

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

PETITIONER'S REPLY TO PATENT OWNER RESPONSE

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Claim Construction.....	1
III.	The CHALLENGED Claims ARE Obvious.	2
A.	Ground 1: Lin and Swenson Render Claims 1-9, 12-24 and 27-31 Obvious.	2
1.	Lin and Swenson Disclose or Render Obvious the Claimed Controller.	2
a.	Lin discloses or renders obvious a controller configured to perform or capable of controlling DPI.	4
b.	Swenson also discloses or renders obvious a controller configured to perform or capable of controlling DPI.	7
c.	A POSA would have combined Swenson’s controller with Lin or adapted such a combination to practice the claimed controller.	11
d.	Lin discloses or renders obvious sending the packet to a second entity or an entity other than the second entity.	14
B.	Ground 2: Shieh and Swenson Render Claims 1, 5-9, 12-24 and 27-30 Obvious.	16
C.	Claims 3-5	19
D.	Claim 6	20
E.	Claim 7	22
F.	Claim 16	23
G.	Claim 30	23

I. INTRODUCTION

The Petition demonstrated Claims 1-9, 12-24 and 27-31 of the '111 Patent are unpatentable as obvious over Lin and Swenson (Ground 1) or Shieh and Swenson (Ground 2). Paper 1. Patent Owner ("PO") is unable to overcome the evidence presented by Petitioner. Instead, the Patent Owner Response ("POR") resorts to mischaracterizing the prior art and making unsupported arguments that require more from the art than is disclosed in the '111 Patent itself. These arguments cannot withstand scrutiny, and they must fail. Petitioner respectfully requests that the Board find the Challenged Claims unpatentable.

II. CLAIM CONSTRUCTION

PO submits the term "controller" should be construed consistent with a preliminary construction in the District Court Case, which was "an entity that is capable of controlling deep packet inspection." Paper 22 at 16-17. However, Petitioner's 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 the disclosure in the '111 Patent. EX1015, ¶¶11-13. 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 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.” EX1001, Col. 5:33-36; *see id.*, Cols. 5:40-59, 8:1-5, 9:67-10:1, Figures 3, 6. PO’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; EX1015, ¶13.

Regardless of whether the Board adopts either Party’s proposed constructions, or provides no claim constructions, the analysis of the unpatentability of the Challenged Claims remains the same. EX1015, ¶14.

III. THE CHALLENGED CLAIMS ARE OBVIOUS.

A. Ground 1: Lin and Swenson Render Claims 1-9, 12-24 and 27-31 Obvious.

1. Lin and Swenson Disclose or Render Obvious the Claimed Controller.

PO incorrectly asserts that neither Lin nor Swenson discloses the claimed controller. POR at 19-38; EX1015, ¶¶7-8, 10, 15-42. Lin discloses that its SDN switch 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; *see id.*, Col. 3:51-52, Figures 1, 6-8; EX1015, ¶17; Paper 1 at 8-10. Lin teaches 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; EX1015, ¶18. A POSA would have understood these disclosures in Lin to teach that the security service 630 could have been implemented using the same hardware or software as the controller, and connected to the SDN switch 620 in the same way as the controller. EX1015, ¶18; Paper 1 at 18-19.¹ 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. EX1015, ¶18; Paper 1 at 18-19.

Further, Swenson teaches the use of a controller configured to perform DPI. EX1015, ¶19. 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], Figures 1, 4A-4B. A POSA would have understood that a “flow” is a series of packets having a specific signature. EX1015, ¶19. Thus, a POSA would have known that the reference to “deep flow inspection” in Swenson refers to performing DPI on

¹ The Parties agree on the definition of a POSA and the priority date for the ’111 Patent to be used in this proceeding. EX1015, ¶¶5-6; EX1016 at 54:16-55:24.

one or more packets in a flow. *Id.* For example, a POSA would have understood Swenson’s discussion of the analysis of the “response payload” of a HTTP packet to be DPI by a DPI-capable controller. EX1007, ¶¶[0065]; EX1015, ¶19. These disclosures in Swenson demonstrate that it would have been well-known to a POSA to implement a controller configured to perform DPI analysis in a system such as Lin. EX1007, ¶¶[0026], [0028]-[0029], [0046], [0059]-[0060], [0073], [0076]-[0077], [0084]-[0086], Figures 1 and 4A-4B; EX1015, ¶19.

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

PO argues that Petitioner “concedes that Lin does not disclose a controller that is configured to perform or capable of controlling deep packet inspection [“DPI”],” but that is incorrect. POR at 20-21. While Lin discusses a separate security service 630, 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 had a reasonable expectation of success. EX1005, Cols. 3:11-12, 3:51-58, 4:8-31, Figures 1, 6-8; EX1015, ¶20.

PO acknowledges that “the security service may share certain common technical characteristics with the controller,” such as having the same physical connections (*see* EX1005, Cols. 3:11-12, 5:51-58; EX1015, ¶21), but PO nonetheless argues that there would be no reason to implement the security service in the controller. POR at 21-22. Nothing could be further from the truth. A POSA

would have understood that it would have been obvious that Lin’s security service could have been implemented as part of the controller or as a separate component. EX1015, ¶21; EX1005, Cols. 3:11-12, 3:51-58, 4:8-31, Figures 1, 6-8. PO asserts that Lin discloses that its security service is a “discrete network element” provided by “network security vendors,” but this proves nothing. POR at 22, quoting EX1005, Col. 3:11-12. Even given the existence of network security vendors, a POSA would have understood that a separate design option was to implement the security service as part of the controller, since—as is the case in Lin—implementing the security service as part of the controller would not require additional physical connections to the SDN. EX1015, ¶¶21-22. 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 it being a separate component. *Id.*, ¶22.

PO attempts to justify its argument by pointing to the ’111 Patent’s discussion of “drawbacks” of the prior art “approach of routing all traffic from network nodes to the central controller.” POR at 22-23, citing EX1001, 2:1-5. These drawbacks do not apply to Lin. EX1015, ¶23. The prior art identified in the ’111 Patent involved systems in which “*all traffic*” was routed from network nodes to the central controller. EX1001, 2:1-5 (emphasis added). That is not the case with Lin, where only specific packets meeting certain criteria are routed to the security device 630, such as routing HTTP packets. *See, e.g.*, EX1005, Cols. 5:16-24, 5:26-36, 6:1-12,

6:40-54, 7:24-8:18, Table 1; EX1015, ¶23. When only certain packets are routed to the security device, the concerns about prior art “drawbacks” fall away 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. EX1015, ¶23. 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. *Id.*, ¶24.

PO also argues that “a security service requires security resources not normally found in a controller or that would be prohibitively expensive to implement as part of the controller.” POR at 23. These arguments are unsupported and require more of the prior art than what is disclosed in the ’111 Patent. EX1015, ¶¶25-27. There is no explanation of what specific “security resources [are] not normally found in a controller.” *Id.*, ¶25. To the contrary, a POSA would have understood that a security service would require “security resources” wherever it is implemented. *Id.* For example, Swenson disclosed that its controller included “[c]onventional components” such as “security functions” and that its controller implemented deep flow inspection (“DFI”) as part of its flow analyzer. EX1007, ¶¶[0026], [0028]-[0029], [0039], [0059], [0060], [0065]. But Swenson made no mention of “security resources” that were not present in the controller. EX1015, ¶25. 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” that

would have made it difficult to achieve this task. *See, e.g.*, EX1001, 5:33-49; EX1015, ¶25.

Further, PO has not shown why it would be “prohibitively expensive to implement [the security service] as part of the controller.” EX2025, ¶55. There is no explanation as to why it would be more expensive to implement the controller and security service as one component as opposed to two components. EX1015, ¶26. Swenson does not say that it was “prohibitively expensive” to implement its “security functions” as part of its controller. EX1007, ¶[0039]. And 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. PO requires more from the prior art than it does of the ’111 Patent.

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

With respect to Swenson’s controller, PO argues that “Swenson discloses deep *flow* inspection” whereas Lin discloses “deep *packet* inspection.” POR at 23-24 (emphasis in original). PO concludes that “Lin and Swenson use different terms of art (deep packet inspection versus deep flow inspection) to disclose *different* techniques.” *Id.* at 24-25 (emphasis in original). Not true. A POSA would have known that the “deep flow inspection” in Swenson refers to performing DPI on one or more packets in a flow. EX1015, ¶28. A “flow” is a series of packets having a specific signature (EX1007, ¶[0031]), and Swenson discloses inspecting the payload

of certain packets.EX1005, ¶28. For example, Paragraph [0065] discloses that Swenson’s controller analyzes the “response payload” of a HTTP packet. This inspection of the payload of individual packets constitutes DPI by a DPI-capable controller. EX1007, ¶[0065]; *see id.*, ¶¶[0026], [0028]-[0029], [0046], [0059]-[0060], [0073]; EX1015, ¶28.

PO admits that DPI was a “well-known technique used for computer network packet filtering.” POR at 25-26. But PO goes too far, without support, in asserting that DPI “presents certain unique challenges” because it “requires significant processing power and may struggle with high-bandwidth networks or encrypted traffic.” *Id.* These “unique challenges” are not recited in the claims of the ’111 Patent or disclosed in its discussion of DPI in the specification. EX1015, ¶29; EX1001, Col. 1:20-29. Lin and Shieh likewise do not discuss any unique challenges when they disclose using DPI. EX1005, ¶[0021]; EX1006, Col. 3:11-24. Further, PO 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).” POR at 26-27 (emphasis added). PO cites no support for this speculation and provides no reason why a POSA would have been discouraged from using DPI on this basis. EX1015, ¶29.

PO notes that “[f]low data typically includes information about the IP addresses, ports and protocol types involved in a communication session.” POR at

27. That is not what is taught by Swenson, which explicitly discloses analyzing the “response payload” of HTTP packets (i.e., performing DPI). EX1007, ¶[0065]; *see id.*, ¶¶[0059]-[0060]; EX1015, ¶¶30-31. Further, PO 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.” POR at 27. That would also be true for DPI. *See* EX1005, ¶[0021]; EX1006, Cols. 3:11-24, 5:16-25; EX1001, Col. 1:20-29; EX1015, ¶31. As such, PO is incorrect to argue that “deep flow inspection is a materially different technique than deep packet inspection.” POR at 27-28.

PO asserts that “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.” POR at 27-30. But this does not evidence that DFI and DPI are materially different. EX1015, ¶32. Swenson teaches redirecting network traffic flows that meet specific criteria (such as HTTP packets) to a controller for inspection and a decision on how to act on that traffic. EX1007, ¶¶[0059]-[0060], [0065]; EX1005, ¶32. A POSA would have understood that this teaching in Swenson also applies to redirecting packets that meet specific criteria to a central controller for DPI. *Id.*, ¶32. This teaching in Swenson is not changed by the reason for inspecting the traffic (i.e. monitoring malicious activity, checking bandwidth usage or optimizing user experience). *Id.* Further, a POSA

would have understood that Swenson 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]; EX1015, ¶33.

PO argues that Swenson “does not require analyzing the message payload,” but that is incorrect. POR at 30-31. PO admits that Swenson discusses inspection of “[a] HTTP GET request header and a portion of the [HTTP] response payload.” *Id.* at 31; EX1007, ¶[0065]. However, PO asserts that in Swenson “the message does not constitute a single packet but a *flow* of packets” and “[t]he reference to a HTTP request and response ‘header’ and ‘payload’ are thus not references to the header and payload of a packet.” POR at 31-32 (emphasis in original). This is an incorrect reading of Swenson, which explicitly states that its inspection techniques include inspection of “a portion of the [HTTP] response payload.” EX1015, ¶34, discussing EX1007, ¶[0065]. A POSA would have understood that Swenson’s implementation of analysis of the “response payload” constitutes DPI by a DPI-capable controller, as DPI refers to monitoring the payload of a packet. PO cites no support for refuting this analysis. EX1015, ¶34. Notably, the ’111 Patent does not require DPI to analyze every packet in a flow, only that the system must have the ability to inspect the payload of a packet. *Id.*

PO recognizes the difficulty with its position regarding DPI in Swenson because PO 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.” POR at 32. But Petitioner’s expert has repeatedly explained that this is incorrect. EX1015, ¶35; *see id.*, ¶¶1-4. Indeed, a HTTP GET request and a HTTP response each can be encompassed in a single packet. In that situation, Swenson’s inspection of the packets containing the request or the response, including “a portion of the [HTTP] response payload,” would be DPI. EX1007, ¶[0065]; EX1015, ¶35.

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

PO also incorrectly asserts that a POSA would not have been motivated to combine the teachings of Lin and Swenson. POR at 32-38. As an initial matter, PO’s attempt to analogize this IPR to *Forest Lab’ys, LLC v. Sigmapharm Lab’ys, LLC*, 918 F.3d 928, 935 (Fed. Cir. 2019) is misplaced. *Id.* at 33. In that case, the stated motivation identified little more than a need for more drug options. In this IPR, Petitioner identified over five pages of specific reasons that the combination of Lin and Swenson leads to increased efficiency and conservation of resources in operating network systems. Paper 1 at 20-25.

Further, PO states that “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).” POR at 33-34. PO also argues that “deep packet inspection as taught in Lin is much more resource-intensive than the deep flow inspection taught in Swenson.” *Id.* at 34. These arguments fail. EX1015, ¶¶36-37. First, the pertinent teaching from Swenson is that certain network flows, which are a series of packets having a specific signature, are directed to a controller for DPI. *Id.*, ¶37. It does not matter whether the inspection is for security services (as in Lin) or for bandwidth monitoring (as in Swenson), as a POSA would have recognized the central point of having the inspection performed at the controller. *Id.*, ¶37. Second, a POSA would have understood that Swenson could analyze 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, ¶¶[0039], [0059]-[0060]; EX1015, ¶38. Third, PO’s argument that DFI is “much less taxing on the controller” than DPI is unsupported. EX1015, ¶38. Neither Swenson nor the ’111 Patent state that performing DFI or DPI at the controller were “taxing” on the controller. *Id.*

Further, PO incorrectly asserts that Swenson’s “disclosure referring to an HTTP request/response does not teach routing packets for deep packet inspection.” POR at 34-35. Swenson discloses routing certain packets (HTTP messages) to the controller for inspection and allowing other packets to proceed to their destination without being routed to the controller. EX1007, ¶¶[0059]-[0060], [0065]; EX1015, ¶39. An HTTP GET request and HTTP response each can be encompassed in a single packet; inspection of such packets constitutes DPI. EX1015, ¶39.

PO also argues that Swenson does not disclose “analyzing packets for a security function” or “send[ing] packets to the controller for DPI.” POR at 35-36. Swenson states that its controller can include “[c]onventional components” such as “security functions.” EX1007, ¶[0039]; EX1015, ¶40. PO cites 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” (POR at 35, citing EX1007, ¶[0039]), but that statement does not support PO. Swenson is simply disclosing that security functions can be included in the controller but are not shown in Figure 3 of Swenson in order to not make the figure overly detailed. EX1015, ¶40. A POSA still would have understood that these components are disclosed to be part of the controller. EX1007, ¶[0039]; EX1015, ¶40. Further, as explained above, a POSA would have known that Swenson is performing DPI at the controller, including for security reasons such as preventing DOS attacks. *See* EX1007, ¶¶[0059]-[0060],

[0065]; EX1015, ¶40. As such, PO is incorrect to argue that Swenson “focuses on network bandwidth and traffic congestion and does not pertain to network security.” POR at 36; EX1015, ¶40.

PO also cites a “drawback” of the prior art cited in the ’111 Patent to argue that Lin would not redirect packets to the controller (POR at 37), but that prior art discussed 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, where only 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. This mitigates PO’s concerns about the prior art “drawbacks.” EX1015, ¶42.

Further, contrary to PO’s assertion (POR at 37-38), a POSA would have had a reasonable expectation of success in placing the security service in the controller, just as if it was in a separate module. EX1015, ¶41; Paper 1 at 18-19. Moreover, it would not have been duplicative to have the security function in Lin’s controller (POR at 38), as there would be no need to have the separate security service 630 in that situation. EX1015, ¶41.

d. Lin discloses or renders obvious sending the packet to a second entity or an entity other than the second entity.

PO also argues that Lin does not disclose sending the packet either to a second entity or an entity other than the second entity, as required by Limitations [1.5]-[1.6]

of the '111 Patent. POR at 39-42. This is incorrect. EX1015, ¶¶43-46. PO's argument is based on the claim that "Petitioner incorrectly asserts that two separate criteria to satisfy this limitation, which is different from the requirement in Claim 1 that a single criterion must be used to make the claimed routing decision." POR at 39. PO argues 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.* at 40-42. This confuses the broader flows rules with the more narrow packet-applicable criterion within the flow rules. EX1015, ¶43. Lin teaches flow rules 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. EX1015, ¶44. 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 id.*, Col. 5:8-12. A POSA would have understood that the "one or more conditions" constitute the packet-applicable criterion because these conditions determine whether or not the packet is forwarded to the security service for inspection. EX1015, ¶44; Paper 1 at 25-26. Lin provides examples of a condition (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.

As such, the “redirect flow rule and the “bypass flow rule” operate in tandem 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”). EX1005, Cols. 7:64-8:18, Table 3; EX1015, ¶45. 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. EX1005, Cols. 7:64-8:18, Table 3. This embodiment accounts for all packets – HTTP packets are redirected and all other packets are forwarded to their destination. EX1015, ¶46.

B. Ground 2: Shieh and Swenson Render Claims 1, 5-9, 12-24 and 27-30 Obvious.

With respect to Ground 2, PO incorrectly argues that Shieh does not disclose the claimed “packet-applicable criterion.” POR at 42-46, citing Paper 8 at 18-19. PO states that “Petitioner asserts that the claimed packet-applicable criterion corresponds to Shieh[’s] disclosure of ‘the identification of ‘TCP FIN or TCP RST packets.’” *Id.* at 43. But that is not the only packet-applicable criterion identified in the Petition. The method disclosed in Shieh checks whether a packet should be

forwarded to a security processing device “based on a bypass flag.” *See* Paper 1 at 65-66, citing EX1006, ¶¶0037], Figure 7; EX1015, ¶¶9, 47-48. This bypass flag was identified as a separate example of a packet-applicable criterion. EX1015, ¶48. Shieh explains that the network access device “determine[s] whether a bypass flag [in a packet] has been set to a predetermined value” and then decides whether to forward the packet to the security device. EX1006, ¶¶0037].

Further, PO states that Shieh does not inform a POSA how to send a TCP FIN or TCP TST packet from the controller to the network switch. POR at 43-44. This is the wrong analysis by Mr. Gomez. The proper question is whether a POSA would have understood from Shieh that the controller communicates to the network access devices to use the “identification of TCP FIN or TCP RST packets” as a packet-applicable criterion to decide whether to send packets to a security service for inspection. EX1015, ¶49. Shieh provides 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 known that the network access device would use the packet-applicable criterion (i.e. the “identification of TCP FIN or TCP RST packets”) sent from the controller to determine which packets should be forwarded to the security device according to the filtering rules. *Id.*, ¶¶[0035]-[0036], [0049]; EX1015, ¶49. This allows the same

packet-applicable criterion to be applied at multiple network access devices. EX1015, ¶49. Similarly, if the packet-application criterion were determining whether a packet should be forwarded to a security service “based on a bypass flag,” a POSA would have understood that this packet-applicable criterion would be sent from a controller to one or more network access devices. *Id.*

In addition, PO states that “the alleged packet-applicable criterion (TCP FIN or TCP RST) in Shieh fails to satisfy the remaining elements of claim 1.” POR at 44-46. Not so. 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]. 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]; EX1015, ¶50. As such, Shieh teaches using “the identification of TCP FIN or TCP RST packets” to decide whether to keep forwarding packets to the security processing device for inspection or skip the security function and send the packets to their destination. EX1015, ¶50.

Shieh also teaches 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* EX1015, ¶51, discussing EX1006, ¶[0037], Figure 7. 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.*

C. Claims 3-5

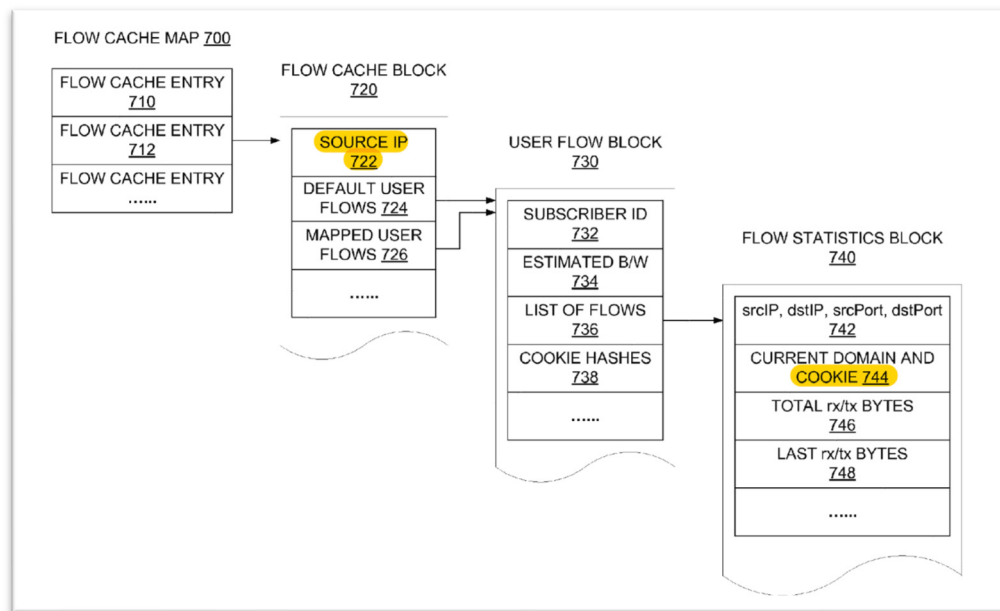
PO asserts that “[t]he prior art does not disclose sending the packet to an entity that is other than the second entity *and* to the controller.” POR at 46-49 (italic emphasis in original). This argument is premised on requiring the method steps in Claims 1 and 3 to be performed in the stated order (*id.* at 46-47), but PO has not explained what requires the steps to be performed in order. EX1015, ¶52. Further, even if the method steps must be performed in order, Lin still renders Claim 3 obvious. *Id.* 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. Claim 3 thus narrows Limitation [1.6], the last step of Claim 1. *Id.* As the Petition explained, the narrowed requirements of Claim

3 are satisfied by the disclosure of mirroring or copying packets in Lin. Paper 1 at 34-36; EX1005, Cols. 3:25-33, 7:10-22; EX1015, ¶52.

PO's arguments concerning Claims 4 and 5 fail for the same reason. EX1015, ¶53.

D. Claim 6

PO asserts that “[t]he prior art does not disclose storing *the packet* by the controller in a memory.” POR at 50-52 (italic emphasis in original). PO is wrong. As an initial matter, PO admits a flow is stored in the cache memory 322 (POR at 50), and a flow is comprised of packets that would be stored as part of the flow. EX1007, ¶[0031]; EX1015, ¶54. Further, PO's argument is flawed because Claim 6 recites “storing the received packet *or a portion thereof*, by the controller, in a memory.” EX1001, Col. 11:31-33 (emphasis added); EX1015, ¶54. Swenson discloses that its flow cache memory stores at least a portion of the received packet, such as the “source IP 722” or the “cookie 744,” as shown in Figure 7 of Swenson, reproduced below:



Annotated Figure 7 of Swenson (EX1007)

Despite PO’s argument (POR at 51-53), 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. EX1015, ¶55. Moreover, even if PO is correct that the IP address is just part of the hash index, the hash index is stored in the flow cache memory; thus, a portion of a packet would be stored in the memory as part of the hash index. *Id.*, ¶55.

Further, PO ignores that Figure 7 of Swenson discloses that “cookie 744” is stored in the flow cache memory, and the cookie constitutes a portion of a packet. *Id.*, ¶56. In addition, 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]; EX1015, ¶56.

E. Claim 7

PO argues “[t]he prior art does not disclose sending ‘a portion of the packet’ as claimed,” asserting that Swenson’s disclosure of sending “a portion of an HTTP request or response still comprises multiple packets—not a portion of a packet.” POR at 52-54. This is wrong. Swenson teaches that “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]; *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. EX1015, ¶57. A HTTP response can be encompassed within a single packet. *Id.* 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. *Id.* Further, even if the HTTP response constitutes multiple packets, the steering device in Swenson could choose to forward only a portion of multiple response packets to the network controller for inspection, which still renders Claim 7 obvious. *Id.*

PO’s reference to Paragraph [0045] of Swenson does not demonstrate otherwise. POR at 53. That paragraph states that “portions of the network traffic” can be routed to the controller, and, in view of the above discussion, 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. EX1015, ¶58.

F. Claim 16

PO does not challenge 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, PO asserts that Lin and Shieh do not teach the claimed “flag bit.” POR at 54-57. While Lin does not specifically 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; EX1015, ¶¶59-60. 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; EX1015, ¶60. Further, Shieh discusses the header fields in a packet and how they are used to route packets. EX1006, ¶[0044]. A POSA would have known that TCP FIN and TCP RST packets include a FIN flag bit and a RST flag bit in their respective headers and that those flag bits identify TCP FIN or TCP RST packets, thereby serving as packet-applicable criterion. EX1015, ¶61.

G. Claim 30

PO asserts Colum 6, Lines 40-63 of Lin and Paragraphs [0018] and [0029] of Shieh do not disclose that the destination of an additional packet changes based on whether the additional packet satisfies the packet-applicable criterion. POR at 57-59. However, this reads too much into Petitioner’s citation of those portions of Lin

and Shieh. They were cited for the limited purpose of disclosing that the respective methods of Lin and Shieh can be applied to subsequent packets. Paper 1 at 53, 73; EX1015, ¶¶62-64. Separate portions of Lin and Shieh address how the destination of the packets can change based on the packet-applicable criterion, as discussed with respect to Limitations [1.4]-[1.6]. *Id.*

Respectfully submitted,

Date: April 8, 2024

/Jeffrey D. Blake/
Jeffrey D. Blake
Registration No. 58,884

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, the undersigned attorney for the Petitioner, Cisco Systems, Inc., declares that the argument section of this reply brief has 5,542 words, according to the word count tool in Microsoft Word™.

/Jeffrey D. Blake/
Jeffrey D. Blake
Registration No. 58,884

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. §§ 42.105 and 42.6, that service was made on the Patent Owner as detailed below.

<i>Date of service</i>	April 8, 2024
<i>Manner of service</i>	Email
<i>Documents served</i>	Petitioner's Reply to Patent Owner Response; Petitioner's Updated Exhibit List; Exhibits 1015- 1016
<i>Persons served</i>	James Carmichael Stephen McBride Minghui Yang CARMICHAEL IP, PLLC Email: jim@carmichaelip.com stevemcbride@carmichaelip.com mitch@carmichaelip.com Orckit-IPRs@carmichaelip.com George Stamatopoulos Michael Ng KOBRE & KIM Email: George.Stamatopoulos@kobrekim.com Michael.Ng@kobrekim.com

/Jeffrey D. Blake/
Jeffrey D. Blake
Registration No. 58,884