

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,

Petitioner,

- vs. -

ORCKIT IP, LLC,

Patent Owner.

Case IPR2023-00554

U.S. Patent No. 10,652,111

REPLY DECLARATION OF SAMRAT BHATTACHARJEE, PH.D.

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Materials Relied on in forming my opinions.....	2
III.	Level of Ordinary Skill in the Art and Priority Date.....	2
IV.	The '111 Patent.....	3
V.	The Prior Art References	3
	A. Lin	3
	B. Shieh.....	3
	C. Swenson	4
VI.	Claim Construction.....	4
VII.	The Prior Art Renders The Asserted Claims Obvious.	6
	A. The Combination of Lin and Swenson Renders Claim 1 Obvious.....	6
	1. Lin and Swenson Disclose or Render Obvious the Claimed Controller Under Either Patent Owner's or Petitioner's Proposed Constructions.	6
	B. The Combination of Shieh and Swenson Renders Claim 1 Obvious.	28
	C. Claim 3	32
	D. Claims 4 and 5.....	33
	E. Claim 6	33
	F. Claim 7	35
	G. Claim 16.....	37
	H. Claim 30	38

I, Samrat Bhattacharjee, Ph.D., hereby declare as follows:

I. INTRODUCTION

1. I have been retained on behalf of Cisco Systems, Inc. (“Cisco”) to provide my technical review, analysis, insights, and opinions concerning the validity of the claims of U.S. Patent No. 10,652,111 (EX1001; “the ’111 Patent”) entitled “Method and System for Deep Packet Inspection in Software Defined Network.” The patent is assigned to Orckit IP, LLC (“Orckit” or “Patent Owner”).

2. I am the same Samrat Bhattacharjee who provided a declaration on February 21, 2023, in support of Cisco’s Petition for *Inter Partes* Review in this proceeding. See EX1004. I maintain the opinions that were set forth in that previous declaration. I provide this reply declaration to respond to certain opinions provided by Miguel Gomez in a declaration (the “Gomez Declaration”) submitted in support of the Patent Owner Response filed by Patent Owner. The Gomez Declaration is marked as Exhibit 2025 in this proceeding.

3. My background and qualifications were set forth in Paragraphs 1-11 of my original declaration (EX1004) in this proceeding, as well as my curriculum vitae marked as Exhibit 1003, and I incorporate that information by reference in this reply declaration. In this reply declaration, I apply the same understanding of the governing law as set forth in Paragraphs 12-19 of my original declaration.

II. MATERIALS RELIED ON IN FORMING MY OPINIONS

4. In forming my opinions in this reply declaration, I have relied on the '111 Patent's claims, specification and prosecution history, on the prior art exhibits to the IPR Petition (Paper 1), any other materials cited in this reply 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 (EX1004), the materials cited in the Gomez Declaration, and the transcript of Mr. Gomez's deposition. I have also reviewed the Decision Granting Institution of *Inter Partes* Review provided by the U.S. Patent and Trademark Office Patent Trial and Appeal Board ("PTAB") in this proceeding. See Paper 8.

III. LEVEL OF ORDINARY SKILL IN THE ART AND PRIORITY DATE

5. In this reply declaration, I apply the same definition of a person of ordinary skill in the art ("POSA") as set forth in Paragraphs 48-49 of my original declaration. EX1004. Mr. Gomez does not dispute my definition of a POSA. EX2025, ¶¶23-25, 46-47; see Paper 22 at 16.

6. In this reply declaration, I apply the same priority date for the '111 Patent of April 22, 2014, as was set forth in Paragraph 47 of my original declaration. EX1004. Mr. Gomez's declaration asserts that the priority date for the '111 Patent should be April 7, 2006. EX2025, ¶¶23. However, he acknowledged during his

deposition that this was a mistake in his declaration, and he agreed that the priority date to be applied should be April 22, 2014. EX1016 at 54:16-55:24.

IV. THE '111 PATENT

7. In Paragraphs 36-39 of the Gomez Declaration, Mr. Gomez provides his description of the '111 Patent. EX2025. Paragraphs 30-46 of my original declaration provide a description of the specification disclosure and claims of the '111 Patent, as well as the prosecution history for the patent application that resulted in the issuance of the '111 Patent. EX1004.

V. THE PRIOR ART REFERENCES

A. Lin

8. Paragraphs 50-56 of my original declaration provide my opinions on the disclosure of Lin. EX1004. Mr. Gomez provides his opinions on Lin in Paragraphs 41-43 of the Gomez Declaration. EX2025. I note that some of the citations in Paragraph 43 of the Gomez Declaration cite to the wrong sections of Lin. Mr. Gomez acknowledged the mistaken citations during his deposition. EX1016 at 61:21-62:18. Further, Mr. Gomez cites to example embodiments in Lin (EX2025, ¶¶42-43), and a POSA would have known that the disclosure of Lin is not limited just to what is disclosed in example embodiments. EX1016 at 61:17-20.

B. Shieh

9. Paragraphs 57-62 of my original declaration provide my opinions on the disclosure of Shieh. EX1004. Mr. Gomez provides his opinions on Shieh in

Paragraph 44 of the Gomez Declaration. EX2025. I note that Mr. Gomez cites to an example embodiment in Shieh, and a POSA would have known that the disclosure of Shieh is not limited just to what is disclosed in an example embodiment.

C. Swenson

10. Paragraphs 63-68 of my original declaration provide my opinions on the disclosure of Swenson. EX1004. Mr. Gomez provides his opinions on Swenson in Paragraph 45 of the Gomez Declaration. EX2025. I again note that Mr. Gomez cites to example embodiments in Swenson, and a POSA would have known that the disclosure of Swenson is not limited just to what is disclosed in example embodiments.

VI. CLAIM CONSTRUCTION

11. Paragraphs 69-73 of my original declaration provide my opinions on the construction of the terms “controller” and “instruction” in the claims of the ’111 Patent. EX1004. In the Institution Decision, the PTAB determined that “no terms need to be construed at this time.” Paper 8 at 12. I maintain my opinion that “controller” and “instruction” should be construed for the reasons stated in my original declaration. EX1004, ¶¶69-73.

12. Patent Owner states in the Patent Owner Response that “the Court in the District Court Case preliminarily construed the term ‘controller’ as ‘an entity that is capable of controlling deep packet inspection.’” Paper 22 at 16. Patent Owner also

“submits that ‘controller’ should be construed consistent with the preliminary construction in the District Court Case as ‘an entity that is capable of controlling deep packet inspection.’” Paper 22 at 17. The Gomez Declaration does not take a position on claim construction. See EX2025, ¶¶26-27, 48.

13. It is my opinion that my proposed construction of controller (i.e., an entity configured to perform deep packet inspection on packets) is the correct construction because it more closely aligns with what is disclosed in the ’111 Patent. For example, the ’111 Patent explains that “the central controller 111 is **configured to perform deep packet inspection on designated packets** from designated flows or TCP sessions.” EX1001, Col. 4:5-7 (emphasis added); see also id., Col. 4:8-18, 4:49-50. In addition, the ’111 Patent states that “the central controller 111 includes a DPI flow detection module 311, a DPI engine 312, and a memory 313, and a processing unit 314,” as shown below in Figure 3. EX1001, Col. 5:33-36; see id., Cols. 5:40-59 (discussing DPI flow detection module 311 located within central controller 111 in Figure 3), 8:1-5, 9:67-10:1, Figure 6. Patent Owner’s proposed construction of “an entity that is **capable of controlling** deep packet inspection” is not as consistent with these disclosures from the ’111 Patent. Paper 22 at 17 (emphasis added).

14. However, regardless of whether the Board adopts my proposed claim constructions or Patent Owner’s proposed construction of “controller,” or provides

no claim constructions, my opinions on the unpatentability of Claims 1-9, 12-24 and 27-31 of the '111 Patent would remain the same.

VII. THE PRIOR ART RENDERS THE ASSERTED CLAIMS OBVIOUS.

15. Paragraphs 74-319 of my original declaration contain my opinions that the combinations of (1) Lin and Swenson or (2) Shieh and Swenson render Claims 1-9, 12-24 and 27-31 of the '111 Patent unpatentable as obvious. EX1004. I maintain those opinions, and, below, I provide my opinions in reply to the analysis of these patent claims in the Gomez Declaration.

A. The Combination of Lin and Swenson Renders Claim 1 Obvious.

1. Lin and Swenson Disclose or Render Obvious the Claimed Controller Under Either Patent Owner's or Petitioner's Proposed Constructions.

16. Paragraphs 49-83 of the Gomez Declaration assert Mr. Gomez's opinion that neither Lin nor Swenson disclose the controller recited in Claim 1. EX2025. I disagree for the reasons stated in my original declaration (EX1004) and throughout this reply declaration.

17. Mr. Gomez provides his opinion that "In other words, Petitioner's theory appears to be that either (i) a POSA would implement DPI as part of Lin's controller, notwithstanding that Lin discloses a security service entity for DPI that is separate from the controller, or (ii) a POSA would have been motivated to combine Lin with Swenson, which Petitioner asserts discloses a controller that is capable of performing DPI." EX2025, ¶50. This statement from Mr. Gomez does not address

the full scope of my opinions. As I explained in my original declaration, Lin discloses that its SDN switch (i.e., the network node) is under the control of a “SDN controller” that is external to the SDN switch, and the SDN controller “provides a logically centralized framework for controlling the behavior of the SDN computer network 600.” EX1005, Col. 4:8-31; Lin also discloses that “[t]he SDN controller 610 and the SDN switch 620 are logically separate components.” Id., Col. 3:51-52; EX1004, ¶78. A POSA would have understood that “logically separate components” can be implemented in the same physical device.

18. Further, as explained in my opening declaration, Lin discloses a security service 630 that performs DPI and that “[t]he security service 630 may be connected to the SDN switch 620 by a physical link (i.e., using a wire), a virtual link (i.e., in a virtualized environment), or by a software tunnel.” EX1005, Cols. 3:11-12, 5:51-58; EX1004, ¶79. It is my opinion that a POSA would have understood these disclosures in Lin to teach that the security service 630 can be implemented using the same hardware or software as the controller, and that the security service 630 can be connected to the SDN switch 620 in the same way as the controller. As such, a POSA would have understood that one of the limited number of design options would have been to implement the security service as part of a controller configured to perform DPI analysis on packets, and a POSA would have had a

reasonable expectation that the controller would have been successful in performing DPI analysis.

19. Further, as explained in my original declaration, it is my opinion that Swenson teaches the use of a controller configured to perform DPI. EX1004, ¶¶80-86. Swenson discloses that “the flow analyzer 312 of the network controller 140 performs a deep flow inspection to determine if the flow is worth bandwidth monitoring and/or user detection.” EX1007, ¶[0059]; see id., ¶[0060] (stating that the “controller 140 ingests the network flow for inspection”), Figures 1, 4A-4B. It is my opinion that a POSA would have understood that a “flow” is a series of packets having a specific signature. Thus, a POSA would have known that the reference to “deep flow inspection” in Swenson refers to performing DPI on one or more packets in a flow. Further, it is my opinion that a POSA would have understood that Paragraph [0065]’s discussion of analysis of the “response payload” of a packet to be DPI by a DPI-capable controller. EX1007, ¶[0065]. These disclosures in Swenson demonstrate that it would have been well-known to a POSA as of the priority date for the ’111 Patent to implement a controller configured to perform DPI analysis in a system such as Lin. Id., ¶¶[0026], [0028]-[0029], [0046], [0059]-[0060], [0073], [0076]-[0077], [0084]-[0086], Figures 1 and 4A-4B.

a. Lin discloses or renders obvious a controller configured to perform or capable of controlling DPI.

20. Paragraphs 52-55 of the Gomez Declaration state Mr. Gomez's opinion that Lin "does not disclose a controller that is configured to perform or capable of controlling deep packet inspection. Lin teaches that DPI is performed by security service 630, not controller 610." EX2025, ¶¶52-55. I disagree. As discussed above, while Lin discusses a separate security service 630, it is my opinion that a POSA would have understood that one of the limited number of design options would have been to implement the security service as part of a controller configured to perform DPI analysis on packets, and a POSA would have had a reasonable expectation that the controller would have been successful in performing DPI analysis. EX1005, Cols. 3:11-12, 3:51-58, 4:8-31, Figures 1, 6-8; EX1004, ¶¶78-79.

21. Mr. Gomez argues that "[t]he mere fact that the security service may share certain common technical characteristics with the controller (i.e., its connection to the network switch and the hardware in which these two separate entities are implemented) cannot in and of itself suggest to a POSA that the function carried out by the security service should also be performed by the controller or that the controller should be configured to perform that function (i.e., deep packet inspection)." EX2025, ¶54. First, Mr. Gomez does not challenge my opinion that the security service 630 has the same physical connections to the SDN switch in Lin as the SDN controller. EX1005, Cols. 3:11-12, 5:51-58; EX1004, ¶79. Second, I

disagree with Mr. Lin's opinion because, taken as a whole, the disclosure of Lin demonstrates that the security service 630 could have been implemented as part of the controller or as a separate component from the controller. EX1005, Cols. 3:11-12, 3:51-58, 4:8-31, Figures 1, 6-8; EX1004, ¶¶78-79. There are limited design options as to where the security service would be implemented, and a POSA would have found it obvious that one of those limited design options was to implement the security service as part of the controller. I note that the '111 Patent does not give any specific technical mechanisms for implementing DPI in its controller. Mr. Gomez seemingly, and without explicating reasons, places a higher burden on the prior art, especially in light of the allegedly inventive aspects or disclosures in the '111 Patent.

22. Mr. Gomez asserts that "Lin explicitly separates network security services (including DPI) from the controller (or the network administrators responsible for configuring the controller), stating: '[n]etwork security vendors provide network security services, such as firewall or deep packet inspection (DPI)' (Ex. 1005, 3:11-12)." EX2025, ¶55. I disagree with this narrow reading of Lin. Certainly, there are network security vendors that can provide network security services as part of a separate module from the controller. However, even with the existence of such network security services, a POSA still would have understood that a separate design option would have been to implement the security service as part of the controller. A packet has to be routed (or mirrored) to the security service

for inspection, and this could just as easily have been done with the security service being part of the controller as the security service being a stand-alone module.

23. Mr. Gomez provides his opinion that the background of the '111 Patent teaches away from implementing the security service as part of the controller because the '111 Patent discusses “drawbacks” of prior art implementing the “straightforward approach of routing all traffic from network nodes to the central controller.” EX2025, ¶55. Mr. Gomez notes that the '111 Patent identifies “increased end-to-end traffic delays between the client and the server; overflowing the controller capability to perform other networking functions; and a single point of failure for the re-routed traffic.” Id., citing EX1001, 2:1-5. Thus, Mr. Gomez argues that “it was known in the art before the '111 [P]atent that performing DPI at the controller presented material challenges and disadvantages.” Id. I disagree. The prior art discussed in the background section of the '111 Patent involved systems in which “all traffic” was routed from network nodes to the central controller. EX1001, 2:1-5. That is not the case with Lin. In Lin, only specific packets meeting certain criteria are routed to the security device 630, such as routing HTTP packets to the security device. See, e.g., EX1005, Cols. 5:16-24, 5:26-36, 6:1-12, 6:40-54, 7:24-8:18, Table 1. When only certain packets are routed to the security device, as opposed to all packets, then Mr. Gomez’s concerns about the prior art “drawbacks” are not

applicable because there is not as much traffic sent to the controller to cause end-to-end traffic delays or an overflow of the controller's capabilities.

24. Further, the existence of a separate security service would be just as likely to cause a "single point of failure for the re-routed traffic" as a security service that is part of a controller. This would not be a reason to avoid implementing the security service as part of the controller. Indeed, there is no logical reason not to combine them, and Mr. Gomez does not provide any.

25. Mr. Gomez also asserts that "a POSA at the time of invention would [have understood] that security services were not normally combined with a controller because the security service requires security resources not normally found in a controller or that would be prohibitively expensive to implement as part of the controller." EX2025, ¶55. Mr. Gomez cites no support for these statements, and I disagree with them. For example, Mr. Gomez does not explain what are the "security resources not normally found in a controller." At his deposition, Mr. Gomez speculated that there can be "management and dataflow issues" with implementing security functions in the controller, but that is not more specific than his declaration. EX1016 at 33:20-37:19. I disagree with Mr. Gomez's argument because the security service would require "security resources" or overcoming "management and dataflow issues" wherever it is implemented. These would be no different if the security service was implemented in the controller or elsewhere.

Indeed, Swenson implemented its deep flow inspection as part of its flow analyzer in its controller without any mention of “security resources” or “management and dataflow issues.” EX1007, ¶¶[0026], [0028]-[0029], [0039], [0059], [0060], [0065]. Swenson discloses an embodiment of its controller in Figure 3 and explains that the controller would include “[c]onventional components” such as “security functions.” EX1007, ¶[0039]. Further, the ’111 Patent disclosed that its “DPI engine 312” was implemented in “the central controller 111” to inspect packets without any mention of additional “security resources” or “management and dataflow issues” that would have made it difficult to achieve this task. See, e.g., EX1001, 5:33-49.

26. In addition, it is my opinion that Mr. Gomez has not shown why it would be “prohibitively expensive to implement [the security service] as part of the controller.” EX2025, ¶55. Mr. Gomez cites no support for this assertion, and he does not explain why it would be cheaper to have two separate components (a separate controller and security service) than to implement them as one. I do not think it would be prohibitively expensive to have the security service as part of the controller. Swenson did not mention that it was “prohibitively expensive” to implement deep flow inspection as part of its controller. EX1007, ¶¶[0026], [0028]-[0029], [0059], [0060], [0065]. Indeed, Swenson states that security functions would be one of the conventional components on the controller. *Id.*, ¶¶[0039], Figure 3. Further, the ’111 Patent does not say it was “prohibitively expensive” to implement

DPI engine 312 in central controller 111. See, e.g., EX1001, 5:33-49. Neither the claims nor the specification of the '111 Patent say anything about how to prevent the alleged prohibitive costs of implementing the security device in the controller. Mr. Gomez is again seemingly imposing a higher burden of disclosure on the prior art requiring more of the prior art, especially in light of the allegedly inventive aspects or disclosures in the '111 Patent.

27. Moreover, a POSA still would have known that it was only one of a limited number of design options to implement the security service as part of the controller, even if the process was expensive or required extra “security resources” or “management resources.” Thus, for the reasons explained throughout this reply declaration and in my original declaration (EX1004), I disagree with Mr. Gomez’s conclusion that “Lin alone does not give a POSA any reason to implement the security service as part of the controller, nor a reasonable expectation of success in doing so.” EX2025, ¶55.

b. Swenson also discloses or renders obvious a controller configured to perform or capable of controlling DPI.

28. Paragraphs 56-69 of the Gomez Declaration state Mr. Gomez’s opinion that Swenson does not disclose or render obvious a controller that is configured to perform or capable of controlling deep packet inspection. EX2025, ¶¶56-69. I disagree. Mr. Gomez provides his opinion that “A POSA would understand that Lin discloses deep packet inspection (DPI) performed at a dedicated security service,

whereas Swenson discloses deep flow inspection (DFI) performed in the flow analyzer of a network controller. Thus, Lin and Swenson disclose different techniques, which a POSA would understand from the use of different terms of art in the two references.” EX2025, ¶57; see id., ¶58 (arguing “that deep *flow* inspection is not the same as deep *packet* inspection” (emphasis in original)). As I explained in my original declaration, it is my opinion that a POSA would have understood that a “flow” is a series of packets having a specific signature. EX1004, ¶¶80-86. Thus, a POSA would have known that the reference to “deep flow inspection” in Swenson refers to performing DPI on one or more packets in a flow. Further, it is my opinion that a POSA would have understood that Paragraph [0065]’s discussion of analysis of the “response payload” of a packet to be DPI by a DPI-capable controller. EX1007, ¶[0065]; see id., ¶¶[0026], [0028]-[0029], [0046], [0059]-[0060], [0073], [0076]-[0077], [0084]-[0086], Figures 1 and 4A-4B.

29. I agree with Mr. Gomez that DPI was a “well-known technique used for computer network packet filtering” that was “used in enterprise security to detect various attacks” as of the priority date for the ’111 Patent. EX2025, ¶58. However, I disagree with Mr. Gomez’s assertion that DPI “presents certain unique challenges” because it “requires significant processing power and may struggle with high-bandwidth networks or encrypted traffic.” EX2025, ¶59. First, these are not requirements of the claims of the ’111 Patent, and the discussion of DPI in the

specification of the '111 Patent does not mention requirements of “significant processing power” or struggles with “high-bandwidth networks or encrypted traffic.” Second, Mr. Gomez provides no support for his assertion. DPI processing was well-known as of the priority date of the '111 Patent, and there was nothing that would have prevented a POSA from using it. EX1005, ¶[0021]; EX1006, Col. 3:11-24; EX1001, Col. 1:20-29. Further, Mr. Gomez speculates that “DPI tools may have limited visibility into the overall traffic patterns of networks in which less traffic flows through core switches (e.g., in modern distributed network environments).” EX2025, ¶59. Again, Mr. Gomez cites no support for this assertion, it is not recited in the specification or claims of the '111 Patent, and I do not see a reason why a POSA would have been discouraged from using DPI on this basis.

30. With respect to DFI, Mr. Gomez asserts that it is “focused on the flow of data within the network rather than the inspection of individual packets.” EX2025, ¶60. I disagree. The DFI performed in Swenson is inspection of the payload of individual packets and thus would constitute DPI, in addition to any other flow-related analysis disclosed in Swenson. EX1007, ¶¶[0059]-[0060], [0065]. As previously explained, a “flow” is a series of packets having a specific signature. EX1004, ¶¶80-86. Paragraph [0065] of Swenson discloses analysis of the “response payload” of a packet. A POSA would have understood the analysis of the “response payload” to be DPI by a DPI-capable controller. EX1007, ¶[0065]; see id., ¶¶[0026],

[0028]-[0029], [0046], [0059]-[0060], [0073], [0076]-[0077], [0084]-[0086], Figures 1 and 4A-4B. Moreover, even if the analysis involves reviewing the response payload of multiple packets, a POSA still would have considered this to be DPI because Swenson is explicitly disclosing the analysis of the payload of individual packets in a flow.

31. Mr. Gomez notes that “[f]low data typically includes information about the IP addresses, ports and protocol types involved in a communication session.” EX2025, ¶61. But that is not what is disclosed in Swenson, which discusses analyzing the “response payload” of HTTP packets (i.e., performing DPI). EX1007, ¶[0065]; see id., ¶¶[0059]-[0060]. Further, Mr. Gomez states that “DFI can be used for purposes like traffic analysis, network performance monitoring, and the detection of unusual or suspicious behavior patterns in network traffic.” EX2025, ¶61. The same is true for DPI. See EX1005, ¶[0021]; EX1006, Cols. 3:11-24, 5:16-25; EX1001, Col. 1:20-29. For these reasons, I disagree with Mr. Gomez’s unsupported assertion that DPI and DFI “entail material differences, and that deep packet inspection entails unique technical capabilities and challenges that distinguish it from deep flow inspection.” EX2025, ¶62.

32. Mr. Gomez asserts that the DFI in Swenson is “a materially different technique” than DPI because “Swenson’s disclosures of a system [are] geared toward bandwidth and user experience optimization through the use of statistic

information relating to flows, not the inspection of packet contents.” EX2025, ¶63. I disagree that this shows DFI and DPI to be materially different. Swenson discloses the monitoring of network traffic by redirecting certain traffic flows that meet specific criteria (such as HTTP packets) to a central controller for inspection and a determination on how to act on that network traffic. A POSA would have understood that this teaching is equally applicable to redirecting certain packets that meet specific criteria to a central controller for DPI. A POSA’s understanding of this technique is not changed by the reason for inspecting the traffic, whether it is to monitor malicious activity, bandwidth usage or user experience optimization.

33. Further, as explained in Paragraph 83 of my original declaration, a POSA would have understood that Swenson, like Lin, could involve analyzing packets for a security function, such as using bandwidth monitoring as a security application to detect Denial of Service (“DOS”) attacks that occupy significant bandwidth in a network. EX1007, ¶¶[0059]-[0060]; see id., ¶[0039] (explaining that the controller can incorporate “security functions”); EX1004, ¶83. As such, Swenson is performing DPI (id., ¶[0065]), and Swenson discloses using its technology for a security function (id., ¶¶[0039], [0059]-[0060]). For these reasons, I do not agree with Mr. Gomez’s statements that “DPI would have little use for the purposes of Swenson’s traffic analysis due to the higher overhead it would impose upon the Swenson system as a whole” or that a POSA would not combine the teachings of

Lin and Swenson. EX2025, ¶¶64-65. Further, I disagree with Mr. Gomez’s statement that “[n]othing in the Petition satisfactorily addresses the distinctions between deep packet inspection and deep flow inspection.” Id., ¶66.

34. Mr. Gomez also provides his opinion that “Swenson’s disclosure of the controller analyzing a message does not require analyzing the message payload.” EX2025, ¶¶67-68. Mr. Gomez acknowledges my analysis of the portion of Swenson that discusses inspection of “[a] HTTP GET request header and a portion of the [HTTP] response payload.” EX1004, ¶81, discussing EX1007, ¶[0065]. However, Mr. Gomez asserts that “[t]he reference to a HTTP request and response ‘header’ and ‘payload’ are thus not references to the header and payload of a packet” and accordingly Swenson does not perform DPI. EX2025, ¶69. I disagree. As I explained in Paragraphs 80-81 of my original declaration, Swenson is explicit in stating that its inspection techniques include inspection of “a portion of the [HTTP] response payload.” EX1004, ¶¶80-81, discussing EX1007, ¶[0065]. A POSA would have understood the analysis of the “response payload” to be DPI by a DPI-capable controller, as DPI refers to monitoring the payload of a packet. Mr. Gomez cites no support for refuting this analysis. Moreover, I note that the ’111 Patent does not require DPI to analyze every packet in a flow; instead, DPI requires that the system must have the capability to look at the payload or body of a packet. A POSA would have understood Swenson to disclose this capability.

35. Indeed, Mr. Gomez appears to understand that Swenson discloses a DPI-capable controller because he argues that “[e]ven assuming that Swenson’s controller were analyzing the header and payload of an HTTP request/response, a POSA would understand that this analysis is not at the packet [level] but at the flow level and thus does not constitute deep packet inspection.” EX2025, ¶¶69. I disagree for the reasons stated in my original declaration and stated above in this reply declaration. EX1004, ¶¶80-81. For example, a HTTP GET request and a HTTP response each can be encompassed in a single packet. In that situation, the inspection of the packets containing the request or the response, including “a portion of the [HTTP] response payload,” would be DPI. EX1007, ¶¶0065].

c. A POSA would have combined Swenson’s controller with Lin or adapted such a combination to practice the claimed controller.

36. Paragraphs 70-76 of the Gomez Declaration state Mr. Gomez’s opinion that “a POSA ... would not have combined Swenson’s controller with Lin’s system, even if Swenson disclosed (it does not) a controller that satisfied either Petitioner’s or Patent Owner’s proposed construction (i.e., an entity configured to perform or capable of controlling DPI).” EX2025, ¶¶70. I disagree for the reasons stated in Paragraphs 82-86 of my original declaration (EX1004) and those stated throughout this reply declaration.

37. Mr. Gomez asserts that a POSA would not have been motivated to combine the teachings of Lin and Swenson because Swenson “is directed to a much narrower function than Lin (bandwidth monitoring) and deploys an altogether different technique (deep flow inspection) in the controller that is much less taxing on the controller than the deep packet inspection, which is performed by a altogether different device in Lin (the security service).” EX2025, ¶71. Mr. Gomez also argues that there is no motivation to combine because “deep packet inspection in Lin is much more resource-intensive than the deep flow inspection taught in Swenson.” Id. I disagree for multiple reasons. First, I disagree that Lin’s discussion of inspection of packets for a security service differentiates it from Swenson. The relevant teaching that a POSA would have understood from Swenson is that certain network flows, which are a series of packets having a specific signature, are directed to a controller for DPI. EX1004, ¶¶80-81. The fact that the inspection may be for security services (as in Lin) or for bandwidth monitoring (as in Swenson) does not matter, as a POSA still would have understood the central point of having the inspection performed at the controller. For example, Claim 1 of the ’111 Patent does not discuss the reason why a packet meeting the packet-applicable criterion is sent to the entity “other than the second entity”; the claim does not reference security services or bandwidth monitoring. See EX1001, Cols. 10:52-11:4. Further, Mr. Gomez does not

address the broader point that the combination of Lin and Swenson involves inspection for security services, regardless of what Swenson does by itself.

38. Second, as discussed above, a POSA would have understood that Swenson, like Lin, could involve analyzing packets for a security function, such as using bandwidth monitoring as a security application to detect DOS attacks that occupy significant bandwidth in a network. EX1007, ¶¶[0059]-[0060]; see EX1007, ¶[0039] (explaining that the controller can incorporate “security functions”); EX1004, ¶83. Third, Mr. Gomez’s argument that DFI is “much less taxing on the controller” than DPI is unsupported, and I disagree with it. A controller would have been able to perform both DFI and DPI, as both techniques were known in the art. Indeed, I note that neither Swenson nor the ’111 Patent recite that performing DFI or DPI at the controller were “taxing” on the controller.

39. Mr. Gomez also provides his opinion that Swenson’s disclosure of “directing HTTP messages—which can consist of numerous packets—to the controller for analysis of that message” does not teach “routing packets for deep packet inspection.” EX2025, ¶72. I disagree. Swenson teaches routing certain packets (HTTP messages), or payloads of a packet, to the controller for inspection and allowing other packets to proceed to their destination without being routed to the controller. EX1007, ¶¶[0059]-[0060], [0065]. As one example, a HTTP GET request and a HTTP response each can be encompassed in a single packet. In that

situation, the inspection of the packets containing the request or the response, including “a portion of the [HTTP] response payload,” by the controller constitutes DPI. EX1007, ¶[0065].

40. Mr. Gomez provides his opinion that Swenson does not disclose “analyzing packets for a security function” or “send[ing] packets to the controller for DPI.” EX2025, ¶73. He acknowledges that Swenson discloses that its controller can include “[c]onventional components” such as “security functions.” Id., citing EX1007, ¶[0039]. However, he relies on a statement in Swenson that these conventional components in the controller “are not shown so as not to obscure the details of the system architecture” (EX1007, ¶[0039]) to assert that Swenson does not teach “technical details pertaining to security (such as DPI or how DPI might be conducted in the context of a SDN).” EX2025, ¶73. It is not clear what point Mr. Gomez is trying to make by citing this portion of Swenson. From my review of Paragraph [0039] in Swenson, it is simply disclosing that security functions (and other conventional components) can be included in the controller but that those components are not shown in Figure 3 of Swenson in order to not make the figure overly detailed. However, a POSA still would have understood that these components are disclosed to be part of the controller. EX1007, ¶[0039]. Further, as explained above, a POSA would have understood that Swenson is performing DPI at the controller, including for security reasons such as preventing DOS attacks. See

EX1007, ¶¶[0059]-[0060], [0065]. As such, I disagree with Mr. Gomez’s assertions that “Swenson focuses on network bandwidth and traffic congestion and does not pertain to network security, let alone resource-intensive techniques such as DPI or the specific manner in which such techniques might be executed or optimized” (EX2025, ¶74) and that “Swenson is not focused on DPI at all, and expressly *omits* controller-based security functions like DPI.” EX2025, ¶75 (emphasis in original).

41. Mr. Gomez also provides his opinion that “Lin does not contain any teaching that its security service—which is the device used to perform DPI—could or should be implemented in the controller.” EX2025, ¶76. This is incorrect for the reasons stated in Paragraph 79 of my original declaration (EX1004) and those stated throughout this reply declaration. A POSA would have understood that one of the limited number of design options would have been to implement the security service 630 in Lin as part of a controller configured to perform DPI analysis on packets, and a POSA would have had a reasonable expectation that the controller would have been successful in performing DPI analysis. EX1005, Cols. 3:11-12, 3:51-58, 4:8-31, Figures 1, 6-8. A packet has to be routed (or mirrored) to the security service for inspection, and this could just as easily have been done with the security service being part of the controller as the security service being a stand-alone module.

42. Mr. Gomez references a “drawback” of the prior art identified in the ’111 Patent (EX2025, ¶75), but the prior art discussed in the ’111 Patent involved

systems in which “all traffic” was routed from network nodes to the central controller. EX1001, 2:1-5. That is not the case with Lin. In Lin, only specific packets meeting certain criteria are routed to the security device 630, such as routing HTTP packets to the security device. See, e.g., EX1005, Cols. 5:16-24, 5:26-36, 6:1-12, 6:40-54, 7:24-8:18, Table 1. When only certain packets are routed to the security device, as opposed to all packets, then Mr. Gomez’s concerns about the prior art “drawbacks” are not applicable because there is not as much traffic sent to the controller to cause end-to-end traffic delays or an overflow of the controller’s capabilities.

d. Lin discloses or renders obvious sending the packet to the second entity “responsive to the packet not satisfying the criterion” or sending the packet to an entity other than the second entity “responsive to the packet satisfying the criterion.”

43. Paragraphs 77-83 of the Gomez Declaration state Mr. Gomez’s opinion that Lin does not disclose or render obvious sending the packet to the second entity “responsive to the packet not satisfying the criterion” or sending the packet to an entity other than the second entity “responsive to the packet satisfying the criterion,” as recited in Claim 1. EX2025. I disagree. Mr. Gomez’s opinion is based on his claim that “the Petition incorrectly relies on two separate criteria to satisfy this limitation, whereas Claim 1 requires a single criterion be used to make the claimed routing decision (i.e., based on whether that criterion is satisfied or not satisfied).” EX2025,

¶78. Paragraphs 79-83 of the Gomez Declaration argue that the embodiment shown in Table 3 of Lin identifies two criteria for deciding what actions to take on a packet, pointing to the “bypass flow rule” and the “redirect flow rule.” Id., ¶¶79-83. I disagree because Mr. Gomez’s analysis seems to misunderstand my opinion, as he confuses the broader flows rules with the more narrow packet-applicable criterion within the flow rules. As I explained in my opening declaration, Lin discloses that its SDN controller inserts “flow rules in a flow table of the SDN switch to create an SDN pipe between a sender component and a security component.” EX1005, Col. 1:60-62. For instance, Lin provides examples of flow rules that are inserted into the SDN switch to determine how to handle HTTP packets received at the SDN switch. See EX1005, Cols. 1:58-2:4, 4:14-31, 4:53-67, 6:1-12. 7:39-8:18.

44. With respect to Table 3, Lin discloses flow rule in the form of a “bypass flow rule” and the “redirect flow rule.” EX1005, Cols. 7:39-8:18. However, these flows rules are not packet-applicable criterion; instead, the flow rules contain packet-applicable criterion. Lin states that the flow rules “may indicate inspection of particular packets (e.g., those that meet one or more conditions) by a security service 630.” EX1005, Col. 4:23-31; see EX1005, Col. 5:8-12. A POSA would have understood that the “one or more conditions” used to identify “particular packets” for inspection would be the packet-applicable criterion. In other words, Lin teaches that criterion specific to a particular packet are used to determine what action to take

on a packet, such as determining which packets are forwarded to security service 630. EX1005, Col. 4:23-31; see id., Col. 5:8-12. Lin provides examples of the conditions (or criterion) applicable to a particular packet, including “‘IN_PORT’, ‘MAC src’ (media access control (MAC) address of the source of the packet), ‘MAC dst’ (MAC address of the destination of the packet), ‘IP src’ (Internet Protocol (IP) address of the source of the packet), ‘IP dst’ (IP address of the destination of the packet).” EX1005, Col. 5:16-21. Lin states, “When the conditions are met, i.e., the particular packet is identified, the action indicated in the corresponding ‘Action’ column is performed on the packet.” EX1005, Col. 5:22-24; see id., Cols. 5:26-36, 6:1-12, 6:40-54, Table 1.

45. In other words, the “redirect flow rule and the “bypass flow rule” work together to decide what to do with a packet based on a single criterion (i.e., whether the packet is a HTTP packet, as indicated by the “TCP src port” or “TCP dst port”). Id., Cols. 7:64-8:18, Table 3. If the single criterion indicates that the packet is an HTTP packet, then the packet is redirected to the security service. If the single criterion indicates that the packet is not an HTTP packet, then the packet is forwarded to its original destination. Id. Though this is implemented using the “redirect flow rule and the “bypass flow rule,” the ultimate determination of the action to take is based on a *single criterion* (whether or not the packet is an HTTP packet).

46. Further, Mr. Gomez provides his opinion that “Lin does not teach how a packet is sent if either the bypass flow rule and redirect flow rule conditions are both not satisfied.” EX2025, ¶82. I disagree. The embodiment shown in Table 3 of Lin accounts for all packets – HTTP packets are redirected and all other packets are forwarded to their destination.

B. The Combination of Shieh and Swenson Renders Claim 1 Obvious.

47. Paragraphs 84-89 of the Gomez Declaration assert Mr. Gomez’s opinion that Shieh does not disclose the claimed “packet-applicable criterion” responsive to which a packet is sent either to a second entity or to another entity that is different from the second entity. EX2025, ¶¶84-89. In providing his opinion, Mr., Gomez notes “that the Board’s Institution Decision previously found that Swenson does not disclose a ‘packet-applicable criterion.’” Id., ¶84, citing Paper 8 at 19. I disagree with Mr. Gomez and with the Institution Decision on this point for the reasons stated in my original declaration (EX1004, ¶¶224, 239-245) and those stated below in this reply declaration.

48. Mr. Gomez first states that “the Petition asserted that Shieh’s ‘the identification of ‘TCP FIN or TCP RST packets’ ... are packet-applicable criterion.’” EX2025, ¶85. I note that, while my original declaration lists the “identification of TCP FIN or TCP RST packets” as an example of packet-applicable criterion, that is not the only packet-applicable criterion that I identified. For example, Paragraphs

241 and 244 of my original declaration also explain that the method disclosed in Shieh checks whether a packet should be forwarded to a security processing device “based on a bypass flag.” See EX1004, ¶¶141 and 144, discussing EX1006, ¶[0037], Figure 7. This bypass flag was identified as a separate example of a packet-applicable criterion. EX1004, ¶¶141, 144. Pages 65-66 of the Petition similarly identify the bypass flag as a packet-applicable criterion. Paragraph [0037] of Shieh explains that the network access device “determine[s] whether a bypass flag [in a packet] has been set to a predetermined value.” EX1006, ¶[0037]. “If the bypass flag matches the predetermined value, the packet is forwarded to security device 273 [which corresponds to the claimed entity that is other than the second entity] via path 282; otherwise, the packet is routed to destination node 274 [which corresponds to the claimed second entity].” Id.

49. Second, Mr. Gomez asserts that “Shieh does not inform a POSA how to send a TCP FIN or TCP TST packet from the controller to the network switch.” EX2025, ¶86. Mr. Gomez appears to misunderstand my opinions on Shieh. It is my opinion that a POSA would have understood from Shieh that the controller communicated to the network access devices 204A-204C to use the “identification of TCP FIN or TCP RST packets” as a packet-applicable criterion for determining whether to route packets to a security processing device for inspection. As I explained in Paragraph 224 of my original declaration (EX1004), Shieh sends a

command from the controller to the network access devices 204A-204C “to set up a set of filtering rules concerning whether and/or what types of packets should be forwarded to a security device.” EX1006, ¶¶[0017]-[0018], [0023], [0028]-[0029]. A POSA would have understood that the network access device would use a packet-applicable criterion to determine which packets should be forwarded to the security device pursuant to the filtering rules. Id., ¶¶[0035]-[0036], [0049]. It is my opinion that a POSA would have known that, in SDN, these packet-applicable criterion would be sent from a controller to one or more network access devices. This allows the same packet-applicable criterion to be applied at multiple network nodes (i.e., network access devices). For the same reasons, if the packet-application criterion were determining whether a packet should be forwarded to a security processing device “based on a bypass flag,” it is my opinion that a POSA would have known that, in SDN, this packet-applicable criterion would be sent from a controller to one or more network access devices.

50. Third, Mr. Gomez asserts that “the alleged packet-applicable criterion (TCP FIN or TCP RST) in Shieh fails to satisfy the remaining elements of claim 1, which requires ‘checking...if the packet satisfies the criterion’ and then ‘sending...the packet to the second entity’ or ‘sending...the packet to an entity that is included in the instruction and is other than the second entity’ based on whether the packet satisfies the criterion.” EX2025, ¶87. I disagree. Paragraph [0036] of

Shieh states that “[d]uring the bypass phase, the I/O function may notify the security-processing function if there are special events in the packet stream. These events could be receipt of TCP FIN or TCP RST packets, or not receiving any packets of the connection within a time threshold.” EX1006, ¶[0036]. Shieh explains that “[t]he notification from I/O function to security processing functions could help to clean up the state in the security-processing nodes.” Id. A POSA would have understood this disclosure in the context of Paragraph [0035] of Shieh, which explains that “communication between I/O functions and security-processing functions [enable] packets to bypass security-processing function if there is no more need to inspect the packets of the connection.” Id., ¶[0035]. In other words, Shieh discloses that its system is using packet-applicable criterion in the form of “the identification of TCP FIN or TCP RST packets” to determine whether to continue to forward packets to the security-processing function for inspection.

51. Further, as explained above, my original declaration explained that Shieh discloses a separate packet-applicable criterion “based on a bypass flag” that is used to determine whether a packet should be forwarded to a security processing device. See EX1004, ¶¶141 and 144, discussing EX1006, ¶[0037], Figure 7. Pages 65-66 of the Petition similarly identify the bypass flag as a packet-applicable criterion. Paragraph [0037] of Shieh explains that the network access device “determine[s] whether a bypass flag [in a packet] has been set to a predetermined

value.” EX1006, ¶¶0037]. “If the bypass flag matches the predetermined value, the packet is forwarded to security device 273 [which corresponds to the claimed entity that is other than the second entity] via path 282; otherwise, the packet is routed to destination node 274 [which corresponds to the claimed second entity].” Thus, the pages 65-66 of the Petition and Paragraphs 141 and 144 of my original declaration contradict Mr. Gomez’s statement that the bypass flag was not “alleged to be a packet-applicable criterion in element 1.1.” EX2025, ¶¶87-89.

C. Claim 3

52. Paragraphs 90-94 of the Gomez Declaration state Mr. Gomez’s opinion that “[t]he prior art does not disclose sending the packet to an entity that is other than the second entity *and* to the *controller*.” EX2025 (heading above ¶90) (italic emphasis in original). This argument is premised on Mr. Gomez’s opinion that “a POSA would understand that the logic and grammar of claim 1 requires that claim to be performed in the stated order of steps.” EX2025, ¶91. I disagree. First, Mr. Gomez has not explained what it is about Claims 1 and 3 that require their steps to be performed in a specific order or where in that order the method step of Claim 3 would fall. Second, even if the method steps have to be performed in a particular order, it is my opinion that Lin still renders Claim 3 obvious. Claim 3 depends from Claim 1 and recites “mirror[ing]” a packet to both “the second entity” and “the controller” in response to “the packet satisfying the criteria.” EX1001, Col. 11:11-

16. As such, Claim 3 narrows Limitation [1.6], the last step of Claim 1. Id. As explained in Paragraphs 119-123 of my original declaration, the narrowed requirements of Claim 3 are satisfied by the disclosure or mirroring or copying packets in Lin. EX1005, Cols. 3:25-33, 7:10-22; EX1004, ¶¶119-123.

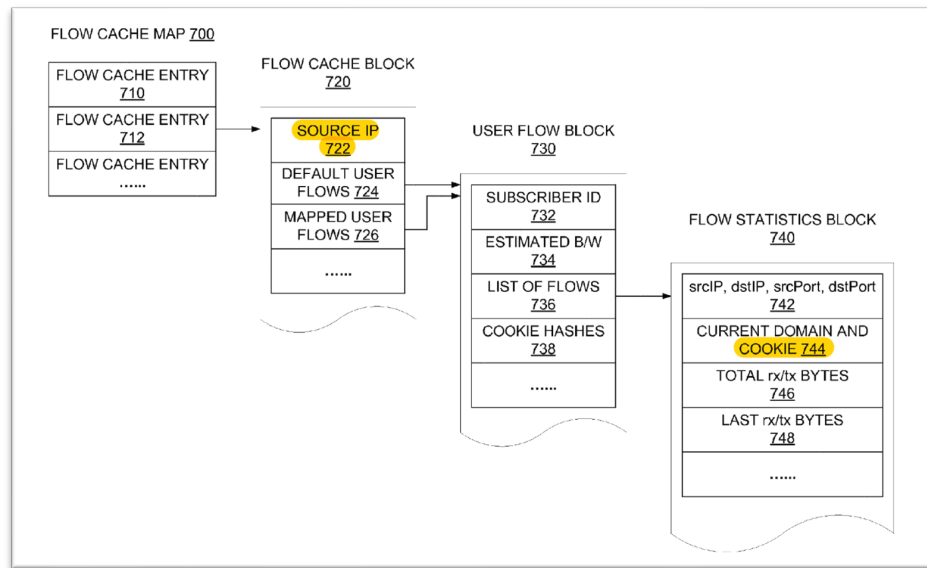
D. Claims 4 and 5

53. Paragraph 95 of the Gomez Declaration states Mr. Gomez's opinion that "claims 4 and 5 are not obvious in view of Lin for the same reasons claim 3 is not obvious in view of Lin." EX2025, ¶95. I disagree for the reasons stated in Paragraphs 119-132 of my original declaration (EX1004) and those stated above with respect to Claim 3.

E. Claim 6

54. Paragraphs 96-102 of the Gomez Declaration state Mr. Gomez's opinion that "[t]he prior art does not disclose storing *the packet* by the controller in a memory." EX2025 (heading above ¶96) (*italic emphasis in original*). Mr. Gomez argues that "Swenson's flow cache memory 322 is at most a disclosure [of] storing flow in a memory and does not suggest storing a packet in a memory," which he asserts is supported by Paragraph [0073] of Swenson. EX2025, ¶¶98-101. I disagree. First, Mr. Gomez acknowledges that a flow is stored in the cache memory 322, and a flow is comprised of packets that would be stored as part of the flow. Second, Mr. Gomez does not address that the language of Claim 6 of the '111 Patent recites

“storing the received packet *or a portion thereof*, by the controller, in a memory.” EX1001, Col. 11:31-33 (emphasis added). Swenson discloses that its flow cache memory stores at least a portion of the received packet, such as the “source IP 722” and the “cookie 744,” as shown below in Figure 7 of Swenson:



Annotated Figure 7 of Swenson (EX1007)

55. Mr. Gomez asserts that Paragraph [0073] of Swenson “does not state that an IP address is stored in the flow cache memory—paragraph 73 actually states that the ‘source IP address, subscriber ID, or other identifier’ are a basis for a hash index to retrieve the flow cache entries stored in the cache.” EX2025, ¶¶98-101, discussing EX1007, ¶[0073]. I disagree. Figure 7 of Swenson (reproduced above) shows that the IP address is stored in the flow cache memory. The fact that the IP address may also be used to create a hash index does not change that the IP address

is stored in the memory. Moreover, even if Mr. Gomez were correct that the IP address is just part of the hash index, the hash index is stored in the flow cache memory, and thus, a portion of a packet would be stored in the memory as part of the hash index.

56. Further, Mr. Gomez's analysis ignores that the Figure 7 of Swenson discloses that "cookie 744" is stored in the flow cache memory, and cookie 744 constitutes a portion of a packet. In addition, Mr. Gomez does not address that Paragraph [0084] of Swenson separately states that a flow cache entry can also store the MAC address or TCP source port associated with a received packet. EX1007, ¶[0084]. A POSA would have understood from these disclosures that Swenson teaches that the controller stores at least a portion of a packet in a flow cache memory.

F. Claim 7

57. Paragraphs 103-107 of the Gomez Declaration state Mr. Gomez's opinion that "[t]he prior art does not disclose sending 'a portion of the packet' as claimed." EX2025 (heading above ¶103). Mr. Gomez provides his opinion that "a POSA would understand that a portion of an HTTP request or response would still comprise multiple packets and would not understand a portion of an HTTP request or response to be a portion of a single packet." EX2025, ¶105; see id., ¶107. I disagree. As explained in Paragraph 137 of my original declaration, Swenson

discloses that, when its system detects a HTTP packet flow matching a particular signature, “the steering device 130 **forwards the HTTP request and a portion of the HTTP response to the network controller 140** over the ICAP client interface 404.” EX1007, ¶[0059] (emphasis added); see EX1007, ¶¶[0060], [0065], Figures 1, 4A-4B. A POSA would have understood that the reference to “a portion of the HTTP response” could refer to a portion of a packet. For example, a HTTP response can be encompassed within a single packet. In that situation, the steering device forwarding “a portion of the HTTP response” to the network controller would constitute forwarding a portion of a packet. Further, even if the HTTP response constitutes multiple packets, the steering device in Swenson could choose to forward only a portion of multiple packets, such as “a portion of the HTTP response,” to the network controller for inspection, which still renders Claim 7 obvious. This is because Swenson covers the situation where portions of each of the response packets are forwarded to the controller.

58. Mr. Gomez’s reference to Paragraph [0045] does not prove otherwise. EX2025, ¶105. The parenthetical in Paragraph [0045] of Swenson modifies the term “network traffic” by noting that network traffic can be “large object network flows.” EX1007, ¶[0045]. However, that paragraph still states that “portions of the network traffic” can be routed to the controller, and a POSA would have found it obvious

that the portion of the network traffic could have been a portion of one packet being forwarded to the network controller.

G. Claim 16

59. Paragraphs 108-110 of the Gomez Declaration state Mr. Gomez's opinion that "[t]he prior art does not disclose 'the packet comprises distinct header and payload fields, the header comprises one or more flag bits, and wherein the packet-applicable criterion is that one or more of the flag bits is set.'" EX2025 (heading above ¶108). I disagree.

60. Mr. Gomez does not challenge my opinion that it would have been well-known to any POSA as of the priority date of the '111 Patent that a packet includes distinct header and payload fields. EX1008, Section 2. Instead, Mr. Gomez asserts that "Lin does not teach a flag bit, and certainly does not teach the use of a flag bit as a condition." EX2025, ¶109. However, while Lin does not recite a flag bit, it would have been well-known to a POSA that the header field includes one or more flag bits. EX1008, Section 2. In addition, it would have been obvious to a POSA that the flow rules of Lin could have used a determination of whether or not a flag bit was set as one of Lin's "conditions" that serve as packet-applicable criterion. EX1005, Col. 4:23-31; see id., Cols. 5:8-12, 7:24-8:18; EX1004, ¶162.

61. Further, Mr. Gomez argues that "Shieh does not teach the TCP FIN flag bit being set or the TCP RST flag bit being set as a criterion." EX2025, ¶110. Shieh

discloses that the identification of TCP FIN or TCP RST packets is a packet-applicable criterion used to determine whether to route packets to the network controller for inspection. EX1006, ¶¶[0035]-[0036]. In addition, Shieh discusses the header fields in a packet and how they are used to route packets. Id., ¶[0044]. A POSA would have understood that a TCP FIN packet includes a FIN flag bit in its header that is set. Further, a POSA would have understood that a TCP RST packet includes a RST flag bit in its header that is set. It is my opinion that a POSA would have found it obvious that the TCP FIN flag bit being set or the TCP RST flag bit being set would be a way to identify TCP FIN or TCP RST packets and thus serve as the packet-applicable criterion recited in Claim 1. See EX1004, ¶280.

H. Claim 30

62. Paragraphs 111-117 of the Gomez Declaration state Mr. Gomez’s opinion that “[t]he prior art does not disclose ‘receiving...one or more additional packets’ as claimed.” EX2025 (heading above ¶111). I disagree.

63. Mr. Gomez provides his opinion that Column 6, lines 40-63 of Lin, which I cited in Paragraph 198 of my original declaration (EX1004), “does not disclose ... that the destination of the packets change between the ‘second entity’ and the ‘entity that is included in the instruction’ based on whether the additional

packet satisfies the criterion as in claim 30.” EX2025, ¶¶112-114.¹ However, I cited that portion of Lin for the limited purpose that it discloses that Lin’s method can be applied to “any packet received by the SDN switch.” EX1004, ¶198, discussing EX1005, Col. 6:40-63. Separate portions of Lin address how the destination of the packets can change based on the packet-applicable criterion disclosed in Lin, as I noted in Paragraphs 198 and 201-202 of my original declaration, which refer back to my discussion of Limitations [1.4]-[1.6] of Claim 1 of the ’111 Patent.

64. Similarly, Mr. Gomez argues that Paragraphs [0018] and [0029] of Shieh do not “disclose that the ‘subsequent packets of a particular session’ are checked for whether the criterion is satisfied, and then sent to either the ‘second entity’ or the ‘entity that is included in the instruction’ depending on whether the criterion is satisfied.” EX2025, ¶¶115-117. However, I cited Paragraphs [0018] and [0037] of Shieh for the limited purpose that they disclose that Shieh’s method can be applied to “subsequent packets of a particular session.” EX1006, ¶¶[0018], [0037]; EX1004, ¶313. Separate portions of Shieh address how the destination of the packets can change based on the packet-applicable criterion disclosed in Shieh, as I

¹ Paragraph 113 of the Gomez Declaration incorrectly cites to Column 12, Lines 59-63 of Lin. EX2025. It appears that this cite was meant to be Column 6, Lines 40-48 of Lin. EX1005.

noted in Paragraphs 313 and 316-317 of my original declaration, which refer back to my discussion of Limitations [1.4]-[1.6] of Claim 1 of the '111 Patent.

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 8th day of April, 2024.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Samrat Bhattacharjee', written over a horizontal line.

Samrat Bhattacharjee, Ph.D.