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

DECLARATION OF KEVIN JEFFAY, PH.D. IN SUPPORT OF PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I, Kevin Jeffay, Ph.D., hereby declare as follows:

I. BACKGROUND

1. I have been retained by Cisco Systems, Inc. ("Cisco") to provide my technical review, analysis, insights, and opinions concerning the validity of the claims of U.S. Patent No. 9,565,213 (EX1001; "the '213 Patent") entitled "Methods and Systems for Protecting a Secured Network."

2. I am the same Kevin Jeffay who provided a declaration in support of Cisco's Petition for *Inter Partes* Review in this proceeding on July 11, 2018. *See* EX1004. I maintain the opinions that were set forth in that previous declaration. I provide this declaration to respond to certain opinions provided by Dr. Michael Goodrich in a declaration (the "Goodrich Declaration") submitted in support of the Patent Owner Response filed by Patent Owner Centripetal Networks, Inc. ("Patent Owner") in this proceeding. The Goodrich Declaration is marked as Exhibit 2004 in this proceeding.

3. My background and qualifications were set forth in Paragraphs 1-11 of my original declaration in this proceeding, as well as my curriculum vitae marked as Exhibit 1003. In this reply declaration, I apply the same understanding of the governing law as set forth in Paragraphs 12-19 and 104 of my original declaration.

4. In this declaration, I apply the same definition of a person or ordinary skill in the art ("POSA") as set forth in Paragraphs 22-24 of my original declaration.

I understand that Dr. Goodrich provided a definition of a POSA that differs from mine. EX2004, ¶¶47-49. I disagree with Dr. Goodrich's proposed definition of a POSA, and I continue to believe my definition more accurately reflects the proper skill level of a POSA. This is particularly true for the professional experience that I believe a POSA would have. It is my opinion that in this ever-changing field of technology, a POSA should have professional experience actually implementing and securing packet-switched networks, and thus have experience with communication protocols and protocol layers, firewalls, security policies, and customized rules to address cyber-attacks. Dr. Goodrich's definition of a POSA ("someone with a bachelor's degree in computer science or related field, and either (1) two or more years of industry experience and/or (2) an advanced degree in computer science or related field") provides an alternative under which a person with no professional experience or training in networking could still be considered a POSA, and I disagree. *Id.*, ¶48. Nonetheless, I believe I would qualify as a POSA under both my definition of a POSA and the definition provided by Dr. Goodrich. Further, the analysis in my original declaration and my analysis herein would be the same under either my definition of a POSA or the definition provided by Dr. Goodrich.

5. In this declaration, I apply the same priority date for the '213 Patent of April 16, 2014, as was set forth in Paragraph 102 of my original declaration. Dr. Goodrich agrees on this priority date. EX2004, ¶46; EX1021 at 9:20-11:21.

6. In forming my opinions, I have relied on the ’213 Patent’s claims, specification, and the prosecution history, on the prior art exhibits to the IPR Petition for the ’213 Patent (Paper 1), any other materials cited in this declaration, and my own knowledge, experience, and expertise, and the knowledge of a POSA in the relevant timeframe. I have also reviewed and relied upon the materials cited in my original declaration and the materials cited in the Goodrich Declaration. I have also reviewed the Decision on Institution of *Inter Partes* Review provided by the U.S. Patent and Trademark Office Patent Trial and Appeal Board (the “PTAB”) in this proceeding. *See* Paper 8.

II. DISCUSSION OF COMPUTER NETWORKING CONCEPTS

7. Paragraphs 25-78 of my original declaration provide a background discussion of computer networking concepts. EX1004. In response, Dr. Goodrich provides his “Overview of Relevant Technologies” in Paragraphs 32-43 of the Goodrich Declaration. EX2004. I agree with some portions of his discussion of the technology, but I find the discussion of packet reassembly set forth in Paragraph 43 of the Goodrich Declaration misleading and irrelevant.

8. Paragraph 43 of the Goodrich Declaration discusses that a “traffic filtering or analysis system often will then need to reassemble the application layer payloads of the packets” in a packet flow. EX2004. Dr. Goodrich goes on to state in Paragraph 43 that “the packets from an HTTP session may need to be reassembled

in order to determine the full contents of a requested web page." *Id.* It is my opinion that reassembly is irrelevant to the technology claimed in the '213 Patent. The claims of the '213 Patent recite identifying, "on a packet-by-packet basis," certain packet header information, such as "application-layer packet-header information" or the "Differentiated Service Code Point (DSCP) selector," and performing a packet transformation function "on a packet-by-packet basis" on each of the packets having the identified header information. EX1001, Col. 25:14-55, 26:60-27:35. The claims do not address reassembly of the payload of the packet or analysis of the reassembled payload content. Dr. Goodrich recognizes this difference between analyzing ***packet headers*** (as claimed) and analyzing reassembled application-layer ***payloads or content***. *See* EX2004, ¶51 (discussing that "the PSGs of the '213 Patent can evaluate the ***header*** information at the network level without resorting to packet reassembly techniques typically required for application-layer ***content*** analysis" (emphasis added).

9. Dr. Goodrich appears to raise the concept of reassembly so that he can contrast it against the narrow view of "packet-by-packet" analysis that he maintains. The packet-by-packet analysis provided by Dr. Goodrich would have each packet read and processed in complete isolation. *See, e.g.*, EX2004, ¶¶50-52, 72-75 and 116-124. Dr. Goodrich argues that the prior art must reassemble application-layer messages before applying the dynamic security policies to them because he does not

believe the prior art performs packet-by-packet analysis under his narrow view. Yet, none of the prior art references discuss reassembly in any manner.

10. Moreover, 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. The Board's institution decision does not so limit the claims. Further, Patent Owner didn't seek a claim construction that would limit "packet-by-packet" to analysis of individual packets in isolation in either this proceeding or the ongoing litigation between Cisco and Patent Owner. *See* Paper 8 at 7-15; EX1005-EX1007, EX2002.

11. In addition, the '213 Patent discloses a broader use of "packet-by-packet." For example, the '213 Patent contemplates that an HTTP request may be 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 and then performing the packet transformation function on all of the packets associated with the HTTP request. This is clear from the dependent claims of the '213 Patent. Claim 4 recites that "application-layer packet-header information identifies one or more hypertext transfer protocol (HTTP) packets." EX1001, Col. 26:4-11. Claim 4 further states that "one or more packets comprising the application-layer packet-header information are ***amongst*** the one or more HTTP packets." *Id.* (emphasis

added). This discloses to a POSA that only certain packets will contain the application-layer packet-header information relating to an HTTP request (such as the request method), but that application-layer packet-header information can be used to identify all of the HTTP packets that make up the HTTP request, and the packet transformation function recited in independent claim 1 will be applied to all of those HTTP packets. *Id.* Thus, the claimed "packet-by-packet" analysis can involve looking at more than just one packet in isolation.

12. Similarly, dependent Claim 5 of the '213 Patent relates to an "HTTP GET method call." Claim 5 recites that "one or more packets comprising the application-layer packet-header information are ***amongst*** the one or more HTTP packets" that make up the HTTP GET method call. EX1001, Col. 26:12-19 (emphasis added). The claimed method determines "that the one or more packets comprising the application-layer packet-header information are associated with the HTTP GET method call." *Id.* In this way, all of the packets comprising the HTTP GET method call are identified from the one or more packets containing the application-layer information, and the packet transformation function is performed on all of the packets comprising the HTTP GET method call.

13. Further, the specification of the '213 Patent supports the fact that the packet-by-packet analysis does more than look at each packet in isolation. For instance, Figure 12 "illustrates an exemplary method for protecting a secured

network that includes performing a packet digest logging function on packets that ***correspond*** to specified packet-identification criteria." EX1001, Col. 22:7-10 (emphasis added); Figure 12. "At step 1208, the packet security gateway may perform, on a packet-by-packet basis, the packet digest logging function on each of the packets ***corresponding*** to the packet-identification criteria." *Id.*, Col. 22:53-57 (emphasis added); *see also id.*, Col. 22:42-53 (reciting "one or more packets corresponding to the packet-identification criteria" such as packets that "comprise" the specified header information). By contrast, the embodiment shown in Figure 11 of the '213 Patent performs the packet transformation function on packets "comprising the application-layer packet-header information" at step 1108. A POSA would understand that the use of the term "comprising" in Figure 11 means the packet transformation function is performed on packets that actually have the application-layer packet-header information, whereas the use of "corresponding" in Figure 12 is broader and indicates that packet B may be treated like packet A if it corresponds to A – such as when packets A and B are part of the same HTTP request – even if packet B does not have the application-layer packet-header information itself. The disclosure in Figure 12 is still "packet-by-packet" analysis because each packet can be fully processed as it is seen. Thus, the specification of the '213 Patent does not support Dr. Goodrich's narrow reading that the term "packet-by-packet" means each packet is viewed in isolation.

14. Indeed, Dr. Goodrich doesn't point to anything in the '213 Patent that contradicts the information discussed above demonstrating the claimed packet transformation function(s) will be performed on packets corresponding to or associated with the packet(s) containing the application-layer packet-header information. It is simply his opinion that it would be implied to a POSA that "packet-by-packet" analysis means the packets must be viewed in isolation. EX2004, ¶¶50-52, 72-75 and 116-124. Yet, Dr. Goodrich contradicts this opinion in other portions of his declaration, where he argues that the "packet-by-packet" analysis is one of the novel features of the '213 Patent that he believes led to Patent Owner's products being considered "best-in-class." EX2004, ¶165. Dr. Goodrich cannot credibly maintain that a POSA would implicitly know that "packet-by-packet" analysis means looking at each packet in isolation, while also arguing that such packet-by-packet analysis is a key distinction between the claimed invention and the prior art that makes the claims of the '213 Patent nonobvious, particularly where this distinction is not even mentioned in the specification.

15. Moreover, Dr. Goodrich's view of "packet-by-packet" would not make sense to a POSA 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. For example, a POSA understands that the payload of

one packet (e.g., a network layer packet) may contain the header and payload of another type of packet (e.g., an application layer packet), as shown below:

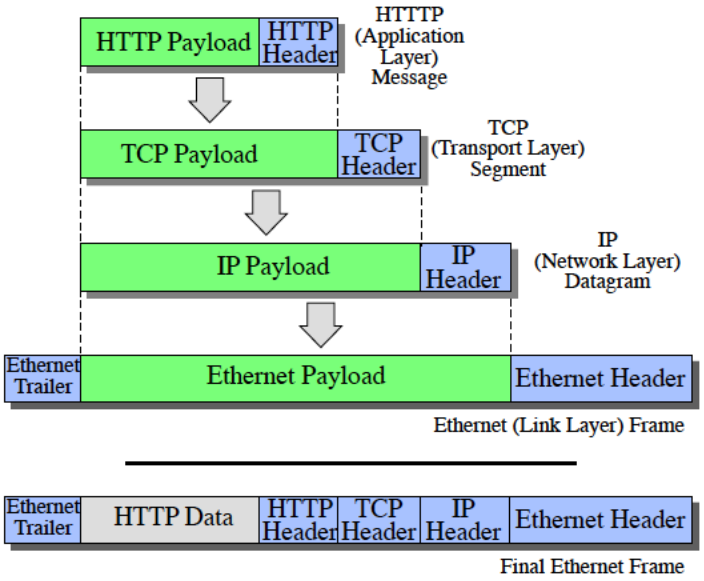

Figure 1: Embedding of protocol data units during the transmission process.

See EX1004, ¶51. If the headers in an HTTP message are large enough to span multiple lower layer packets, the technology claimed in the '213 Patent (as interpreted by Dr. Goodrich) can only identify packets based on application-layer packet-headers in the first packet of a lower layer protocol in a data flow containing application layer data. This is because per the specification of (virtually) all application layer protocols, fixed strings (protocol commands or responses such as "GET" in the case of HTTP) appear at the start of the application-layer message and can thus be used as a means of uniquely identifying the first packet as conforming to a specific application layer protocol.

16. If the headers continue into the second packet of a lower layer protocol, the technology of the ’213 Patent can’t analyze those headers based on examining the second packet alone (i.e., based on doing packet-by-packet analysis in isolation), because the second packet likely will not contain any unique strings or “markers” and as such one can’t determine with any certainty that the contents of the second packet are HTTP headers or HTTP payload data (e.g., payload data that happens to resemble header data). For example, if you see the string “Accept-Language: en-US” in a packet, unless this packet is the first packet in an HTTP connection (as determined by finding a command such as GET in the first line of the application-layer message), you can’t tell if this string is a part of the header of the application-layer message, or part of the payload of the application message. *See, e.g.*, EX1023 (https://en.wikipedia.org/wiki/List_of_HTTP_header_fields) (where the string “Accept-Language: en-US” appears in both the header and payload of the application-layer message that returns the requested webpage). Moreover, HTTP does not specify the order in which data items appear in the application-layer packet-header. *See* EX1010. Therefore, a particular name-value pair (i.e., particular header information) may be in the first packet or a subsequent packet. As a result, the technology claimed in the ’213 Patent that looks for application-payer packet-header information on a “packet-by-packet basis,” as Dr. Goodrich construes that phrase, may not identify a name-value pair in the header of an HTTP request where the

name-value pair does not appear in the first packet of a lower layer protocol transmitting an HTTP request or response.

17. One method of addressing this problem is to analyze more than one packet at a time. Prior art systems classify packets (such as HTTP packets) according to the flow to which they belong. *See* EX2004, ¶¶40-42. Once the flow has been established, prior art systems can analyze the packets by: (1) looking at each packet in isolation, (2) analyzing each packet, in part, by comparing it to other packets in a flow, or (3) analyzing groups of packets within a flow. The 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. These analysis techniques can also be implemented such that a system still inspects each packet on a packet-by-packet basis.

III. THE ’213 PATENT

18. Paragraphs 79-101 of my original declaration provide an overview of the ’213 Patent, including its specification, claims and prosecution history. Dr. Goodrich provides his overview of the ’213 Patent in Paragraphs 44-45 and 50-58 of the Goodrich Declaration. I disagree with certain opinions provided by Dr. Goodrich in his overview of the ’213 Patent, as discussed below.

19. Dr. Goodrich begins his discussion of the ’213 Patent with a statement that “Centripetal develops and produces products and software solutions in the field

of cybersecurity that are designed to protect computer networks against advanced cyber-attacks." EX2004, ¶44. Dr. Goodrich does not cite anything in support of this statement or any of the other statements in Paragraphs 44-45 concerning Patent Owner's products. Further, Dr. Goodrich admitted in his deposition in IPR2018-01386 that he does not know anything about the operation of Patent Owner's products. EX1021 at 7:22-9:19, 11:22-12:16. He had not heard of Patent Owner or Patent Owner's products prior to being retained by Patent Owner to work on the litigations involving the '213 Patent. *Id.* It is therefore my opinion that Dr. Goodrich has no basis for his statements in Paragraphs 44-45 about the operation and capabilities of Patent Owner's products. Moreover, Dr. Goodrich does not cite anything to show that Patent Owner's products embody the technology claimed in the '213 Patent. In addition, I disagree with the statement by Dr. Goodrich in Paragraph 45 that the '213 Patent "provides a novel approach to detect sophisticated network attacks as a part of a proactive solution." It is my opinion that the claims of the '213 Patent are not "novel" for the reasons stated in Paragraphs 146-235 and 241-302 of my original declaration (EX1004) and Paragraphs 56-108 below, as well as my opinions provided in another *inter partes* review proceeding relating to the '213 Patent. *See* IPR2018-01386.

20. Dr. Goodrich also makes the statement that "[a]pplication-layer packet-header information is structured into standardized fields at specific locations of an

IP packet." EX2004, ¶51. This is not necessarily true. As discussed in Paragraphs 15-16 above, there are protocols, such as HTTP, where headers can consist of an arbitrary number of (literally) arbitrary name-value pairs. As a result, application-layer packet-header information may span multiple packets. Further, the specification for the HTTP protocol specifies the order in which some but not all data items appear in the header. Thus, different application-layer packet-header information may be present in different packets, and it is not all structured into standardized fields at specific locations in a packet.

21. Dr. Goodrich also addresses reassembly in his analysis of the '213 Patent. EX2004, ¶¶51-53. As discussed above in Paragraph 8, I do not believe that reassembly is relevant to the analysis of the claims of the '213 Patent. The claims and the specification of the '213 Patent do not mention reassembly. Further, while I agree with Dr. Goodrich that the system disclosed in the ACNS Guide is "flexible," I do not agree that the methods disclosed in the ACNS Guide would be disfavored by a POSA because they are "computationally expensive." EX2004, ¶53. All systems that scan for malware, such as viruses, have to employ a large number of rules to keep up with the ever-growing number of attacks that have been seen over the years. Dr. Goodrich acknowledges that "the methods of the '213 Patent can protect a network with ***huge numbers*** of computationally inexpensive ***rules***…" EX2004, ¶53 (emphasis added). Dr. Goodrich's purported point of difference is that

he characterizes the prior art as "computationally expensive" whereas the '213 Patent method is "computationally inexpensive" in his opinion. I disagree. The processing power and memory needed to implement the application-layer packet-header filtering in the ACNS Guide would be similar to the processing power and memory needed to implement the methods claimed in the '213 Patent.

IV. CLAIM CONSTRUCTION

22. Paragraphs 104-123 of my original declaration provide my opinion on the proper construction of certain terms recited in the claims of the '213 Patent. The PTAB subsequently construed those terms in its Institution Decision. *See* Paper 8 at 7-15. Dr. Goodrich adopts the constructions of the terms "rule/rules," "security policy management server," "packet security gateway," and "packet transformation function" set out by the PTAB. EX2004, ¶59. I agree.

23. Packet – I also agree with Patent Owner's and Dr. Goodrich's construction that the term "packet" refers to a link layer (Layer 2) packet or a network layer (Layer 3) packet. *See* Paper 15 at 9-12; EX2004, ¶¶51, 54, 126; EX2009 at 46:10-47:11. I applied this construction of "packet" in my original declaration (EX1004), and I also apply it herein. Patent Owner and Dr. Goodrich are incorrect when they say that I applied a different construction of packet in my original declaration.

24. Dynamic Security Policy – Dr. Goodrich also tries to implicitly change the construction of "dynamic security policy," though he stops short of proposing a new construction. EX2004, ¶¶114-115. As I explained in my original declaration, it is my opinion that the term "dynamic security policy" should be construed 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." EX1004, ¶¶105-107. This construction was taken directly from the specification of the '213 Patent. EX1001, Col. 4:58-63. I acknowledge that this construction encompasses security policies with either static (i.e., manually updated) or non-static (i.e., automatically updated) rules, but the inventors chose to provide this explicit definition of the term in the '213 Patent. The PTAB acknowledged this fact and adopted this construction in its Institution Decision. Paper 8 at 7-9.

25. Dr. Goodrich implies that the term "dynamic security policy" should have a different construction. EX2004, ¶¶136-137. Dr. Goodrich states that "the word 'dynamic' in the term 'dynamic security policy' means that the SPM that stores the dynamic security policy and sends it to one or more PSGs can 'automatically create or alter one or more of such rules as new network addresses associated with malicious network traffic are determined.'" *Id.*, ¶115. I disagree. Dr. Goodrich's position contradicts the explicit definition of "dynamic security policy" found in

column 4, lines 58-63 of the ’213 Patent. Further, as the PTAB 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. It is my opinion that the proper construction of “dynamic security policy” should be the express construction stated in the ’213 Patent and adopted by the Board in the Institution Decision.

26. Packet-by-Packet – Separately, I note that Patent Owner didn’t seek a claim construction that would limit “packet-by-packet” to analysis of individual packets in isolation in either this proceeding or the ongoing litigation between Petitioner and Patent Owner. *See* Paper 8 at 7-15; EX1005-EX1007, EX2002. However, Dr. Goodrich implicitly seeks to narrow “packet-by-packet” to mean that a packet is viewed in isolation itself without reference to any other packet in a packet flow. A POSA would not view the term “packet-by-packet” so narrowly, particularly when it is to be given the broadest reasonable understanding of the term. I address Dr. Goodrich’s specific positions on “packet-by-packet” in the invalidity analysis provided in Paragraphs 59-60 and 67-70 below.

V. PRIOR ART TO THE ’213 PATENT

A. ACNS

27. I addressed the capabilities of ACNS in Paragraphs 146-147 of my original declaration, as well as in the analysis of the individual claim elements.

EX1004. Dr. Goodrich provides his description of ACNS in Paragraphs 62-76 of the Goodrich Declaration. EX2004. I disagree with Dr. Goodrich's discussion of ACNS for several reasons.

28. Dr. Goodrich first offers his opinion that he does "not believe that Cisco has established the date of when Ex. 1008 [the ACNS Guide] was published or first available to the public." EX2004, ¶62. It is my opinion the neither Dr. Goodrich nor I are qualified to provide an opinion on when the ACNS Guide was publicly available. Dr. Goodrich does not claim to have any personal knowledge about when the ACNS Guide was publicly available. Instead, Dr. Goodrich discusses deposition testimony of Eli Fuchs. *Id.*

29. I note that Mr. Fuchs submitted a declaration concerning the ACNS Guide in which Mr. Fuchs stated that the ACNS Guide was publicly available based on: the guide itself, certain "Release Notes" relating to the ACNS Guide, and Mr. Fuchs's knowledge of Cisco's policies for providing the ACNS Guide to customers. EX1012. I note that Dr. Goodrich does not address the information in the Fuchs Declaration. I also note that the deposition testimony of Mr. Fuchs quoted by Dr. Goodrich states that Mr. Fuchs conducted research on Google that identified that the "Cisco website had the documentation with the date associated with it." EX2004, ¶62. Further, Dr. Goodrich fails to cite portions of the deposition testimony of Mr. Fuchs where he explained that his Google search uncovered the ACNS Guide and

the Release Notes, and those documents are what corroborate the declaration statement from Mr. Fuchs that the ACNS Guide was publicly available before the priority date:

> Q. So what is your basis for your testimony that there is an update associated with Exhibit 12? Exhibit 8, excuse me.
>
> A. That there are dates associated with publishing on the website that I recall from the Google search about a year ago, both the documentation – primary documentation guides and release notes.
>
> Q. So the last sentence of the same paragraph, paragraph 9, says, "For example, release 5.5.1 was updated on March 20, 2008"; is that correct?
>
> A. It's what I – it's in my declaration, so I would say yes.
>
> Q. What is the basis for saying that?
>
> A. When I signed this declaration, I was able to Google search ***for the documentation and the release notes and those – and validate the dates that I was signing to***.
>
> * * *
>
> Q. Are there any documents that you're aware of other than the release notes that form your basis for your understanding that the ACNS Guide was –
>
> A. ***The basis for this declaration were user guides and release notes for ACNS***.

EX2021 at 34:3-36:14 (emphasis added).

30. Dr. Goodrich also cites a number of sections of the ACNS Guide stating that the ACNS software can be used to deliver requested content. EX2004, ¶¶64-

70. I agree that the "primary role" of the Cisco ACNS software is to "serve client requests for content." *See* EX1008 at 1-2. However, as I explained in my original declaration, the ACNS Guide also discloses that its Content Engines perform "security functions" that include intercepting traffic and enforcing policies within a network. EX1004, ¶152, citing EX1008 at 1-9 (discussing that the Content Engine may, for example, prevent viruses from spreading). Further, the Content Distribution Manager disclosed in the ACNS Guide may propagate rules to provide these security functions based on application-layer packet header information, such as a rule allowing or refusing packets with certain HTTP Request Methods. EX1004, ¶153, citing EX1008 at 8-23 – 8-24. The Board also correctly recognized that the ACNS Guide discloses that the ACNS software performs security functions. Paper 8 at 16-17, quoting EX1008 at 1-9. Indeed, Dr. Goodrich acknowledges in Paragraph 71 of his declaration that the ACNS Guide teaches that the ACNS software can be used for "system security." EX2004, ¶71, citing EX1008 at 1-9.

31. Dr. Goodrich also notes that the ACNS Guide states that the system can "authenticate users, e.g., by asking the client 'to provide a username and password so that it can consult an authentication, authorization, and accounting (AAA) server, and check[] whether the client is allowed to access the web.'" EX2004, ¶71. In addition, Dr. Goodrich states that the ACNS Guide explains that "ACNS 5.5 software ***relies on third-party software to implement content filtering.***" EX2004,

¶71, citing EX1008 at 1-10 (emphasis in original). However, I do not rely on either of these two statements in my analysis, and I do not think they are relevant to the teachings of the ACNS Guide as applied to the claims of the '213 Patent. With respect to the latter, Dr. Goodrich acknowledged during his deposition that any third-party software for content filtering could be integrated within the ACNS system, so it would be part of the functionality taught by the ACNS Guide. EX1026 at 47:3-8.

32. Dr. Goodrich incorrectly argues in Paragraphs 72-73 of his declaration that "Content Engines in ACNS are processing HTTP requests as completed messages, not on a packet-by-packet basis." EX2004, ¶72. Dr. Goodrich focuses on the fact that the ACNS Guide discusses "HTTP requests" and concludes from this that "ACNS must reassemble application-layer messages to authenticate HTTP requests or to log transactions between the Content Engines and their clients." *Id.*, ¶73. I disagree. A POSA would have understood from the ACNS Guide that the ACNS 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. 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. EX1026 at 27:20-29:8. Moreover, Claim 5 of the '213 Patent 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, a POSA would have understood that the system disclosed in the ACNS Guide necessarily operates on a packet-by-packet basis.

33. Further, even where an HTTP request spans multiple packets, a POSA would still understand the ACNS Guide to teach operating on packets on a packet-by-packet basis. As I explained in my original declaration, a POSA would have understood that 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). A POSA would have known that, when a request is made, the system 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. 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. The same would be true if the ACNS software was using ICAP instead of HTTP. *See* EX1008 at 19-1 – 19-5. Thus, the ACNS Guide teaches a POSA that the ACNS software looks at each packet on a packet-by-packet basis. Indeed, I note that the ACNS Guide does not mention the reassembly of packets in its discussion of the ACNS software.

34. Further, Dr. Goodrich acknowledges that the ACNS Guide discloses logging, but he asserts that "the logging in ACNS is occurring with respect to complete transactions, not on a packet-by-packet basis." EX2004, ¶¶74-75. Dr. Goodrich cites an example of a "transaction whose length (3436) in bytes is longer than the typical upper bound on the size of a packet excluding HTTP headers (which a POSA would understand to be 1500 bytes)." *Id.*, ¶75. I do not agree with Dr. Goodrich's conclusion. The ACNS Guide also discloses sample log entries that apply to a single packet, which demonstrates that the ACNS software is capable of logging on a packet-by-packet basis. Below is an example "squid" log entry (also shown in Paragraphs 162 and 181 of my original declaration) for a transaction whose length is 1,100 bytes. *See* EX1004, ¶162. This is smaller than the size of a packet excluding HTTP headers. Thus, this log entry is for a single packet, and it shows that that ACNS Guide teaches logging on a packet-by-packet basis.

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). Moreover, even in the case of the 3,436 byte transaction Dr. Goodrich discusses, the mere fact that the transaction may have spanned multiple packets does not rule out that packet-by-packet processing is performed. 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 aggregating or reassembling packets. A POSA would understand that packets need only be analyzed to determine properties of the transaction such as the length of the transaction and that this process can be done by examining each packet individually such that after the packet is analyzed it can forwarded, dropped, or logged as needed.

35. In addition, Dr. Goodrich states that I admitted that "ACNS does not log information about packets" in Paragraph 165 of my original declaration. EX2004, ¶76. That is not an accurate reflection of my opinion. My opinion was expressed as follows: "While the ACNS Guide does not explicitly teach logging only those packets identified by a rule within a dynamic policy, Kjendal does so. Specifically, Kjendal teaches a policy-based system for mirroring packets to monitoring devices or logging devices." EX1004, ¶165, citing EX1009, Col. 10:46-58. My opinion correctly reflected that ACNS does log information about packets.

B. Kjendal

36. I addressed the capabilities of Kjendal in Paragraph 148 of my original declaration, as well as in the analysis of the individual claim elements. EX1004. Dr. Goodrich provides his description of Kjendal in Paragraphs 77-81 of the Goodrich Declaration. EX2004. I agree with some of Dr. Goodrich's discussion of Kjendal. However, some parts of it require further elaboration. For instance, Dr. Goodrich

discusses the "network management control function 125 inside the Policy Server 103" in Kjendal, but he does not cite all of the relevant disclosure. EX2004, ¶80. Kjendal explains that the network management control function 125 "may be embodied in a single device of the network infrastructure 101 or it may be embodied in multiple devices, wherein different devices may contain one or more of the specific controllers described herein." EX1009, Col. 16:34-38.

37. Dr. Goodrich also asserts that "none of the figures in Kjendal that illustrate the example topologies for its embodiments (i.e., Figs. 1 and 7-10) show the dynamic mirroring function 300 installed in the firewall 118." EX2004, ¶81. This mischaracterizes the disclosure in Kjendal, which specifically teaches that firewall 118 can implement mirroring:

> The policy server 103 either has established one or more network policies, which may include one or more ***mirroring policies*** and/or rules for implementing mirroring policies, on the network entry device 105 or ***firewall 118*** for the purpose of allowing blocking or restricting the transfer of frames from the network entry device 105 to the core switching device 106 and/or access to resources of the network system.

EX1009, Col. 31:10-17 (emphasis added).

VI. MOTIVATION TO COMBINE ACNS, KJENDAL AND THE DIFFSERV SPECIFICAITON

38. I addressed the motivation to combine ACNS and Kjendal in Paragraphs 148, 166 and 198 of my original declaration. For example, I noted that "a POSA would very reasonably expect to include monitoring and logging features

from Kjendal to improve ACNS by allowing the system to send packets to other devices for analysis and logging, and such a POSA would expect such a combination to yield predictable results (packets would be mirrored to the monitoring device without problems)." EX1004, ¶148. The Board correctly found that there would have been a motivation to combine ACNS and Kjendal. Paper 8 at 31-32. The Board noted that Kjendal teaches that, rather than logging every HTTP packet, a system could log only packets that meet certain criteria. *Id.*

39. Dr. Goodrich argues that there is no motivation to combine ANCS and Kjendal. The primary basis for Dr. Goodrich's argument is that ACNS and Kjendal "teach fundamentally different techniques" because ACNS performs "transaction logging" while Kjendal performs "packet-mirroring." EX2004, ¶86; *see also id.*, ¶¶87-94. I disagree. A flaw in Dr. Goodrich's reasoning is that in many instances, an HTTP "transaction" (such as an HTTP GET or HTTP PUT method call) will be small enough that it can fit inside a ***single*** packet. Indeed, Dr. Goodrich admitted in his deposition that a POSA would understand that a transaction can fit inside a single packet. EX1026 at 27:20-29:8. Moreover, Claim 5 of the '213 Patent 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). Further, as discussed in Paragraph 34 above, Chapter 19 of the ACNS Guide discloses examples of "transaction logging" where

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. EX1008 at 19-1 – 19-2; EX2004, ¶75 (discussing the size of a packet). Thus, a POSA would understand that a transaction less than 1,500 bytes fits within a single Layer 3 and a single Layer 2 packet, and, in that situation, logging the information relating to a transaction is the same as logging the information relating to a packet. Indeed, the process of extracting the HTTP transaction from the Layer 3 packet (i.e., an IP datagram) would involve nothing more than stripping away the IP datagram headers and the TCP Segment headers to leave the HTTP transaction. Thus, the logging in ACNS is not "fundamentally different" from the packet-mirroring for the purpose of logging taught in Kjendal. Both operate on individual packets.

40. Moreover, even in the situation where a HTTP transaction spans multiple packets, there is no evidence that the logging in ACNS is fundamentally different the packet-mirroring in Kjendal. As I discussed in Paragraphs 17 and 33-34 above, when HTTP transactions span multiple packets, a POSA would understand that a system may analyze each packet to determine the properties of the transaction, such as the length of the transaction. 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. Thus, a POSA would have understood that the ACNS Guide discloses a system

which can analyze packets to create a log, and it is not "fundamentally different" than Kjendal.

41. Further, in discussing the operation of ACNS, Dr. Goodrich takes a sentence from page 36 of the Petition out of context. EX2004, ¶86. Contrary to Dr. Goodrich's analysis, Petitioner did not assert that ACNS would base an authentication error on "application-layer header information." *Id.* Instead, Petitioner explained, as did I in Paragraphs 163-165 of my original declaration, that it is not desirable for ACNS to log all packets because the number of log entries may overload a syslog server. EX1004. For this reason, ACNS teaches logging only HTTP authentication failures to reduce the number of log entries. *Id.*, ¶¶163-165. A POSA would understand from Kjendal that the problem created by logging all packets can also be addressed by selectively logging for other types of application-layer information. *See, e.g.*, EX1009, Cols. 10:46-58; 29:60-30:16. Thus, the fact that the ACNS Guide focuses on authentication errors, as Dr. Goodrich notes in Paragraph 88 of his declaration (EX2004), only strengthens the motivation to combine the ACNS Guide and Kjendal because Kjendal teaches other ways to selectively log and reduce the number of log entries sent to the syslog server.

42. Dr. Goodrich argues that "there is no motivation to combine ACNS and Kjendal [because] Kjendal teaches a technique for mirroring packets, based on multiple criteria, which is neither transaction-based nor logging (as in ACNS)."

EX2004, ¶¶89-90. I discussed why I disagree with the "transaction-based" portion of this sentence in Paragraphs 39-40 above. With respect to the claim that Kjendal does not disclose logging, I disagree. Dr. Goodrich is correct that Kjendal discloses the mirroring of packets, as noted by the portion of Kjendal that he cites from Col. 10, lines 1-17, but Kjendal also explains in Column 10 that the mirrored packets may be sent to a "network logger." EX1009, Col. 10:46-58. A POSA would understand the reference to a "network logger" to mean that one of the outcomes of the rule-based policies in Kjendal is that it can determine certain packets should be logged and send them to a logger to perform the logging functions. *See id.*, Col. 20:15-19. As such, Kjendal discloses logging, just like the ACNS Guide.

43. Dr. Goodrich implicitly admits that Kjendal discloses logging when he asserts that "any logging that [Kjendal] does occurs after and as a separate function from mirroring." EX2004, ¶91. I agree, but there is still a reason to combine the teachings of Kjendal with the disclosures of the ACNS Guide. Kjendal teaches rule-based policies that use application-layer header information to determine that certain packets should be logged. *See* EX1009, Col. 29:60-30:16. That teaching can be implemented in the ACNS Guide, irrespective of whether the logging in Kjendal occurs after mirroring.

44. Further, while Paragraph 91 of Dr. Goodrich's declaration is not entirely clear, a point that Dr. Goodrich seems to be implying is that the packet

mirroring in Kjendal (which I equate to the claimed "routing…to a monitoring device" in element [1.9]) has to be performed "in response to a logging action" for Kjendal to be relevant to the ACNS Guide. EX2004. I disagree. This is seeking to impose the claim limitations of the '213 Patent on the prior art references in an attempt to argue that their disclosures can't be combined. It is my understanding that this is not a correct analysis of how a motivation to combine is determined. Moreover, it is not a proper reading of the claims of the '213 Patent. The claims require "routing… to a monitoring device in response" to "the performing the packet transformation function." EX1001, Cols. 25:51-55, 27:31-35. However, the packet transformation function in the claims is defined in an open-ended way using the term "comprising," which means the packet transformation function can include more than just the "packet digest logging function." *Id.*, Cols. 25:20-23, 26:65-27:1. For instance, the packet transformation function can include a forwarding function, in addition to the packet digest logging function, and the routing (i.e., packet mirroring) can be as a result of the forwarding function, which it is in Kjendal.

45. Paragraph 92 of the Goodrich declaration repeats Dr. Goodrich's argument that Kjendal is different than the ACNS Guide because the ACNS Guide "logs transactions." EX2004. In response, I repeat my analysis in Paragraphs 39-40 above concerning the transaction logging in the ACNS Guide.

46. In addition, Dr. Goodrich incorrectly asserts that I am "using the '213 Patent as a guide or blueprint" to come up with the motivation to combine the teachings of Kjendal with the ACNS Guide. EX2004, ¶93. That is wrong. The ACNS Guide itself notes that logging too many things can overwhelm a syslog server; thus, it discloses the possibility of logging only authentication errors. EX1008 at 19-19 – 19-22. As the system disclosed in the ACNS Guide operates to maintain "system security" (*see id.* at 1-9), a POSA would understand that it would be useful to implement other types of rule-based monitoring for security threats or objectionable content, as disclosed in Kjendal. *See* EX1009, Col. 10:46-58, 10:23-33. Separately, as part of maintaining "system security," a POSA would understand the benefit of mirroring (i.e., routing) packets that may contain security threats or objectionable content to a monitoring device, as also taught in Kjendal. *Id.*

47. Dr. Goodrich also argues that "incorporating the teachings of Kjendal into ACNS would degrade the performance of ACNS while not improving the operating principle of ACNS." I disagree. I discussed how the disclosures of Kjendal can improve the operating performance of the system disclosed in the ACNS Guide in Paragraphs 38 and 41-43 above. Further, incorporating the disclosures of Kjendal into the ACNS system will not degrade its performance. Dr. Goodrich's basis for this is again his claim that ACNS performs "transaction logging" and there would be no reason to perform "both transaction logging and packet logging

simultaneously." However, as discussed in Paragraphs 39-40 above, a POSA would understand that the logging disclosed in the ACNS Guide can be based on packets, just like the logging in Kjendal. Thus, there would not be two separate steps of performing both "transaction logging" and "packet logging." Kjendal teaches how to improve, not degrade, the logging disclosed in the ACNS Guide by using rule-based logging.

48. With respect to the combination of the ACNS Guide, Kjendal and the Diffserv Specification, I addressed the motivation to combine them in Paragraphs 237-240, 247-249 and 256 of my original declaration. EX1004. Specifically, the ACNS Guide teaches the use of differentiated services and the DSCP field, while the Diffserv Specification provides specifics on the implementation and use of differentiated services and the DSCP field. Kjendal also teaches use of mirroring with network services including QoS. EX1009, Col. 2:14-16, 3:1-7. The Board agreed. Paper 8 at 38-39.

49. Dr. Goodrich argues that I have not provided a reason "why a POSA would be motivated to log information about packets identified by a DSCP selector." EX2004, ¶95. I disagree. As an initial matter, I note that the '213 Patent provides no explanation of why a POSA would want to log packets identified by the DSCP selector. Column 10, lines 23-37 is the only discussion of the DSCP in the specification of the '213 Patent. EX1001. However, that discussion states that "one

or more rules contained within the dynamic security policy may include an arbitrary selector which may correspond to one or more parameters or fields associated with a packet." *Id.*, Col. 10:23-26. It identifies the DSCP as one of those "arbitrary selectors," but it does not explain why a POSA would want to log packets with the DSCP selector. *Id.*

50. By contrast, my declaration explains that the classifier rules using the DSCP disclosed in the Diffserv Specification can be used as packet identification criteria for packet filtering, similar to the other packet filtering criteria already disclosed in the ACNS Guide, such as whether or not an HTTP request method is supported. EX1004, ¶256. Indeed, a POSA would have understood that, where a system is getting overwhelmed with traffic that slows system operation (such as can occur in a DoS or DDoS attack), the DSCP field can be used to provide a different quality of service to different packets in order to alleviate and manage the effects of the attack. For instance, packets that may be associated with the malicious traffic would be given a lower priority of service using the DSCP such that they have less of an effect on the system. A POSA also would have known that malicious packets given this lower priority of service could be logged for later analysis by an administrator or someone else trying to understand an attack. Alternatively, packets that are not suspected to be associated with malicious traffic can be given a higher quality of service so that they continue to be delivered even when the system is

stressed by an attack. This helps provide a remedy to the attack, and it is the reason that a POSA would understand to implement the DSCP as a packet identification criteria as part of a rule in a dynamic security policy.

51. Moreover, the fact that the ACNS Guide already uses the DSCP as part of its content delivery provides further motivation to use the DSCP in this security context because a POSA knows that it can be an effective identifier of packets. Thus, I do not agree with Dr. Goodrich's assertion that there is no reason to view "DSCP fields as an indication of a possible security threat or as an attack remedy" because the ACNS Guide views the DSCP as a "beneficial feature." EX2004, ¶¶98-99. A POSA would readily understand that the DSCP could be used for multiple reasons. As Dr. Goodrich and I agree, the ACNS Guide discloses that it can be used as part of content delivery. However, a POSA would also understand that the DSCP field can be used to remedy the effects of an attack as discussed above. Indeed, the two features work hand-in-hand. The Content Engines are in-line devices that can prioritize the delivery of content based on the priority of service indicated by the DSCP, and the priority can be determined, in part, based on whether the network traffic is suspected to be malicious. The Diffserv Specification teaches how to implement the DSCP for these purposes.

52. Dr. Goodrich acknowledged during his deposition that the DSCP can be used as discussed above as part of a dynamic security policy to remedy an attack.

EX1026 at 11:25-12:20. However, he claims that this would not have been known in the prior art and was discovered by the inventors of the '213 Patent. *Id.* at 12:21-13:14. This is contradicted by the '213 Patent itself, which describes the DSCP as an "arbitrary selector" and provides no explanation of why it should be used in a dynamic security policy or logged. EX1001, Col. 10:23-26. The fact is that this use of a DSCP as an identifier of packets in a dynamic security policy would have been known to a POSA before the priority date of the '213 Patent, and the specifics of implementing it were taught by the Diffserv Specification, which explains why the '213 Patent does not explain the use of a DSCP as an identifier of packets in detail.

53. Dr. Goodrich also asserts there is no motivation to combine the ACNS Guide and the Diffserv Specification by repeating his argument that the ACNS Guide teaches transaction logging that would not be related to operations on packets. EX2004, ¶¶96-97. This is incorrect for the reasons I explained in Paragraphs 39-40 above concerning the operation of the transaction logging. For instance, in many situations, a transaction will fit within a single packet, and thus the transaction logging taught by the ACNS Guide is logging a portion of the single packet that summarizes the transaction. Further, the ACNS Guide teaches logging a summary of a transaction and doesn't require logging of the entire packet. Thus, the use of the DSCP as packet identification criteria in a rule within a dynamic security policy in the ACNS system would not require "double the storage" of the ACNS system.

54. As such, I maintain my opinion that there is a motivation to combine the ACNS Guide, Kjendal and the Diffserv Specification.

VII. GROUNDS OF INVALIDITY

55. I remain of the opinion that a POSA would understand that claims 1-9 of the ’213 Patent are rendered obvious by the ACNS Guide in light of Kjendal for the reasons stated in my opening declaration. EX1004. These references may be further combined with the Diffserv Specification to demonstrate the obviousness of claims 10-16. *Id.* Dr. Goodrich asserts that the prior art identified for Ground 1 and Ground 2 do not render the claims of the ’213 Patent obvious. I disagree, and I set forth below my reply to Dr. Goodrich’s discussion of the invalidity analysis.

A. ACNS Teaches Element [1.1] of Claim 1.

56. Element [1.1] of Claim 1 recites “[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….” EX1001, Col. 25:14-20. My opinion that the ACNS Guide teaches element [1.1] is set out in Paragraphs 149-159 of my original declaration. EX1004. The Board specifically considered element [1.1] in the Institution Decision and found that element is taught by the combination of the ACNS Guide and Kjendal. Paper 8 at 19-23. Yet, Dr. Goodrich argues in Paragraphs 104-115 of his

declaration that neither the ACNS Guide nor Kjendal teach element [1.1] in. EX2004.

57. Dr. Goodrich first argues that "the Content Engine [in the ACNS Guide] is not the 'packet security gateway' because the Content Engine ***does not inspect packets*** and ***is not concerned with the security*** when it processes requests and responses from clients." EX2004, ¶106 (emphasis in original). I disagree. With respect to the assertion that the Content Engine disclosed in the ACNS Guide is not concerned with security, the Board already heard and rejected this position. Specifically, the Board found "that 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, citing EX1008 at 1-9. The ACNS Guide also provides an example that its system is designed to make sure that "[v]iruses such as 'Code Red' are prevented from being propagated inside the corporate network." EX1008 at 1-9. Given these statements in the ACNS Guide, I agree with the Board that the system disclosed in the ACNS Guide is concerned with security, and the Content Engine functions as a packet security gateway.

58. The testimony of Mr. Eli Fuchs cited in Paragraph 106 of Dr. Goodrich's declaration does not change my opinion that the ACNS Guide discloses that its system performs security analysis. Mr. Fuchs provided a supplemental declaration after his deposition in which he explained that, while the ACNS Guide

states that the primary purpose of ACNS is content delivery, the above-referenced statements from the ACNS Guide disclose that it also is concerned with security. EX1027). Given that the ACNS Guide is more than ten years old, it is not surprising that Mr. Fuchs did not initially remember every function described in the 900-page document. Moreover, I note that Mr. Fuchs testified that, as a "Senior Engineering Manager," he was a project manager who would have known about the availability of the ACNS Guide to customers. EX2021 at 10:6-22, 21:1-17.

59. With respect to the inspection of packets, as discussed in Paragraphs 32-33 and 39-40 above, the Content Engine inspects individual packets and thus constitutes a packet security gateway. While the ACNS Guide refers to processing "HTTP requests," a POSA would understand that, 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 and as Claims 5 and 7 of the '213 Patent acknowledge. EX1026 at 27:20-29:8; EX1001, Col. 26:12-13, 26:29-30. Where an HTTP request fits inside a single packet, a POSA would have understood that the Content Engine necessarily inspects those individual packets on a "packet-by-packet" basis even under Dr. Goodrich's excessively narrow interpretation of that term.

60. Further, where an HTTP request spans multiple packets, a POSA would still have understood that the Content Engine inspects those individual packets on a

packet-by-packet basis. A POSA would have known that, when a HTTP request is made, the system can identify that the request is HTTP from the request method information in the first packet. EX1004, ¶155, citing EX1008 at 8-23 – 8-24. 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. The same would be true if the ACNS software was using ICAP instead of HTTP. *See* EX1008 at 19-1 – 19-5. Thus, the ACNS Guide teaches a POSA that the ACNS software looks at each packet on a packet-by-packet basis. Thus, regardless of Dr. Fuchs's testimony, it remains my opinion based on the written disclosure of the ACNS Guide that the Content Engine discussed in the ACNS Guide operates as a packet security gateway that inspects individual packets and is concerned with security.

61. In addition, Dr. Goodrich states that "Dr. Jeffay agrees at least that the Content Engine is not able to inspect the payload of a packet for malware." EX2004, ¶107. My actual testimony was different in that I testified that "I don't think there are any disclosures in ACNS of the functions that you would need to be able to perform in order to do things like search payloads for malware." EX2020 at 69:10-16. In any event, I do not believe that this is relevant to whether the Content Engine acts as the claimed packet security gateway because my opinion is based on the fact that the Content Engine looks to a ***packet header*** to determine whether a packet is

an HTTP packet using a supported method. I did not provide an opinion that the Content Engine is inspecting the payload of packets.

62. Dr. Goodrich also argues that "ACNS does not disclose that the Content Distribution Manager provisions any security policy to the Content Engines." EX2004, ¶¶108-110. Dr. Goodrich's position is that "ACNS merely discloses that a user may add or otherwise modify a policy already existing on a Content Engine." *Id.* Patent Owner already presented this argument to the Board, and the Board rejected it. Paper 8 at 20-22. The Board first pointed to Chapter 2 of ACNS, which discusses the initial configuration of the ACNS system. *Id.* at 21. The Board acknowledged that "all ACNS devices are factory shipped as Content Engines," and it noted that "[t]he administrator can then use the Quick Start tool to 'select a set of content engines and provision them for caching, streaming, and pre-positioning[…] using a small subset of options,' with advanced option[s] available from the main user interface." *Id.*, quoting EX1008 at 2-12 – 2-13. The Board further explained that the Content Distribution Manager Graphical User Interface ("GUI") is used by the administrator to access the Content Distribution Manager and configure the Content Engine properly. Paper 8 at 21. The Board invoked the appropriate example of using the Content Distribution Manager to configure a Content Engine to work with a "WCCP enabled router." *Id.* at 21-22.

63. The Board specifically addressed the argument now raised by Dr. Goodrich that the Content Distribution Manager in ACNS "merely discloses that a user may add or otherwise modify a policy already existing on a Content Engine." EX2004, ¶108. The Board explained that the Content Distribution Manager configures the performance of a Content Engine, regardless of the default settings:

> That some methods are supported by default ***does not change the fact that ACNS teaches the administrator configures an active Content Engine*** either initially or at a later time by clicking the 'Edit' icon next to the name of the corresponding Content Engine on the CDM GUI to add other HTTP request methods to the selected Content Engine. [EX1008] at 8-23-24. Thus, the administrator customizes the rules implemented in the Content Engines. To the extent an administrator manipulates settings, such as port numbers and HTTP request methods accepted by the Content Engine, such manipulation is the result of externalities, such as HTTP standards. ***It is the administrator who, through the Content Distribution Manager, configures the performance of a Content Engine in the context of such externalities***.

Paper 8 at 22 (emphasis added). I agree with the Board that a POSA would understand that the modification of the Content Engine through the Content Distribution Manager constitutes the Content Engine receiving a dynamic security policy from the Content Distribution Manager. For example, a POSA would consider the addition of any new HTTP request method to the list of those supported by the ACNS system to be the provision of a new dynamic security policy from the Content Distribution Manager to the Content Engine. Contrary to Dr. Goodrich's statements in Paragraph 110 of his declaration (EX1004), this is not the administrator updating "an already implemented policy on a Content Engine," but it

is instead providing a new policy containing a rule (a newly supported HTTP request method) and a packet transformation function (the understanding to forward packets relating to the supported method).

64. Dr. Goodrich asserts that the "ACNS' command-line interface fails [to teach element [1.1]] for the same reasons" – modifying a setting or rule already on the Content Engine. EX2004, ¶¶111-112. I disagree for the same reasons. Namely, the command-line interface can be used by an administrator to add new HTTP request methods to the list of those supported by the ACNS system, which a POSA would understand to be the provision of a new dynamic security policy to the Content Engine. EX1008 at C-6.

65. Finally, Dr. Goodrich argues that the ACNS Guide does not teach element [1.1] because the security policy disclosed in the ACNS Guide is "static." EX2004, ¶¶114-115. Dr. Goodrich seeks to change the construction of dynamic security policy to require that the policy be able to "automatically create or alter one or more of such rules as new network addresses associated with malicious traffic are determined." *Id.* at ¶115. I disagree. As discussed in Paragraphs 24-25 above, the term "dynamic security policy" should be given the express definition set out in the '213 Patent, which covers either static or non-static rules. The rules disclosed in the ACNS Guide qualify as a dynamic security policy under the proper construction for the reasons discussed above and in Paragraphs 149-159 of my original declaration.

Moreover, as noted by the Board, the disclosures in the ACNS Guide 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.

B. The Combination of ACNS and Kjendal Each Teach Element [1.2].

66. Element [1.2] of Claim 1 recites "…and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information." EX1001, Col. 25:20-23. My opinion that the combination of the ACNS Guide and Kjendal teaches element [1.2] is set out in Paragraphs 160-167 of my original declaration. EX1004. In its Institution Decision, the Board agreed that the combination of the ACNS Guide and Kjendal teaches element [1.2]. Paper 8 at 23-25. The ACNS Guide teaches the logging of packets, where either all packets are logged or packets relating to authentication failures are logged. *See* EX1008 at 19-1 – 19-22. While the ACNS Guide does not explicitly teach logging packets based on application-layer packet-header information, Kjendal does teach that to a POSA. EX1004, ¶165. As the Board noted, Petitioner and I cite Kjendal for its disclosure of a system where application-layer packet-header information is used to determine what should be logged. Paper 8 at 23, 25; Paper 1 at 31; EX1004, ¶¶164-167. A POSA would apply

the teaching of Kjendal that other types of data could be logged to the logging functions disclosed in the ACNS Guide.

67. Dr. Goodrich sets out his opinion that neither the ACNS Guide nor Kjendal teach element [1.2] in Paragraphs 116-124 of his declaration. Dr. Goodrich first repeats his argument that the ACNS Guide discloses "transaction logging and does not identify and log packets on a packet-by-packet basis." EX2004, ¶¶117-118. I disagree for the reasons discussed in Paragraphs 32-33 and 39-40 above. A POSA would have understood that an HTTP "transaction" (such as an HTTP GET or HTTP PUT method call) often can fit inside a ***single*** packet. Dr. Goodrich admitted this in his deposition. EX1026 at 27:20-29:8. Further, Claim 5 of the '213 Patent 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). In addition, Chapter 19 of the ACNS Guide discloses examples of "transaction logging" where 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. EX1008 at 19-1 – 19-2; EX2004, ¶75 (discussing the size of a packet). For example, the below entry from page 19-1 of the ACNS Guide shows a Squid log entry with a size of 1,100 bytes (shown in highlight) in the transaction, which a POSA would have

understood to mean that the transaction fits within a single Layer 3 packet and a single Layer 2 packet:

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. Dr. Goodrich argued in his deposition that the "-" in this log entry and the statement on page 19-2 that "this field always contains a '-' (dash) if no user information is available" means that the log entry cannot relate to a packet. EX1026 at 52:2-54:8. I do not agree, as nothing about that information prevents the log entry from reflecting information about a logged packet.

68. Further, page 19-2 of the ACNS Guide shows an example log entry in Apache format. EX1008. This log entry is for a transaction with a size of 632 bytes. Again, a POSA would have understood that to mean the transaction fits within a single Layer 3 and a single Layer 2 packet.

172.16.100.152 - - [Wed Jan 30 15:26:26 2002]
"GET/http://www.cisco.com/images/homepage/support.gif HTTP/1.0" 200 632

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

Dr. Goodrich argued in his deposition that the date and time information about the log entry means it cannot relate to a packet. EX1026 at 55:7-18. That is wrong, as the date and time information can simply be information associated with a packet that forms part of a log entry about the packet.

69. Given that a POSA would understand that a transaction can fit within a single packet, a POSA would have understood that the transaction logging disclosed in Chapter 19 of the ACNS Guide teaches the claimed packet digest logging function. In the situation where an HTTP transaction fits within a packet, logging the information relating to a transaction is the same as logging the information relating to a packet. Indeed, the process of extracting the HTTP transaction from the Layer 3 packet (i.e., an IP datagram) would involve nothing more than stripping away the IP datagram headers and the TCP Segment headers to leave the HTTP transaction.

70. Moreover, even in the situation where a HTTP transaction spans multiple packets, a POSA would still understand the ACNS Guide to disclose a packet digest logging function. As I discussed in Paragraphs 34 and 40 above, when HTTP transactions span multiple packets, a POSA would understand that a system such as ACNS can still analyze packets on a packet-by-packet basis to determine the properties of the transaction, such as the length of the transaction. 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. Thus, even in the case of the 3,436 byte transaction Dr. Goodrich discusses (*see* EX2004, ¶118), the mere fact that the transaction may have spanned multiple packets does not prevent a packet digest logging function

from being performed. A POSA would have understood that the log entry is generated by analyzing each of the packets individually to determine properties of the transaction and then creating a packet digest based on the information from the different packets. Thus, a POSA would have understood that the ACNS Guide discloses a system which can analyze packets to create a log.

71. Dr. Goodrich next argues that the ACNS Guide does not teach logging packets having the specified application-layer packet-header information. EX2004, ¶¶119-120. Dr. Goodrich argues that the ACNS Guide discloses logging either "**every** HTTP request or only those HTTP requests for which user **authentication** had failed." *Id.*, ¶119. I agree, but this misunderstands the combined teachings of the ACNS Guide and Kjendal. As the Board noted in its Institution Decision, I (and Petitioner) cite Kjendal for its disclosure of a system where application-layer packet-header information is used to determine what should be logged. Paper 8 at 23, 25; Paper 1 at 31; EX1004, ¶¶164-167. The teachings of Kjendal are combined with the disclosure in the ACNS Guide of creating the log, and the combination teaches element [1.2].

72. With respect to Kjendal, Dr. Goodrich acknowledges that "one use of its technology is to mirror copies of packets to a network logger." EX2004, ¶121. However, he argues that "mirroring a packet is **not** a packet digest logging function" because "any logging it does occurs **after and as a separate function from**

mirroring." *Id.* (emphasis in original for both). This, again, misunderstands how Kjendal relates to element [1.2]. Kjendal teaches a POSA that application-layer packet-header information is used to determine which packets to log. EX1009, Col. 10:46-58, 29:60-30:16. This teaching, in combination with the logging functionality disclosed in the ACNS Guide, renders element [1.2] obvious. EX1004, ¶¶165-167. It is irrelevant that the logging in Kjendal is a separate function performed after mirroring. The mirroring is an intermediate step of delivering packets that have been identified as having certain application-layer packet-header information to a network logger to be logged. *Id.* But that intermediate step does not change the fact that Kjendal teaches logging based on packets identified as having certain application-layer packet-header information.

73. In addition, Dr. Goodrich asserts that the "network logger" in Kjendal does not perform the claimed packet digest logging function because Kjendal does not disclose that the network logger performs the steps of "identifying a subset of information," "generating… a record comprising the subset of information," and "reformatting… the subset of information." EX2004, ¶¶122-123. Again, I rely on the combination of the ACNS Guide and Kjendal, and not Kjendal by itself, to disclose the packet digest logging function. As I explained in Paragraphs 179-191 of my original declaration and discuss further in Paragraphs 82-86 below, it is my opinion that the ACNS Guide discloses the "identifying," "generating" and

"reformatting" steps required by the packet digest logging function. Thus, it is irrelevant that the network logger in Kjendal is not disclosed as performing these steps.

C. ACNS teaches Element [1.4].

74. Element [1.4] of Claim 1 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." EX1001, Col. 25:27-31. My opinion that the ACNS Guide teaches element [1.4] is set out in Paragraphs 172-175 of my original declaration. EX1004. The Board accepted this position in the Institution Decision. Paper 8 at 26-27. Dr. Goodrich sets out his opinion that the ACNS Guide does not teach element [1.4] in Paragraphs 125-130 of his declaration. EX2004.

75. As an initial matter, it appears that Dr. Goodrich identifies the wrong claim wording in Paragraph 125 of his declaration, as he cites the same wording that he also identifies as element [1.6] in Paragraph 131 of his declaration. For purposes of my reply, I will assume this was a typographical error, and Dr. Goodrich's analysis of element [1.4] refers to the same element [1.4] as my original declaration.

76. Further, I agree with Dr. Goodrich "that the term 'packet' refers to a link-layer (L2) or network-layer (L3) packet based on the OSI model," as I stated as

part of my reply on claim construction in Paragraph 23 above. *See* EX2004, ¶126. The analysis is my original declaration and this declaration applies that understanding of the term "packet."

77. However, Dr. Goodrich asserts that the ACNS Guide "does not teach identifying application-layer packet-header information in L2 or L3 packets." EX2004, ¶¶127-128. Dr. Goodrich argues that the system disclosed in the ACNS Guide must "reassemble the payloads 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." *Id.* In other words, Dr. Goodrich believes the ACNS Guide does not teach identifying packets containing application-layer packet-header information on a "packet-by-packet basis." *Id.* That is wrong. Indeed, the ACNS Guide never mentions the words "reassemble" or "reassembly," as Dr. Goodrich admitted during his deposition. EX1026 at 42:2-13, 43:12-16, 52:2-7 and 57:7-23.

78. Dr. Goodrich's analysis focuses on the fact that the ACNS Guide discusses "HTTP requests" and concludes from this that "ACNS must reassemble the L2 and/or L3 packets received by the Content Engine to identify the request method." EX2004, ¶128. I disagree. As discussed in Paragraphs 32-33 and 39-40 above, a POSA would have understood from the ACNS Guide that the ACNS 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. For example, in many instances, an HTTP request (such as a 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. EX1026 at 27:20-29:8; *see also* EX1001, Col. 26:12-13, 26:29-30 (Claims 5 and 7 reciting that a HTTP GET or a HTTP PUT method call can be found in "one or more packets"). Where an HTTP request fits inside a single packet, a POSA would have understood that the system disclosed in the ACNS Guide necessarily identifies packets containing the application-layer packet-header information (i.e., the request method) on a packet-by-packet basis.

79. Further, even where an HTTP request spans multiple packets, a POSA would have understood that the ACNS Guide teaches identifying packets containing the application-layer packet header information on a packet-by-packet basis. A POSA would have understood that 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 which will appear in the first packet of the request. EX1004, ¶155, citing HTTP 1.1 Specification (EX1010). A POSA would have known that, when a request is made, the system 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. 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.

As such, the ACNS Guide teaches a POSA that its system can identify packets containing a HTTP request method on a packet-by-packet basis.

80. I note that this teaching from the ACNS Guide (and the HTTP 1.1 Specification) is similar to the structure claimed in dependent Claims 4, 5 and 7 of the '213 Patent. *See* EX1001, Col. 26:4-19, 26:29-36. For example, Claim 5 recites that "one or ***more HTTP packets*** comprise an HTTP GET method call" and that "the one or more packets comprising the application-layer packet-header information are ***amongst*** the one or ***more HTTP packets***." *Id.* at Col. 26:12-19 (emphasis added). In other words, Claim 5 contemplates that an HTTP request may be contained in multiple packets, and, where the request is contained in multiple packets, the packets containing the application-layer packet-header information can be identified on a packet-by-packet basis even though they are "amongst the one or more HTTP packets." Dr. Goodrich asserts that the '213 Patent can perform this analysis on a packet-by-packet basis, without reassembly. *See* EX2004, ¶¶51-52. A POSA would understand the same is true of the system disclosed in the ACNS Guide.

81. The same would be true if the ACNS software was using ICAP instead of HTTP. *See* EX1008 at 16-1, 16-15 – 16-25; EX1004, ¶174. Dr. Goodrich does not seriously challenge this analysis. See EX2004, ¶129. Dr. Goodrich notes only that "the Content Engines in ACNS are concerned with content management" and are not "concerned with applying rules to individual packets." This is incorrect for

the reasons I have explained in Paragraphs 30-35 above, and the same logic applies in the ICAP context.

D. ACNS Teaches Element [1.6].

82. Element [1.6] of Claim 1 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." EX1001, Col. 25:38-41. My opinion that the ACNS Guide teaches element [1.6] is set out in Paragraphs 179-181 of my original declaration. EX1004. The Board accepted this position in the Institution Decision. Paper 8 at 28. Dr. Goodrich argues that the ACNS Guide does not teach element [1.6] in Paragraphs 131-136 of his declaration. EX2004. I disagree.

83. Dr. Goodrich asserts that the squid log entry that I cited in Paragraph 181 of my declaration is a "transaction log" and "not a log for an individual packet." EX2004, ¶¶132-133. He does not provide the basis for his opinion about this squid log entry. I disagree with his opinion because the length of the transaction is shown in the log entry to be 1,100 bytes, which Dr. Goodrich acknowledges is smaller than the size of a single packet. EX1008 at 19-1; EX1026 at 49:3-17. Thus, this transaction will fit within a single packet. As such, a POSA would understand that a log entry about the transaction is the same as a log about the packet. Further, Dr. Goodrich admits that logging the byte size of the transaction constitutes one type of

the claimed "subset of information." EX2004, ¶134. Thus, this squid log entry is an example in the ACNS Guide of a packet digest logging function that identifies a subset of information about a packet containing application-layer packet-header information (e.g., the "GET" request method).

84. Further, even in the case of the 3,436 byte transaction that Dr. Goodrich discusses (*see* EX2004, ¶134), the mere fact that the transaction may have spanned multiple packets does not prevent a packet digest logging function from being performed. A POSA would have understood that the log entry is generated by analyzing each of the packets of the transaction individually, on a packet-by-packet basis, to determine properties of the transaction and then creating a packet digest based on the information from the different packets. Thus, a POSA would have understood that the ACNS Guide discloses a system which can analyze packets to create a packet digest or log.

85. In addition, Dr. Goodrich argues that the system disclosed in the ACNS Guide "lacks the ability to log packet information with the level of granularity and specificity enabled by the techniques claimed in the '213 Patent." EX2004, ¶135. This assertion is based on Dr. Goodrich's earlier arguments that the ACNS Guide does not perform packet logging, and it is incorrect for the reasons I provided in Paragraphs 34-35 and 39-41 above. A POSA would have understood that the system disclosed in the ACNS Guide is able to log information about individual packets and

it allows for specific, granular information to be placed in the logs, as disclosed in examples on pages 19-1 – 19-22 of the ACNS Guide. In any event, the claims of the '213 Patent do not recite any particular level of "granularity or specificity" beyond the packet-by-packet logging also disclosed and taught in the prior art, and thus this argument is not commensurate with the scope of the claims.

E. The Combination of ACNS and Kjendal Teaches Element [1.7].

86. Element [1.7] of Claim 1 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." EX1001, Col. 25:42-45. My opinion that the combination of the ACNS Guide and Kjendal teaches element [1.7] is set out in Paragraphs 182-187 of my original declaration. EX1004. Dr. Goodrich sets out his opinion that the ACNS Guide does not teach element [1.7] in Paragraphs 137-139 of his declaration. EX2004. Dr. Goodrich repeats his earlier argument that "ACNS does not perform logging at the granular level of logging information about each packet." EX2004, ¶138. Dr. Goodrich asserts that the ACNS Guide instead discloses "transaction logging." *Id.* I disagree because a POSA would understand that the ACNS Guide teaches logging information about each packet, and thus generating a record for each packet, for the reasons discussed in Paragraphs 34-35 and 39-41 above.

F. Kjendal Teaches Element [1.9] of Claim 1

87. Element [1.9] of Claim 1 recites "and 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." EX1001, Col. 25:51-55. My opinion that Kjendal teaches element [1.9] is set out in Paragraphs 192-198 of my original declaration. EX1004. In response to the Petition, Patent Owner asserted a number of arguments that Kjendal does not teach this claim limitation in its Patent Owner Preliminary Response. Paper 7 at 28-29. The Board considered and rejected those arguments in finding that Kjendal does teach element [1.9] in the Institution Decision. Paper 8 at 29-31.

88. Dr. Goodrich now raises the new argument that Kjendal does not teach routing packets to a monitoring device "in response to applying the packet transformation function," as required by element [1.9]. EX2004, ¶188. With respect to this argument, the Board's finding in IPR2018-01386, another *inter partes* review proceeding relating to the '213 Patent, 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). The Board further explained as follows:

> Thus, Kjendal recognizes the inefficiencies of mirroring all packets and mirrors only selected packets. Of course, Kjendal must examine all packets in order to determine which packets to mirror. Even if Kapoor fails to teach routing packets to a monitoring device in response to performing the transformation function, Kjendal's selective mirroring suggests examining packets and ***executing a transformation function that forwards packets and mirrors only certain packets depending on their characteristics***.

Id. (emphasis added). In other words, the Board in IPR2018-01386 explained that Kjendal teaches identifying packets that meet certain criteria, performing the packet transformation function of forwarding packets, and mirroring (i.e., routing) the forwarded packets that meet the criteria to a monitoring device. I agree with this analysis of Kjendal and that this meets the limitations of element [1.9].

G. Claims 2-9 are Obvious

89. Claims 2-9 of the '213 Patent are rendered obvious in light of the combination of ACNS and Kjendal for the reasons discussed in Paragraphs 199-234 of my original declaration (EX1004) and above in Paragraphs 56-88. Dr. Goodrich asserts that Claims 2-9 are not obvious for the reasons that he provides for Claim 1. EX2004, ¶190. I disagree for the reasons that I stated above for Claim 1.

H. The Combination of ACNS, Kjendal and the DiffServ Specification Teaches All Elements of Claim 10.

90. My opinion that the combination of ACNS, Kjendal and the DiffServ Specification teaches all elements of Claim 10 of the '213 Patent is set out in Paragraphs 241-281 of my original declaration. EX1004. Dr. Goodrich begins his

opinions on Claim 10 by repeating his earlier assertions with respect to Claim 1. EX2004, ¶¶145-150, 154-157. Therefore, I incorporate by reference my analysis of Claim 1 set forth in Paragraphs 56-88 above.

91. The only element of Claim 10 that Dr. Goodrich discusses in detail is element [10.3], which recites "wherein the packet-identification criteria comprises a Differentiated Code Point (DSCP) selector." EX2004, ¶¶151-153. Dr. Goodrich appears to acknowledge that the disclosures in ACNS and the DiffServ Specification would have taught the use of DSCP data. *Id.*, ¶151. However, Dr. Goodrich asserts that the DSCP data 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." *Id.* Specifically, Dr. Goodrich argues that the DSCP data is used in the ACNS Guide as part of content delivery and "ACNS does not express any benefit to using DSCP to perform security services." *Id.*, ¶152. I disagree.

92. The ACNS Guide explains that "you can ***configure Content Engines,*** Content Routers, and Content Distribution Managers for Type of Service (ToS) or ***differentiated services code point (DSCP)*** either through the CLI [or] through the Content Distribution Manager GUI." EX1008 at 10-9 (emphasis added). It further states, "The differentiated services architecture is based on a simple model where ***traffic entering a network is classified and possibly conditioned at the boundaries of the network***. The class of traffic is then ***identified with a differentiated services***

(DS) code point or bit marking the IP header." *Id.* (emphasis added). A POSA would understand from these disclosures that packets are classified first and then marked with a differentiated services code point and that Content Engines in the ACNS system are configured to use the DSCP as a criteria of policies to identify incoming packets. Further, the ACNS Guide emphasizes that 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 viruses or other malicious network traffic, and to take action on such packets.

I. Claims 11-16 are Obvious

93. Claims 11-16 of the '213 Patent are rendered obvious in light of the combination of ACNS, Kjendal and the DiffServ Specification for the reasons discussed in Paragraphs 282-300 of my original declaration (EX1004) and above in Paragraphs 90-92. Dr. Goodrich asserts that Claims 11-16 are not obvious for the reasons that he provides for Claim 10. EX2004, ¶158. I disagree for the reasons that I stated above for Claim 10.

VIII. SECONDARY CONSIDERATIONS/OBJECTIVE INDICIA OF NONOBVIOUSNESS

94. Dr. Goodrich discusses purported "objective indicia of nonobviousness" in Paragraphs 159-170 of the Goodrich Declaration. As stated in my original declaration, I understand that such objective indicia can support the non-obviousness of an invention. EX1004, ¶17. I further understand that such objective indicia can include long-felt but unresolved need, failure of others and industry praise, among other things. *Id.* I further understand that in order for objective indicia of nonobviousness to be applicable, the indicia must have some sort of nexus to the subject matter in a patent claim that was not known in the art. *Id.*

A. The Subject Matter Claimed in The '213 Patent Did Not Fulfill a Long-Felt Need That Others Failed to Solve.

95. Dr. Goodrich argues that "[t]he '213 Patent satisfied a long-felt need in the industry that others had failed to solve." EX2004, ¶159. I disagree for several reasons. First, Dr. Goodrich has not established any nexus between the subject matter in the claims of the '213 Patent and the purported long-felt need that Dr. Goodrich asserts was satisfied. The patent itself cannot fulfill the need, so Dr. Goodrich must be talking about products of Patent Owner that supposedly fulfilled the need. Dr. Goodrich discusses two products of Patent Owner in his declaration: (1) a Threat Intelligence Gateway ("TIG"), or RuleGATE and (2) a QuickThreat Gateway. *See, e.g.*, EX2004, ¶¶161-162, 164-165, 167-168. Dr. Goodrich,

however, does not explain whether either of these products embody the claims of the '213 Patent. For example, he does not explain whether or how either of these products perform the claimed "packet digest logging function" or the claimed "routing" of packets "to a monitoring device." Thus, Dr. Goodrich does not identify any technology that embodies the claims of the '213 Patent that purportedly solved a long-felt need.

96. Indeed, Dr. Goodrich could not have done so because he admitted in his deposition that he did not know anything about the operation of the Centripetal Threat Intelligence Gateway ("TIG")/RuleGATE or the Centripetal QuickThreat Gateway. EX1021 at 7:22-9:19. He had not heard of Patent Owner or these products prior to being retained by Patent Owner to work on the litigations involving this patent. *Id.* at 7:22-9:19, 11:22-12:16. Moreover, Dr. Goodrich was not familiar with competitor products to Patent Owner's products, so he was not able to provide opinions about whether other products in the industry were fulfilling any long-felt need, or whether other products succeeded or failed. *Id.* at 12:24-13:23.

97. Second, even if Patent Owner's products did embody the claimed technology, Dr. Goodrich's analysis does not establish that Patent Owner's products fulfilled a long-felt need or that others failed in fulfilling that need. Dr. Goodrich cites a presentation by Dr. Stanley Chincheck at the "Computer Network Defense/Information Assurance (CND/IA) Enabling Capability (EC) Industry Day"

at the U.S. Naval Research Laboratory in 2010. EX2004, ¶160; EX2013. Dr. Goodrich was not present to see this presentation (*see* EX1021 at 19:1-22), but he still claims that it shows that "[t]he failure of signature behavior based systems to keep up with emerging threats demanded new solutions." EX2004, ¶160. However, Dr. Goodrich admits that the Chincheck presentation does not discuss any specific product. EX1021 at 20:22-21:15. In fact, the Chincheck presentation does not discuss or even mention application layer protocols, or packet headers of any kind or generally any of the specific techniques employed by the ACNS Guide. Instead, the Chincheck 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). Moreover, Dr. Goodrich admits that Broad Agency Announcement ("BAA") presentations such as the Chincheck presentation specifically do not comment on particular products or approaches. EX1021 at 19:23-20:21. In it is common knowledge, that such BAA presentations are related to specific funding opportunities for research and development by a military research organization (the Office of Naval Research [ONR] in this case). BAA 10-1004 was for a program entitled "Proactive Computer Network Defense and Information Assurance (CND/IA)." ONR described the program as follows:

> The Office of Naval Research seeks innovative proposals for technologies that support "pro-active cybernetwork defense and information assurance" which can be adapted and integrated into an advanced prototype offering leading edge capabilities. This advanced

> prototype will ensure maximum continuity of cyber operations and availability of national assets and data during cyber conflict. The prototype will lead to new concepts for protecting data traversing the Department of the Navy (DON) networks and will provide decision management, intelligent decision aids, data fusion and correlation, and visualization capabilities.

See EX1022.

98. Thus, the Chincheck presentation relates to the highly specialized need of a military organization and its networks that arises "during cyber conflict." EX1022. It is not clear from this presentation what disclosures, if any, are relevant to the broader industry as a whole. For these reasons, the Chincheck presentation provides no insight into a potential long-felt need or the failure of others.

99. Dr. Goodrich also relies on an ESG Paper for the alleged satisfaction of long-felt need and failure of others (and industry praise). EX2004, ¶¶161-165. I disagree with his analysis. Dr. Goodrich does not address the fact that the ESG Paper states on its front page that it was "***commissioned by Centripetal Networks,***" i.e., Patent Owner. EX1006 at 1 (emphasis added). In other words, the ESG Paper is a marketing white paper that Patent Owner sought to have created. As such, it is my opinion that the ESG Paper is not objective evidence of a long-felt need or whether Patent Owner's products discussed in the ESG Paper fulfilled the long-felt need.

100. Further, Dr. Goodrich acknowledges that the ESG Paper does not discuss whether Patent Owner's products embody the claims of the '213 Patent. EX1021 at 24:12-30:7. For example, the quote from the ESG Paper recited in

Paragraph 162 of the Goodrich Declaration does not state whether Patent Owner's products perform the claimed "packet digest logging function" or the claimed "routing" of packets "to a monitoring device." Dr. Goodrich states that "[t]he claims of the '213 Patent are ***generally*** directed to receiving a 'dynamic security policy' from a 'security policy management server.'" EX2004, ¶163 (emphasis added). Dr. Goodrich does not explain how Patent Owner's products perform these steps or how any benefit attributed to the products derives from these steps

101. Dr. Goodrich cites page 7 of the ESG Paper for the "packet digest logging function" and "routing" limitations. EX2004, ¶¶162-164. However, page 7 of the ESG Paper contains only one general reference to "logging." EX1006 at 7. It does not explain how the logging occurs, or whether it involves the specific logging steps recited in the claims of the '213 Patent. *Id.* Dr. Goodrich claimed at his deposition that a POSA would have understood the claimed logging steps to be taking place from the single, general reference to "logging" in the ESG Paper. EX1021 at 24:12-29:15. If that is the case, then a POSA would also have understood the claimed logging steps to have been obvious to a POSA reading Kapoor's of Johnson's references to "logging."

102. Further, page 7 of the ESG Paper says nothing about "routing" packets "to a monitoring device." EX1006 at 7. In fact, the ESG Paper never uses the term "routing." EX1006.

103. Dr. Goodrich's long-felt need analysis also asserts that "Centripetal's TIG" has "best-in-class performance." EX2004, ¶165. He has no citation to support this assertion.

104. Thus, it is my opinion that Dr. Goodrich is unable to establish that any products of Patent Owner satisfied a long-felt need where others had failed.

B. Dr. Goodrich does not Establish Industry Praise.

105. Dr. Goodrich's analysis of industry praise begins with the statement that "[p]roducts embodying the invention claimed in the '213 Patent have received substantial industry praise." EX2004, ¶167. Again, Dr. Goodrich cites the ESG Paper that was "commissioned by Centripetal Networks" and discusses Patent Owner's TIG product. *Id.*; *see* EX1006 at 1. As discussed above, the ESG Paper does not explain whether Patent Owner's TIG product embodies the limitations of the claims of the '213 Patent. *See* Paragraphs 100-101 above. Further, the ESG Paper is essentially a marketing paper from Patent Owner itself, and a POSA would not consider this to be "industry praise" or objective evidence.

106. Dr. Goodrich also cites a Gartner publication that discusses Patent Owner generally and references Patent Owner's QuickThreat Gateway product. EX2004, ¶168. The Gartner publication does not explain if the QuickThreat Gateway embodies the claims of the '213 Patent, or how the QuickThreat Gateway differs from Patent Owner's TIG product. EX2007. Similarly, Dr. Goodrich's

citation to the American Banker article on "Top 10 FinTech Companies to Watch" for 2014 does not explain if Patent Owner's products embody the claims of the '213 Patent. EX2004, ¶168; EX2011. Moreover, both the Gartner publication and the American Banker article focus at a high level on Patent Owner and not the specifics of how the products operate or should be praised. EX2007; EX2011.

107. Thus, it is my opinion that Dr. Goodrich is unable to establish any objective evidence of industry praise that rebuts the obviousness of the claims of the '213 Patent in view of the prior art.

108. I reserve the right to supplement my opinions as appropriate if Patent Owner alleges or offers any purported evidence of any such secondary considerations of non-obviousness.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed this 7th day of October, 2019.

Respectfully submitted,

Dr. Kevin Jeffay