 7:54-56); EX1020, ¶88. The Board further explained that "Kjendal's selective

mirroring suggests examining packets and executing a transformation function that forwards packets and mirrors only certain packets depending on their characteristics." IPR2018-01386, Paper 8 at 31.

6. There is a motivation to combine ACNS and Kjendal.

A POSA would be motivated to combine the teachings of ACNS and Kjendal. Paper 1 at 24-25, 62; EX1004, ¶¶146, 166, 198; EX1020, ¶¶38-47. The Board correctly found a motivation to combine these references despite earlier arguments to the contrary from PO. Paper 8 at 31-32. Nonetheless, PO again asserts (incorrectly) that there is no motivation to combine. Paper 15 at 35-41.

Predictably, PO's position suffers from the fundamental flaw that PO mischaracterizes ACNS as not teaching logging on a packet-by-packet basis. PO argues that ACNS and Kjendal teach "fundamentally different logging techniques" because ACNS performs "transaction logging" while Kjendal performs "mirroring" of packets. Paper 15 at 37-41. Yet, as discussed above, the HTTP "transactions" referenced in ACNS are often small enough to fit inside a single packet, and thus logging information relating to a transaction is the same as logging the information relating to a packet. EX1020, ¶39. Moreover, even in the situation where a HTTP transaction spans multiple packets, the system may analyze the packets containing the transaction one at a time and in isolation, and the system would create a log from information extracted from the various packets in the group. *Id.*, ¶40.

PO also asserts that Petitioner has not identified a reason why an administrator would combine ACNS and Kjendal. This is wrong. It is not desirable for ACNS to log all packets because the number of log entries may overload a syslog server. EX1020, ¶41. For this reason, ACNS teaches logging only HTTP authentication failures to reduce the number of log entries. EX1008 at 19-19 – 19-22. A POSA would understand from Kjendal that the problem created by logging all packets can also be addressed by selectively logging based on other types of information. *See, e.g.*, EX1009, Cols. 10:46-58; 20:15-19; 29:60-30:16; EX1020, ¶41. PO offers that the combination of ACNS and Kjendal (which both relate to network security) must be "using the '213 Patent as a guide or blueprint," but that is misplaced. Paper 15 at 40. Indeed, the fact that ACNS focuses on authentication errors strengthens the motivation to combine ACNS and Kjendal because Kjendal teaches other ways to selectively log and reduce the number of log entries. EX1020, ¶¶41, 46.

Finally, PO incorrectly asserts that "incorporating the teachings of Kjendal into ACNS would change the operating principal of ACNS." Paper 15 at 40-41. This is again based on the incorrect assumption that ACNS is logging transactions. To the contrary, because ACNS and Kjendal both log based on packets, the combination would improve the performance of the system disclosed in ACNS because Kjendal teaches additional ways to selectively log packets. EX1020, ¶47.

C. The Board Correctly Found that the Combination of ACNS, Kjendal and the Diffserv Specification Renders Claims 10-16 Obvious.

Independent Claim 10 differs from Claim 1 in that Claim 10 recites that the dynamic security policy comprises "packet identification criteria compris[ing] a Differentiated Service Code Point (DSCP) selector" instead of application-layer packet-header information. EX1001, Cols. 26:64-27:3. PO's discussion of Claim 10 by and large incorporates its analysis of Claim 1. Petitioner therefore incorporates its replies on Claim 1.

The only element of Claim 10 that PO addresses in detail is element [10.3], which recites the use of the DSCP as the packet identification criteria. Paper 15 at 54-56. PO appears to acknowledge that the disclosures in ACNS and the DiffServ Specification taught the use of DSCP data. *Id.* However, PO asserts the DSCP data is "used [in ACNS] for packet classification prior to the application of any security policy and not as the packet-identification criteria specified by a dynamic security policy." *Id.* at 55. That is not correct. A POSA would understand the disclosures in ACNS to teach that packets are classified and then marked with a DSCP. EX1020, ¶¶90-92. ACNS discloses that its Content Engines are configured to use the DSCP as a criteria of policies to identify incoming packets. The Content Engine policies may perform security measures, such as virus scanning, "because of the Content Engine's special place as an 'in-line' device between end users and the Internet."

Id., at 1-9. Given that network traffic passes through the in-line Content Engines, a POSA would readily understand that the DSCP can be used as part of a security policy to identify packets to check for malicious network traffic, and to take action on such packets. EX1020, ¶92.

V. OBJECTIVE INDICIA OF NONOBVIOUSNESS

A. PO Did Not Establish a Long-Felt but Unresolved Need, or Failure of Others

PO's evidence of objective indicia of non-obviousness is not compelling. For objective indicia "to be accorded substantial weight, there must be a nexus between the merits of the claimed invention and the evidence of secondary considerations." *Apple, Inc. v. Ameranth, Inc.*, CBM2015-00080, Paper 44 at 36-37 (P.T.A.B. Aug. 26, 2016). The burden of establishing a nexus lies with PO. *See CaptionCall LLC v. Ultratec Inc.*, IPR2013-00540, Paper 78 at 50 (PTAB Mar. 3, 2015).

PO fails to provide the required nexus. EX1020, ¶¶95-96. PO identifies its Threat Intelligence Gateway ("TIG"), or RuleGATE, as fulfilling a long-felt need. Paper 15 at 59-64. PO, however, does not explain whether this product embodies the claims of the '213 Patent, such as performing the claimed "packet digest logging function" or the claimed "routing" of packets "to a monitoring device." EX1020, ¶¶95-96. Dr. Goodrich certainly did not provide the required nexus; he admitted at his deposition that he did not know anything about the operation of the product. EX1021 at 7:22-9:19, 11:22-12:16.

Moreover, PO cannot establish that its products fulfilled a long-felt need or that others failed in fulfilling that need. EX1020, ¶¶97-104. Here, Dr. Goodrich directly undermines PO's position. He had not heard of PO or its products prior to being retained by PO to work on the litigations involving this patent. EX1021 at 7:22-9:19, 11:22-12:16; 12:24-13:23.

The Chincheck presentation (EX2013) demonstrates little. Dr. Goodrich was not present to see the Chincheck presentation, and knows nothing about it. *See* EX1021 at 19:1-22. Moreover, the presentation does not discuss PO's products, ACNS or Kjendal. EX2013. In fact, the presentation specifically states that it "***will not comment on a specific approach***, etc. being considered by an Offeror [i.e., defense contractors for the military]". EX2013 at 3 (emphasis added); EX1021 at 19:23-20:21; EX1020, ¶¶97-98.

PO also relies on an ESG Paper (EX1006) for the alleged satisfaction of long-felt need and failure of others (and industry praise). However, the ESG Paper states on its front page that it was "***commissioned by Centripetal Networks***", i.e. PO. EX1006 at 1 (emphasis added). In other words, PO had the ESG Paper created, and it is not objective evidence. It is entitled to no weight. EX1020, ¶99.

Further, Dr. Goodrich acknowledges that the ESG Paper does not disclose whether the products discussed within it embody the claims of the '213 Patent. EX1021 at 24:12-30:7; EX1020, ¶¶100-103.

B. PO Did Not Establish Industry Praise

PO's industry praise argument also lacks support. Paper 14 at 60-63. PO again argues that its TIG product received industry praise without showing a nexus between the product and the claims of the '213 Patent. EX1020, ¶¶105-107. Moreover, the alleged praise for the TIG product comes from ESG Paper, which PO commissioned. EX2006 at 1. The ESG Paper is PO praising itself, not praise from others in the industry. EX1020, ¶105.

PO also cites a Gartner publication that discusses PO generally and references its QuickThreat Gateway product. Paper 15 at 65-66; EX2007 at 5. The Gartner publication does not explain if the QuickThreat Gateway embodies the claims of the '213 Patent, or how or whether the QuickThreat Gateway differs from Centripetal's TIG product. EX2007 at 5. Thus, the required nexus is again lacking. EX1020, ¶106. Similarly, the American Banker article on "Top 10 FinTech Companies to Watch" does not explain if PO's products embody the claims of the '213 Patent. EX2011 at 14; EX1020, ¶106.

C. PO Did Not Establish Commercial Success or Licensing

PO's argument for commercial success, which relies upon the declaration of Jonathan Rogers, also fails. Paper 15 at 66-68; EX2016. Again, PO fails to prove a nexus between its RuleGATE product and the claims of the '213 Patent. PO and Mr. Rogers baldly state that RuleGATE "embodies the '213 Patent," but they

provide no element-by-element analysis to support this claim. This failure is particularly important in a commercial success analysis because PO is not entitled to a presumption of nexus without proving that a product embodies the claimed invention and is co-extensive with it. *See Brown & Williamson Tobacco Corp. v. Philip Morris Inc*., 229 F.3d 1120, 1130 (Fed. Cir. 2000).

The evidence does not prove commercial success either. Mr. Rogers only identifies three sales of RuleGATE (*see* EX2016 at ¶¶4-6.). He does not state how much revenue was received from these sales, whether PO made a profit on these sales, how much of PO's total revenue is tied to these RuleGATE sales, or how the sales revenues for RuleGATE compare to competitor products.

Mr. Rogers also references sales of "Centripetal's technologies" or "Centripetal's products" in Paragraphs 7-9 of his declaration. EX2016. He does not explain if these other sales include the RuleGATE product. Nor does he state whether the technologies and products discussed in these paragraphs embody the claims of the '213 Patent. PO markets more than one product, so PO has not carried its burden of proving the sales discussed in Paragraphs 7-9 of the Rogers declaration have a nexus to the '213 Patent. Similarly, Mr. Rogers provides almost no details about the "innovation contracts" that allegedly furthered the "commercialization of the RuleGATE product. *Id.*, ¶10.

Finally, PO only identifies one license – to Keysight Technologies to settle a patent litigation. *See* EX1012. The evidentiary value of a license taken to resolve litigation is weakened "because it is often cheaper to take a license than defend [an] infringement suit." *Iron Grip Barbell Co. v. USA Sports, Inc.*, 392 F.3d 1317, 1324 (Fed. Cir. 2004). The Keysight license is of particularly little value here because Keysight was sued on the '213 Patent and other patents. It is impossible to tell what portion of the license revenues are related to the '213 Patent.

VI. CONCLUSION

For the reasons above, and those stated in the Petition (Paper 1), Petitioner asks that the Board cancel claims 1-16 of the '213 Patent as unpatentable.

Respectfully submitted,

Date: October 7, 2019

/Daniel W. McDonald/

Daniel W. McDonald, Reg. 32,044
Merchant & Gould P.C.
150 South Fifth Street
Suite 2200
Minneapolis, MN 55402

Jeffrey D. Blake, Reg. 58.884
Merchant & Gould P.C.
191 Peachtree Street NE
Suite 3800
Atlanta, Georgia 30303

Kathleen Ott, Reg. 64,038
Michael Wagner, Reg. 75,924
Merchant & Gould P.C.

1801 California Street
Suite 3300
Denver, Colorado 80202

Counsel for Petitioner
Cisco Systems, Inc.

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. § 42.24

This paper complies with the type-volume limitations of 37 C.F.R. § 42.24. This paper includes 5,561 words, excluding the parts of the paper exempted by § 42.24(a).

This paper also complies with the type-face requirements of 37 C.F.R. § 42.6(a)(ii) and the type-style requirements of § 42.6)a)(iii) and (iv).

Date: October 7, 2019

/s/ Jeffrey D. Blake
Counsel for Petitioner

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R.42.6(e), that service was made on the Patent Owner as detailed below.

Date of service	October 7, 2019
Manner of service	Electronic Mail (jhannah@kramerlevin.com; jprice@kramerlevin.com; mhlee@kramerlevin.com; bwright@bannerwitcoff.com)
Documents served	PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE
Served upon	James Hannah Jeffrey H. Price Michael Lee Bradley C. Wright (Counsel for Patent Owner)

Date: October 7, 2019

/s/ Jeffrey D. Blake
Counsel for Petitioner