UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

Case No. IPR2018-01512
Patent No. 9,565,213

PATENT OWNER'S SUR-REPLY

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes & Regulations

I. INTRODUCTION

Petitioner's Reply fails to provide any convincing evidence that successfully rebuts Patent Owner's position that the cited references do not render the challenged claims obvious. Petitioner's supplemental declarations and testimony are unable to rescue their own expert's admissions that the cited Content Engines disclosed by the ACNS user guide do not perform any security analysis on packets, and therefore are not packet security gateways, in the context of the claims. Also, Petitioner's Reply is unsuccessful in countering the salient point that the ACNS user guide does not disclose operations be performed on a "packet-by-packet basis," as required by the claims. Further, Petitioner has not substantively addressed Centripetal's arguments that the secondary considerations weigh strongly in favor of patentability. Accordingly Petitioner has not met the high "preponderance of the evidence" standard needed to invalidate the challenged claims of the '213 Patent.

II. CLAIM CONSTRUCTION

A. "packet-by-packet"

In the POR, Centripetal applied a plain and ordinary meaning for "packet-by-packet," similar to a construction that Petitioner's expert articulated during his deposition in a related proceeding involving the patent-at-issue, *i.e.* "you're

working a packet at a time." Patent Owner Response (Paper 15, "POR") at 42-43 (citing Ex. 2009 at 48:8-16).

Despite not disputing that "working a packet at a time" is the correct construction for the term "packet-by-packet," Petitioner argues for a far broader conception of this term in its Reply, one that—incredibly—encompasses "analyz[ing] more than one packet at a time." *See* Petitioner's Reply (Paper 17, "Reply") at 6-9; Ex. 1020, ¶ 17; *id*. at ¶ 26 (Petitioner's expert explicitly discussing the claim construction of "packet-by-packet"). Because Petitioner has raised an issue of claim interpretation in its Reply, Centripetal addresses its arguments and demonstrates that the conception of "packet-by-packet" applied in the POR is correct. 37 C.F.R. § 42.23.

Petitioner attempts to argue that "packet-by-packet" could not possibly mean that "each packet [is] read in complete isolation" because "the technology claimed in the '213 Patent would be limited in its capabilities and may fail to identify packets having certain application layer packet-header information." Ex. 1020, ¶¶ 9-10, 15. Yet this aspect of the meaning of the term "packet-by-packet" was fully acknowledged by Dr. Goodrich, who demonstrated that the "best-in-class performance of Centripetal's TIG" involves a **tradeoff** that foregoes performing "deeper inspection of the application layer" in favor of "implement[ing] rules on a packet-by-packet basis." POR at 63-64; Ex. 2004, ¶ 165; Ex. 2007 at 6; Ex. 2006

at 7-8 (discussing Centripetal's TIG that applies rules "bi-directionally and **without state**" both "delivers more than is possible with firewalls and IPS systems" and achieves "the highest performance network filter that ESG has tested or seen in action to date")(emphasis added). Petitioner failed to address this argument in its Reply.

Based on his misunderstanding or mischaracterization of this tradeoff, Dr. Jeffay opines that the term "packet-by-packet" must be read broadly enough "to analyze more than one packet at a time." Ex. 1020, ¶ 17. However, Dr. Jeffay's position lacks support in the specification of the '213 Patent for such a broad and incongruous reading of the term packet-by-packet, which is directly in contrast to any plain-language understanding of the term as well as his own acknowledgment of what the term means. *Id.*, ¶¶ 9-17; Ex. 2022 (Reply Depo. of Dr. Jeffay) at 22:19-23:14 ("I've just simply taken the plain ordinary meaning of packet-by-packet . . . . I think looking at one packet and **then** looking at another packet and **then** looking at a third packet would certainly be a form of packet-by-packet analysis.")(emphasis added).

The challenged claims are patentable because ACNS discloses "analyz[ing] more than one packet at a time" rather than identifying 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. *See* § III.A, *infra*.

B. "dynamic security policy"

The Board should adopt Patent Owner's proposed construction of the term "dynamic security policy" to mean a "non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets." POR at 12.

Petitioner does not address the arguments advanced in the POR supporting this proposed construction, stating only that "Patent Owner's semantic argument that the specification used 'includes' instead of 'means' does not allow Patent Owner to ignore its definition." Reply at 2. Centripetal agrees and does not seek to change the definition provided in the specification, which should be uncontroversial given that its proposed construction **includes** what the specification says a "dynamic security policy" **includes**. However, Centripetal does dispute that the term "dynamic security policy" **means** any one or more of the things that it can **include**. Thus, while a single "rule… associated with one or more packets" may be **included** within a dynamic security policy, the specification's disclosure does not mean that any "rule… associated with one or more packets" **qualifies as** a dynamic security policy. POR at 14.

Contrary to Petitioner's allegations, this proposed construction is consistent with the specification. *See* Reply at 2. The phrase "set of rules" is used repeatedly throughout the specification (*e.g.*, '213 Patent at 12:22-24, "the dynamic security

policy may be constructed to include a set of rules…"), and is proper under a broadest reasonable interpretation in light of the specification. Furthermore, Petitioner mischaracterizes Patent Owner's proposed construction as requiring the rules be "non-static" even though Patent Owner's proposed construction clearly set forth a "non-static set of rules." *See* Reply at 2; POR at 14-16. Patent Owner's proposed construction correctly interprets the claims with an eye towards giving effect to all terms in the claim by giving appropriate patentable weight to the word "dynamic" in the term "dynamic security policy." POR at 15-16; *Bicon, Inc. v. Straumann Co.*, 441 F.3d 945, 950 (Fed. Cir. 2006).

C. "monitoring device"

The term "monitoring device" should be accorded its plain and ordinary meaning, which is "a device configured to monitor packets."

Petitioner does not dispute Centripetal's argument that the Board's preliminary construction adds limitations from an embodiment (*i.e.* that the monitoring device "**may** be configured to copy the packets or data contained within them") while stripping any patentable weight from the term "monitoring." Reply at 3. Copying packets or the data contained within them is one thing that a monitoring device may do, but that disclosure is not definitional and it is improper to import limitations from the specification into the claims. *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 913 (Fed. Cir. 2004).

Petitioner attempts to rely on extrinsic evidence (e.g., Ex. 1015 citing the fifteenth dictionary definition of "monitor") to add limitations of copying and storing packet data from an embodiment, to the exclusion of the plain language of the claims. Reply at 2-3. The preliminary construction of the term "monitoring device" should therefore be rejected in favor of the plain and ordinary meaning of the term, which is "a device configured to monitor packets."

III. SPECIFIC REASONS WHY THE CITED REFERENCES DO NOT INVALIDATE THE CLAIMS

A. ACNS Does Not Act on a Packet-by-Packet Basis

As a preliminary matter, both parties agree that the term "packet" refers to a link layer (L2) or network layer (L3) packet of the OSI model. POR at 9; Reply at 1. ACNS fails to disclose identifying or logging packets including specified application-layer header information on a packet-by-packet basis. POR at 42–46.

ACNS fails to disclose logging packets on a packet-by-packet basis. As discussed in the POR, the Petition points to ACNS's disclosure of transaction logs, but transaction logs in ACNS are not logs of individual packets identified as having application-layer packet-header information. *See id.* at 31-35; '213 Patent, claim 1 ("performing…on a packet-by-packet basis…"). To the contrary, ACNS teaches creating a record of each transaction requested of the Content Engine. *See* Ex. 1008 at 706-11 (19-10 – 19-15) (describing how to set up a transaction log). A POSA 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 19-10 – 19-11, as opposed to logging information about ***each packet*** that includes application-layer packet-header information. Ex. 2004 (Goodrich Decl.), ¶¶ 116-24; *see also* Ex. 2020 (6/5/19 Jeffay Tr.) at 33:1-11 (describing chapter 19 of ACNS as "logging . . . aspects of [a] transaction").

Petitioner attempts to counter the overwhelming evidence that ACNS is limited to transaction (not packet) logging, by fabricating a sample log entry for a transaction that Petitioner alleges can fit into a single packet. Reply at 8 (citing Ex. 1008 at 19-1, 19-2). At the outset, it should be noted that this log entry is not in the prior art and Petitioner has not met its burden to prove that this actually happened. Furthermore, Petitioner's untenable position that "this log entry is for a single packet, and it shows that that [sic] ACNS teaches logging on a packet-by-packet basis" is baseless. *Id*. The transaction log entry does not mean that the packet transformation function 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. POR at 43-44. Even Petitioner's expert Dr. Jeffay recognized that the plain ordinary meaning of "packet-by-packet basis" required consideration of another packet after another packet, which simply does not occur in ACNS. Ex. 2022 at 22:19-23:14 ("I've just simply taken the plain ordinary meaning of packet-by-packet . . . . I think looking at one packet and then looking at

another packet and then looking at a third packet would certainly be a form of packet-by-packet analysis.").

Petitioner attempts a similar rescue of their position with regards to the claim element of identifying packets on a packet-by-packet basis. Reply at 6-7. But, contrary to Petitioner's contentions, ACNS and Kjendal, taken alone or in combination, fail to teach or suggest "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] As discussed in the POR, Petitioner's argument as to how ACNS allegedly teaches this claim element relies on a fundamental misinterpretation of the subject matter recited in the '213 Patent. Rather than identifying packets that include the recited "application-layer packet-header information" on a **packet-by-packet** basis, ACNS must reassemble the payloads of the packets of HTTP (web) communications flows before determining whether or not a web object should be cached or whether a request for web content should be logged. *See* POR at 41-46; Ex. 2004 (Goodrich Decl.) ¶ 118. In other

[1] Petitioner does not refute or rebut Patent Owner's contention that Petitioner does not assert that Kjendal teaches or suggests identifying packets with application-layer packet-header information on a packet-by-packet. *See* POR at 41.

words, the techniques disclosed in ACNS do **not** include packet-filtering rules that are used to identify packets that include specified application-layer packet-header information on a "packet-by-packet basis." *Id.*

Petitioner's arguments that ACNS "identif[ies]… on a packet-by-packet basis, one or more packets comprising the application-layer packet header information" by identifying an "HTTP request" is incorrect. The fact of the matter is that in order for ACNS to identify an "HTTP request," ACNS must reassemble L2 and/or L3 packets to identify the HTTP request method. POR at 41-42. Neither Petitioner nor Dr. Jeffay directly dispute this fact and instead state that "ACNS never mentions reassembly." Reply at 6; Ex. 1020 at ¶ 77. This statement does little to dispute Dr. Goodrich's explanation of why ACNS needs to reassemble the payloads of HTTP communications. *See* POR at 41-46; Ex. 2004 (Goodrich Decl.) at ¶ 118.

Dr. Jeffay stops short of providing any expert opinion to support Petitioner's position that reassembly would not be required. Ex. 1020 at ¶ 33. Instead, Petitioner and Jeffay rely on a hypothetical example where a HTTP request is small enough to fit inside a single packet to justify their position that "ACNS necessarily operates on a packet-by-packet basis." Reply at 7; Ex. 1020 at ¶¶ 32-33. This is the same logical error as discussed above with respect to logging on a packet-by-packet basis. Aside from the fact that Petitioner has not shown that this

actually happened during the time in question based on the evidence in the record, 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. *See* POR at 41-45.

Petitioner's heavy reliance on their expert's declaration rather than the text of ACNS itself reveals that ACNS, despite its voluminous page count, is scant on the details that are required to render obvious to a POSA the claimed element of "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." Indeed, Petitioner's expert, Dr. Jeffay, admitted repeatedly to the deficiencies of operations with packets (i.e., Layer 2 or Layer 3 packet) in ACNS. *See* Ex. 2022 at 15:23-16:5 ("[T]he ACNS guide I don't believe goes into the details of Layers 2 and 3 because they're not really – they're not really central to its function."); *id*. at 19:5-6 ("I don't believe the ACNS guide discusses much about Layer 2 or Layer 3, as I recall."); *id.* at 15:9-11 ("So, again, what ACNS actually does with regard to TCP I don't believe is disclosed in the guide.").

Additionally, Patent Owner has demonstrated that ACNS's disclosure of using Internet Content Adaption Protocol (ICAP) server functionality does not teach identifying packets with application-layer packet-header information on a

packet-by-packet basis. POR at 45-46. Dr. Jeffay acknowledged that ICAP server rule action are applied to content requests or content response, not individual packets. *See* Ex. 2020 (6/5/19 Jeffay Tr.) at 58:4-11 (stating that the rule actions listed in Table 16-6 are applied to web requests and responses). Petitioner fails to address or rebut this argument in their Reply.

B. ACNS and Kjendal Do Not Disclose Receiving a Dynamic Security Policy From a Security Policy Management Server (Elements [1.1] & [1.2])

Patent Owner has demonstrated that ACNS and Kjendal fail to disclose or render obvious "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," as recited in independent claim 1. *See* POR at 23-31.

Petitioner fails to directly dispute the fact that the Content Engine disclosed by ACNS cannot be a packet security gateway because the Content Engine does not perform any security analysis on packets. Reply at 10. With respect to performing security analysis, Petitioner's reliance on the Board's Institution Decision is misplaced, as that preliminary decision was rendered on an undeveloped record. That record, for example, had yet to include deposition testimony from Mr. Fuchs, the Senior Engineering Manager at Cisco that led the software development team responsible for ACNS, who testified unequivocally

that the Content Engine does not inspect packets and does not "perform any security analysis on the request itself." Ex. 2021 at 15:2-19.

Petitioner attempts to cure this damning admission through a Supplemental Declaration by Mr. Fuchs. Ex. 1027 (the "Fuchs Supplemental Declaration"). However, the Fuchs Supplemental Declaration should be given little weight for the reasons set forth below, and fails to correct Mr. Fuchs's actual testimony. Ex. 1027 at ¶ 6 ("I was asked during my deposition whether the ACNS Guide disclosed that its Content Engine performs any security analysis. I responded, 'It does not.' . . . I want to correct this answer. I have now had the opportunity to further review the ACNS Guide, and it discloses that, while the main function of ACNS is content delivery, the Content Engine can also perform security analysis.").

It is clear from the record that Mr. Fuchs was "responsible for . . . software development team that developed some of the software related to ACNS with a team of approximately 40 engineers responsible for elements of the overall solution." Ex. 2021 at 10:16-22. Throughout Mr. Fuchs's deposition, Mr. Fuchs demonstrated comprehensive knowledge and experience related to ACNS's capabilities and features. *Id.* at 19:18-21:12.

Petitioner now asks the Board to believe that the engineering manager in charge of the ACNS product, who was able to speak at great length about ACNS's

capabilities and features with little prompting, suddenly wishes to correct their answer by quoting the same scant sentences from ACNS that mention the word "security" and that are used by Petitioner to justify their position that the ACNS system is directed towards network security and security analysis. *See* Petition at 32-33. It is simply not persuasive, and as such, Fuchs's Supplemental Declaration should be afforded little creditable weight.

Moreover, Cisco's own expert witness, Dr. Jeffay confirmed that the Content Engines are not capable of performing security analysis, such as inspecting the payload of a packet for malware. Ex. 2020 (6/5/19 Jeffay Tr.) at 68:8-69:16. Petitioner attempts to recast Dr. Jeffay's admission as being related to whether ACNS discloses searching the payloads of HTTP (i.e., application-layer) packets. Reply at 10 (citing Ex. 1020 at ¶ 61). However, a close reading of Dr. Jeffay's Reply Declaration reveals the declaration does not directly state that Dr. Jeffay intended to refer to HTTP Packets rather than L2 and L3 packets in his testimony. Moreover, Dr. Jeffay failed to clarify his testimony during two follow-up questions at deposition, or during cross-examination. Ex. 2020 at 68:13-69:16 ("why do you say ACNS doesn't allow you to, for example, directly inspect the payloads to see if there's malware in the payload?").

Thus, the overwhelming evidence on record establishes that the Content Engines of ACNS are not packet security gateways, and cannot teach or render

obvious "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," as required by the claims.

C. ACNS and Kjendal Do Not Disclose the Claimed Packet Digest Logging Function (Element [1.2]).

Petitioner attempts to argue that 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. Reply at 13. This statement is incorrect and unsupported by the record. Using the below example discussed in the POR, an example transaction logged by ACNS shows that a client made a request ("GET") to the Content Engine to retrieve a resource from a web address at cisco.com. Notably, the below log entry includes information about the entire transaction—in this case an HTTP GET Request—not about a single packet. *Id.*

> [11/Jan/2003:02:12:44 -0800] "***GET*** ***http://www.cisco.com/swa/i/site_tour_link.gif*** HTTP/1.1" 200 ***3436*** "http://www.cisco.com/" "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)"

Ex. 1008 at 699 (19-3) (emphasis added). Again, this log includes information about the transaction (time transaction received, size of the transaction, domain, etc.); the log does not include information about individual packets. Thus, ACNS

does not teach or suggest performing a packet digest logging function for individual packets, as the claims require.

Additionally, Petitioner acknowledges that "ACNS does not explicitly disclose that the logging function can be applied to log packets based on application-layer packet-header information identified by the HTTP request method or ICAP rules." Petition at 35. Petitioner instead relies on "Kjendal teach[ing] that 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 specific application types." *Id.* However, as discussed in the POR, mirroring a packet as discussed in Kjendal is **not** a packet digest logging function, regardless of where the mirrored packet is sent. *See* POR at 34; Ex. 2004, ¶ 121.

Indeed, Kjendal's rules do not control what occurs at the network logger, let alone specify that the network logger carry out a specified packet digest logging function. Ex. 1009 at 10:46–49. That is, simply sending a copy of a packet to a device called a "network logger" is not a packet digest logging function, as claimed, which requires *inter alia* "identifying a subset of information," "generating… a record comprising the subset of information," and "reformatting… the subset of information." *See* '213 Patent, claims 1 and 10. Petitioner fails to

rebut this argument, and instead provides the conclusory statement "those steps are disclosed by ACNS," without further explanation.

For at least these reasons, ACNS in view of Kjendal does not teach or suggest "receiving… a dynamic security policy that comprises at least one rule specifying… a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information," as required by claims 1 and 10.

D. ACNS and Kjendal Do Not Disclose the Claimed Routing Limitation (Element [1.9])

Petitioner has not demonstrated that Kjendal discloses "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." As a preliminary matter, Petitioner does not dispute that the Petition fails to assert that ACNS meets this claim limitation. *See* Petition at 45-47.

Kjendal fails to disclose this element of the challenged claims at least because it does not disclose routing "packets corresponding to the application-layer packet-header information ***in response to*** the performing the packet transformation function" on a packet-by packet basis. POR at 51. Petitioner fails to rebut this argument directly, but instead points to an Institution Decision in another proceeding. Reply at 16-17. Petitioner's reliance on the other proceeding

IPR2018-01386 is misplaced here, because the Board there did not consider the Patent Owner's present argument in full with the presently developed record.

Specifically, Patent Owner argues that claim 1 requires that these packets be routed in response to a packet transformation function being applied to the packets. The Institution Decision has construed the term "packet transformation function" to mean "operations performed on a packet." *See* Institution Decision at 13. Thus, to meet this claim limitation, Petitioner must show that Kjendal routes packets in response to an operation being performed on the packets. However, that is not how Kjendal functions. As discussed in the POR, Kjendal mirrors packet flows based on identifying certain criteria in the packet flow, such as the "selectively" language mentioned by the Institution Decision of IPR2018-01386 quoted by Petitioner. *See* POR at 52; Reply at 16-17. But, that is not enough, particularly in the case of claim 1 of the '213 Patent, where the claim recites that a packet transformation function itself comprises three steps. '213 Patent at 25:38–50 (reciting identifying, generating, and reformatting steps).

Kjendal's disclosure of mirroring packets that have been identified as meeting a criteria, e.g. having the presence of a selected field, does not teach "routing…on a packet-by-packet basis, to a monitoring device each of the one or more packets…***in response to the performing the packet transformation***

function," as recited by claim 1. As such, Kjendal is unable to teach or suggest a modification to ACNS so as to yield the claimed invention.

E. ACNS, Kjendal, and Diffserv Do Not Render Claims 10-16 Obvious

As discussed above, Petitioner has not met its burden to demonstrate that ACNS in view of Kjendal discloses a number of claim elements including: "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;" and "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." *See* POR at 53-57; § III.A., *supra*. Petitioner relies on the same deficient arguments for its application of ACNS and Kjendal to independent claim 10. Petitioner's argument with respect to claim 10 fails for the same reasons that it fails for claim 1.

Additionally, as discussed in the POR, Petitioner fails to establish that the combination of ACNS and DiffServ teaches "wherein the packet-identification criteria comprises a Differentiated Service Code Point (DSCP) selector." POR at 55. To the extent that ACNS and DiffServ disclose utilizing DSCP data, it is used for packet classification prior to the application of any security policy and not as the packet-identification criteria specified by a dynamic security policy. Ex. 2004

at ¶¶ 151-53. Petitioner appears to acknowledge that ACNS fail to disclose using DSCP data for the packet-identification criteria specified by a dynamic security policy, as required by the claims, because Petitioner attempts to rely on expert testimony to cure the deficiencies within ACNS's own disclosure. However, this combination is not supported by the record. *Id*.

Patent Owner respectfully requests, therefore, that the Board find patentable claim 10 and claims 11–16, which depend therefrom.

IV. OBJECTIVE INDICIA OF NONOBVIOUSNESS

Centripetal demonstrated significant objective indicia of nonobviousness with several points of nexus to the challenged claims.

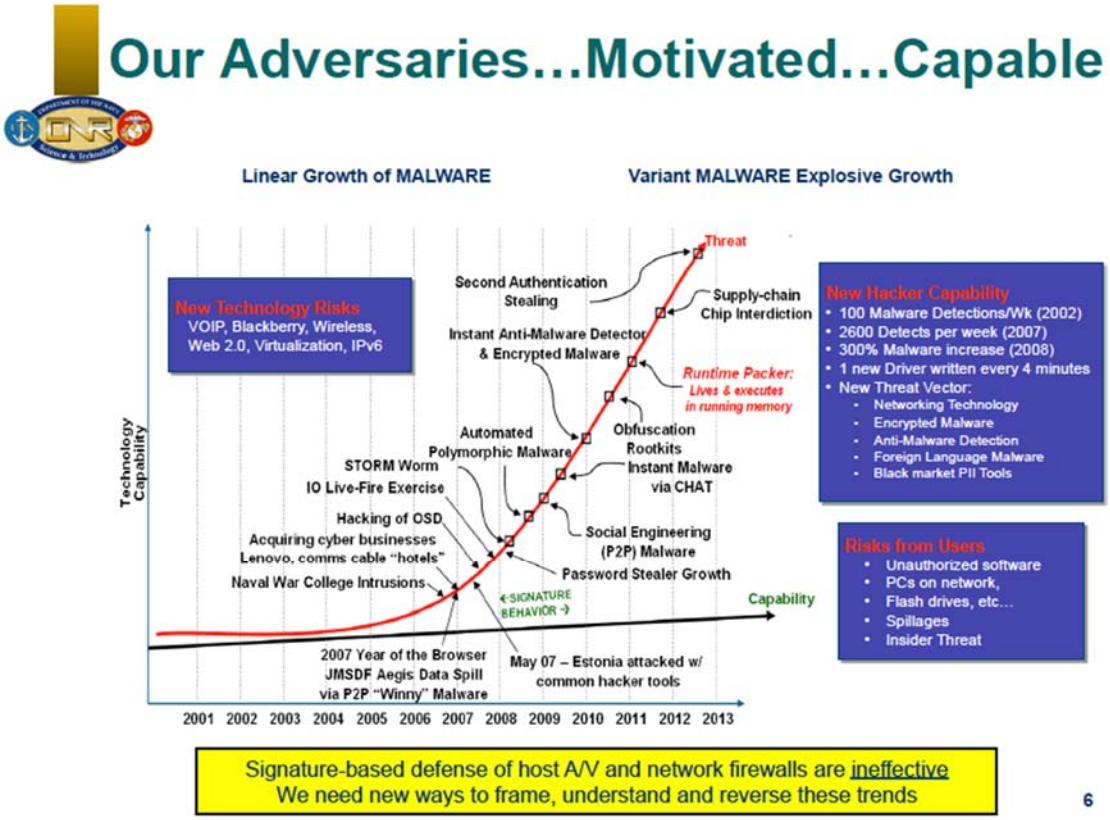
A. Centripetal Demonstrated a Long-Felt But Unresolved Need and Failure of Others

Centripetal produced significant evidence of a long-felt but unresolved need and failure of others as well as a nexus to elements of the challenged claims that were not "readily available in the prior art." *ClassCo, Inc. v. Apple, Inc.*, 838 F.3d 1214, 1220 (Fed. Cir. 2016) (citations omitted).

Petitioner's argument that Centripetal did not establish that Centripetal's Threat Intelligence Gateway, RuleGATE, performed the "packet digest logging function" or "routing" elements of the challenged claims (Reply at 20) mistakes the proper test for finding a nexus between the evidence provided and the challenged claims because it is not necessary to show that any particular product

embodies every aspect of the claim under review. Rather, the proper test for nexus asks whether "a nexus exists between the claimed features of the invention and the objective evidence offered to show non-obviousness." *WMS Gaming, Inc. v. Int'l Game Tech.,* 184 F.3d 1339, 1359 (Fed. Cir. 1999) (citation omitted). The evidence reviewed and discussed by Dr. Goodrich easily meets this standard.

Petitioner also curiously discounts the Chincheck presentation for not discussing the '213 Patent or the prior art. Reply at 21. This argument mistakes Centripetal's reliance on this document. In particular, this presentation was cited to **establish** a long felt need in the industry, *i.e.* that "previous strategies for protecting networks could not keep up with changes in the environment." POR at 60-61 (citing Ex. 2013 at 5-6; Ex. 2004 at ¶ 160). The chart reproduced in the POR establishes that "[t]he failure of signature behavior based systems, such as the ones disclosed in [Narayanaswamy and Kapoor], to keep up with emerging threats demanded new solutions." *Id.* at 61.



Ex. 2013 at 6.

Other evidence, including the ESG Whitepaper (Ex. 2006) and the Gartner Cool Vendors report (Ex. 2007), establish that Centripetal's TIG **fulfilled** this long-felt need. Petitioner dismisses the ESG Paper out of hand, arguing that the paper's acknowledgment that it was "commissioned by Centripetal Networks" means that "it is not objective evidence" and is entitled to no weight. Reply at 21. To the contrary, Cisco identifies the Enterprise Security Group as a "well-known analyst research company." https://blogs.cisco.com/security/cisco-annual-security-report-2015-secure-access-for-defending-against-threats. Given that this well-

known analyst research company's reputation would suffer if it disseminated baseless propaganda, it is unreasonable to suggest that the ESG Paper is entitled to no weight.

Tellingly, Petitioner does not quibble with the substance of the ESG Paper, arguing only that it does not discuss packet digest logging function or routing to a monitoring device features, as specifically claimed in the '213 Patent. Reply at 21. Yet the proper test only that the evidence is "reasonably commensurate with the scope of the claims." *Rambus Inc. v. Rea*, 731 F.3d 1248, 1257 (Fed. Cir. 2013) (citation omitted).

More importantly, Petitioner entirely ignores other evidence discussed in the ESG Paper that is explicitly tied to elements of the challenged claims. For example, Centripetal explained that the '213 Patent's "dynamic security policy" being received from a "security policy management server" is what enables "the transformation of CTI into protective action at scale." POR at 62-63. Furthermore, Centripetal established that the ESG Paper's praise of Centripetal's TIG's performance was explicitly tied to the fact that its rules are applied on a "packet-by-packet" basis. *Id*. at 62-64. Petitioner does not address, let alone rebut, this evidence that Centripetal's technology satisfied a long-felt need in the industry.

B. Industry Praise

Petitioner also failed to address the significant evidence of industry praise on its face, arguing that the praise in the ESG paper is evidence of "Patent Owner praising itself," when ESG is, by Cisco's own admission a "well-known analyst research company." Reply at 22. Petitioner also attempts to dismiss the Gartner report on the basis that it does not "explain if the QuickThreat Gateway embodies the claims of the '213 Patent." *Id.* Again, however, this is not the test. *See* § IV.A, *supra*. Centripetal's unrebutted evidence and testimony ties the industry praise to both the "dynamic security policy" and "packet-by-packet" elements of the challenged claims demonstrating that the challenged claims are not obvious over the prior art. POR at 65-66.

C. Commercial Success and Licensing

Centripetal also produced evidence of commercial success and licensing. Petitioner faults this evidence for not including an "element-by-element analysis." Reply at 22-23. However, Petitioner cites no authority that an "element-by-element analysis" is necessary. In fact, the sole case cited as authority for its broad conclusion states that "if the marketed product embodies the claimed features, and is coextensive with them, then a nexus is presumed." *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1130 (Fed. Cir. 2000).

Centripetal's COO, Jonathan Rogers, executed a declaration in this case, testifying under oath that the RuleGATE product embodies the claims of the '213 Patent. Ex. 2016. If Petitioner had reason to question Mr. Rogers's testimony, it was free to depose him on his declaration. It did not. Thus "a nexus is presumed," and it was incumbent on Cisco to put forth evidence rebutting the presumption. *Brown & Williamson*, 229 F.3d at 1130. It did not.

Petitioner also argues that evidence that "[t]he 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.'" Reply at 24, citing *Iron Grip Barbell Co. v. USA Sports, Inc.*, 392 F.3d 1317, 1324 (Fed. Cir. 2004). That may be true in circumstances where the defendant takes a license to a patent early in the case, but in the *Keysight* case the parties settled halfway through the infringement trial. *Centripetal Networks, Inc. v. Keysight Tech's, Inc.*, No. 2:17-cv-00383, Dkts. 576, 581 (E.D. Va.). In this case, the full evidentiary value of the license should be accorded because it is more likely that Keysight was more concerned with a potential infringement verdict than a few more days of trial in a case that already spanned over a year.

V. PETITIONER HAS NOT ESTABLISHED THAT ACNS WAS PUBLICALLY AVAILABLE BEFORE THE PRIORITY DATE

The declarations and exhibits accompanying Petitioner's Reply provide conflicting evidence and fail to demonstrate that ACNS is a printed publication

within the definition set forth by 35 U.S.C. §311(b). Reply at 3-6; Exs. 1027-1031. Petitioner's declarant, Mr. Fuchs, had previously testified that Cisco's standard operating procedure relating to software release notes, in that software releases "[were] accompanied with release notes which were issued after the public release of the ACNS Guide Version 5.5." Ex. 1012 at ¶ 13. Petitioner attempts to argue that the Release Notes (Ex. 1028) corroborate that the ACNS Guide was accessible to customers who purchased the ACNS product at least as early as March 20, 2008. *See* Reply at 5; Ex. 1027 (Fuchs Supp. Decl.) at ¶ 4.

However, the Release Notes appear to have a publication date (May 12, 2006) that does not match or approximate the purported publication date of the ACNS Guide (March 20, 2008), suggesting that the dates provided by the Cisco documentation and website are unreliable. Ex. 1028 at 1. No explanation is provided for this discrepancy of nearly 2 years. No explanation is provided for why the Release Notes appear to have been published before the purported public release of the ACNS Guide, and not "issued after the public release of the ACNS Guide Version 5.5" that Petitioner's declarant testified was Cisco's standard operating procedure. Ex. 1012 at ¶ 13; *see also Kinetic Techs., Inc. v. Skyworks Sols., Inc*., IPR2014-00690, Paper 43 at 19 (P.T.A.B. Oct. 19, 2015)("A 'printing date' is not, however, without more, sufficient evidence of public accessibility as of that particularly date").

Furthermore, Fuchs's Supplemental Declaration states that the Release Notes corroborate that the ACNS Guide was accessible to customers who purchased the ACNS product at least as early as March 20, 2008, but provides no allegation or supporting evidence that any sales or actual distributions of the ACNS user guide occurred. *See* Ex. 1027 at ¶ 4; Ex. 2021 at 28:8-10 ("Q. Do you know approximately how many people have purchased Cisco ACNS? A. I do not.").

Accordingly, Petitioner fails to demonstrate by a preponderance of the evidence that the ACNS user guide is a printed publication available before the priority date of the patent-at-issue.

VI. CONCLUSION

Petitioner has not established by a preponderance of the evidence that the challenged claims 1–16 of the '213 Patent are invalid. Centripetal accordingly requests that the Board find claims 1–16 patentable.

Respectfully submitted,

Dated: October 29, 2019

/James Hannah/

James Hannah (Reg. No. 56,369)
Michael Lee (Reg. No. 63,941)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road
Menlo Park, CA 94025
Tel: 650.752.1700 Fax: 212.715.8000

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: 212.715.7502 Fax: 212.715.8302

Bradley C. Wright (Reg. No. 38,061)
Banner & Witcoff, Ltd.
1100 13th Street NW, Suite 1200,
Washington, DC 20005.
Tel: 202.824.3160. Fax: 202.824.3000.
Email: bwright@bannerwitcoff.com.

(Case No. IPR2018-01512)

Attorneys for Patent Owner

CISCO SYSTEMS, INC.,
v.
CENTRIPETAL NETWORKS, INC.,

Case IPR2018-01512
Patent 9,565,213

PATENT OWNER'S EXHIBIT LIST

Exhibit-2001	Opinion and Order re Claim Construction, *Centripetal Networks, Inc., v. Keysight Tech's, Inc., et al*., No. 2:17-cv-00383 (Dkt. 484).
Exhibit-2002	Amended Joint Claim Construction Statement, Exhibit 2, *Centripetal Networks, Inc., v. Keysight Tech's, Inc., et al*., No. 2:17-cv-00383 (Dkt. 244-2).
Exhibit-2003	Intentionally Omitted
Exhibit-2004	Declaration of Dr. Michael Goodrich in Support of Patent Owner's Response with Appendix A (CV)
Exhibit-2005	Intentionally Omitted
Exhibit-2006	ESG White Paper – Centripetal Networks Threat Intelligence Gateway, by Tony Palmer (May 2018)
Exhibit-2007	Gartner – Cool Vendors in Security for Technology and Service Providers, 2017, published May 4, 2017
Exhibit-2008	Excerpts from Tanenbaum, *Computer Networks*, 5th edition, Prentice-Hall, 2011
Exhibit-2009	Deposition Transcript of Dr. Kevin Jeffay in IPR2018-01386, taken on April 18, 2019
Exhibit-2010	Gupta and McKeown, *Algorithms for Packet Classification*, IEEE NETWORK, March/April 2001.
Exhibit-2011	American Banker article, "Top 10 FinTech Companies to Watch," published November 6, 2013.

Exhibit-2012	KeySight Technologies, Inc. Annual Report 2018
Exhibit-2013	Stanley Chincheck, US Naval Research Laboratory, Computer Network Defense/Information Assurance (CND/IA) Enabling Capability (EC) Industry Day
Exhibit-2014	Schuster, "Introducing the Microsoft Vista event log file format," *Digital Investigations* 4S (2007), S65-S75, Elsevier Ltd.
Exhibit-2015	"7.8. Packet Reassembly" from https://www.wireshark.org/docs/wsug_html_chunked/ChAdvReassemblySection.html
Exhibit-2016	Declaration of Jonathan Rogers
Exhibit-2017	Cisco webpage, Cisco ACNS Software Version 5.5, https://www.cisco.com/c/en/us/support/application-networking-services/acns-software-version-5-5/model.html
Exhibit-2018	Cisco webpage, Cisco ACNS Software Version 5.5 – Retirement Notification, https://www.cisco.com/c/en/us/obsolete/application-networking-services/cisco-acns-software-version-5-5.html
Exhibit-2019	Wikipedia – Maximum transmission unit, https://en.wikipedia.org/wiki/Maximum_transmission_unit
Exhibit-2020	Deposition Transcript of Dr. Kevin Jeffay in IPR2018-01512, taken on June 5, 2019
Exhibit-2021	Deposition Transcript of Eli Fuchs in IPR2018-01512, taken on June 28, 2019
Exhibit-2022	Deposition Transcript of Dr. Kevin Jeffay in IPR2018-01512, taken on October 22, 2019

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

This paper complies with the type-volume limitation of 37 C.F.R. § 42.24. The paper includes 5,594 words, excluding the parts of the paper exempted by § 42.24(a).

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

/James Hannah/

James Hannah (Reg. No. 56,369)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road,
Menlo Park, CA 94025
(650) 752-1700

CERTIFICATE OF SERVICE

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

Date of service October 29, 2019

Manner of service Electronic Mail (dmcdonald@merchantgould.com; jblake@merchantgould.com; kott@merchantgould.com; mwagner@merchantgould.com; CiscoCentripetalIPR@merchantgould.com)

Documents served PATENT OWNER'S SUR-REPLY

Persons Served Daniel W. McDonald
Jeffrey D. Blake
Kathleen E. Ott
Michael S. Wagner
Merchant & Gould P.C.

/James Hannah/
James Hannah
Registration No. 56,369
Counsel for Patent Owner