

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

CISCO SYSTEMS, INC.,  
Petitioner,

v.

ORCKIT CORPORATION,  
Patent Owner.

---

Case IPR2023-00554  
U.S. Patent No. 10,652,111

---

**PATENT OWNER'S RESPONSE PURSUANT TO 37 C.F.R. § 42.120**

**TABLE OF CONTENTS**

|                                                                                                                                                                           | <b><u>Page</u></b> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>I. INTRODUCTION .....</b>                                                                                                                                              | <b>1</b>           |
| <b>II. BACKGROUND .....</b>                                                                                                                                               | <b>6</b>           |
| <b>A. Procedural History .....</b>                                                                                                                                        | <b>6</b>           |
| <b>B. Patent Owner .....</b>                                                                                                                                              | <b>6</b>           |
| <b>C. '111 Patent.....</b>                                                                                                                                                | <b>8</b>           |
| <b>1. Prosecution History .....</b>                                                                                                                                       | <b>11</b>          |
| <b>D. Petitioner's Cited References and Challenged Claims .....</b>                                                                                                       | <b>12</b>          |
| <b>1. Lin (Ex. 1005) .....</b>                                                                                                                                            | <b>13</b>          |
| <b>2. Shieh (Ex. 1006).....</b>                                                                                                                                           | <b>14</b>          |
| <b>3. Swenson (Ex. 1007) .....</b>                                                                                                                                        | <b>15</b>          |
| <b>E. Level of Ordinary Skill .....</b>                                                                                                                                   | <b>16</b>          |
| <b>III. CLAIM CONSTRUCTION.....</b>                                                                                                                                       | <b>16</b>          |
| <b>IV. NO COMBINATION OF THE CITED PRIOR ART<br/>REFERENCES TEACHES OR SUGGESTS EVERY<br/>LIMITATION OF THE CLAIMS.....</b>                                               | <b>17</b>          |
| <b>A. Claim 1: Petitioner's First Ground Fails. ....</b>                                                                                                                  | <b>19</b>          |
| <b>1. [1.0] Lin and Swenson do not disclose or render<br/>obvious the claimed controller under either Patent<br/>Owner's or Petitioner's proposed constructions. ....</b> | <b>19</b>          |

|    |                                                                                                                                                                                                                                                                 |    |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| a. | Lin does not disclose or render obvious a controller configured to perform or capable of controlling DPI.....                                                                                                                                                   | 20 |
| b. | Swenson does not disclose or render obvious a controller configured to perform or capable of controlling DPI.....                                                                                                                                               | 23 |
| c. | A POSA would not have combined Swenson’s controller with Lin’s or adapted such a combination to practice the claimed controller in Lin’s system in any event.....                                                                                               | 32 |
| 2. | [1.5] – [1.6]: Lin does not disclose 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.” ..... | 39 |
| B. | Claim 1: Petitioner’s Ground 2 fails.....                                                                                                                                                                                                                       | 42 |
| 1. | 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.....                                                             | 42 |
| C. | Claim 3: The prior art does not disclose sending the packet to an entity that is other than the second entity <i>and</i> to the <i>controller</i> .....                                                                                                         | 46 |
| D. | Claims 4 and 5: The prior art does not disclose sending the packet to an entity that is other than the second entity <i>and</i> to the <i>controller</i> .....                                                                                                  | 49 |
| E. | Claim 6: The prior art does not disclose storing <i>the packet</i> by the controller in a memory .....                                                                                                                                                          | 50 |
| F. | Claim 7: The prior art does not disclose sending “a portion of the packet” as claimed .....                                                                                                                                                                     | 52 |

**G. Claim 16: The 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” .....54**

**H. Claim 30: The prior art does not disclose “receiving...one or more additional packets” as claimed .....57**

**V. CONCLUSION .....59**

**TABLE OF AUTHORITIES**

|                                                                                                       | <b>Page(s)</b> |
|-------------------------------------------------------------------------------------------------------|----------------|
| <b>Cases</b>                                                                                          |                |
| <i>Arendi SARL v. Apple Inc.</i> ,<br>832 F.3d 1355 (Fed. Cir. 2016) .....                            | 56             |
| <i>DSS Tech. Mgmt. Inc. v. Apple Inc.</i> ,<br>885 F.3d 1367 (Fed. Cir. 2018) .....                   | 55             |
| <i>Forest Lab’ys, LLC v. Sigmapharm Lab’ys, LLC</i> ,<br>918 F.3d 928 (Fed. Cir. 2019) .....          | 33             |
| <i>Mformation Tech. v. Research in Motion Ltd.</i> ,<br>764 F.3d 1392 (Fed. Cir. 2014) .....          | 46, 48, 49     |
| <i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> ,<br>851 F.3d 1270 (Fed. Cir. 2017) ..... | 55             |
| <i>Realtime Data, LLC v. Iancu</i> ,<br>912 F.3d 1368 (Fed. Cir. 2019) .....                          | 16             |
| <i>Samsung Elecs. Co., Ltd. v. Elm 3DS Innovations, LLC</i> ,<br>925 F.3d 1373 (Fed. Cir. 2019) ..... | 34             |
| <b>Statutes</b>                                                                                       |                |
| 35 U.S.C. § 103 .....                                                                                 | 11             |
| <b>Agency Decisions</b>                                                                               |                |
| <i>Xerox Corp. et al. v. Bytemark, Inc.</i> ,<br>IPR2022-00624, Paper 12 (PTAB Feb. 10, 2023) .....   | 43             |

| EXHIBIT LIST |                                                                                                                                                                                                                                                                                                                                                             |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2001         | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 46 (E.D. Tex., Jan. 15, 2023), First Amended Docket Control Order (“First Amended Docket Control Order”)                                                                                                                                                                |
| 2002         | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 28 (E.D. Tex., Nov. 4, 2022), Notice of Compliance (“11-4-2022 Notice of Compliance”)                                                                                                                                                                                   |
| 2003         | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 47 (E.D. Tex., Jan. 19, 2023), Notice of Compliance (“1-19-2023 Notice of Compliance”)                                                                                                                                                                                  |
| 2004         | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 55 (E.D. Tex., Mar. 23, 2023), Defendant’s Motion To Stay                                                                                                                                                                                                               |
| 2005         | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 56 (E.D. Tex., Mar. 29, 2023), Order Denying Motion to Stay                                                                                                                                                                                                             |
| 2006         | United States District Courts National Judicial Caseload Profile For the 12 Months Ending March 31, 2023 (available at <a href="https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0331.2023.pdf">https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0331.2023.pdf</a> ) (“Judicial Caseload Statistics”) |
| 2007         | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 50 (E.D. Tex., Feb. 3, 2023), Notice of Compliance (“2-3-2023 Notice of Compliance”)                                                                                                                                                                                    |
| 2008         | Reserved                                                                                                                                                                                                                                                                                                                                                    |
| 2009         | December 11, 2008 Final Rejection (U.S. Appl. No. 11/123,801) (“’801 Application Final Rejection”)                                                                                                                                                                                                                                                          |
| 2010         | July 28, 2008 Claim Amendments (U.S. Appl. No. 11/123,801) (“’801 Application Pending Claims”)                                                                                                                                                                                                                                                              |
| 2011         | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 59 (E.D. Tex., Mar. 30, 2023), Order Granting Motion To Amend Invalidity Contentions                                                                                                                                                                                    |
| 2012         | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 61 (E.D. Tex., April 13, 2023), Order Granting Motion To Amend Invalidity Contentions                                                                                                                                                                                   |
| 2013         | “About Orckit-Corrigent: Executive Summary,” 2011                                                                                                                                                                                                                                                                                                           |

|      |                                                                                                                                                                                                                                                                                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2014 | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (Cover Pleading)                                                                                                                                                                                                  |
| 2015 | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (Exhibit A - ’904 Patent Charts)                                                                                                                                                                                  |
| 2016 | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (Exhibit B - ’821 Patent Charts)                                                                                                                                                                                  |
| 2017 | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (Exhibit C - ’740 Patent Charts)                                                                                                                                                                                  |
| 2018 | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (Exhibit D - ’111 Patent Charts)                                                                                                                                                                                  |
| 2019 | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (Exhibit E - Combination Charts)                                                                                                                                                                                  |
| 2020 | <i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (SME Contentions)                                                                                                                                                                                                 |
| 2021 | United States District Courts National Judicial Caseload Profile For the 12 Months Ending December 31, 2022 (available at <a href="https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile1231.2022.pdf">https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile1231.2022.pdf</a> ) (“December 22 Judicial Caseload Statistics”) |
| 2022 | Declaration of George Stamatopoulos in support of Patent Owner’s Motion for Pro Hac Vic Admission                                                                                                                                                                                                                                                                          |
| 2023 | Declaration of Michael Ng in support of Patent Owner’s Motion for Pro Hac Vice Admission                                                                                                                                                                                                                                                                                   |
| 2024 | Stipulation of Dismissal                                                                                                                                                                                                                                                                                                                                                   |
| 2025 | Declaration of Miguel Gomez                                                                                                                                                                                                                                                                                                                                                |
| 2026 | CV of Miguel Gomez                                                                                                                                                                                                                                                                                                                                                         |
| 2027 | “DPI & DFI: A Malicious Behavior Detection Method Combining Deep Packet Inspection and Deep Flow Inspection” by Guo et al., <i>Procedia Engineering</i> 174, 1309-1314 (2017)                                                                                                                                                                                              |

## I. INTRODUCTION

Orckit Corporation (“Orckit” or “Patent Owner”) submits this Patent Owner Response (“POR”) to Cisco Systems, Inc.’s (“Petitioner”) Petition challenging claims 1-9, 12-24, and 27-31 (the “Challenged Claims”) of U.S. Patent No. 10,652,111 (the “’111 Patent”).

The ’111 Patent is directed to novel methods for implementing deep packet inspection (“DPI”) in software defined networks (“SDN”). The ’111 patent explains that protocols used in software defined networks (*e.g.*, the OpenFlow protocol) allowed the programmability of network nodes (*e.g.*, switches or routers) by a central controller but failed to provide a mechanism for deep packet inspection, a technique that was useful among other things for detecting security threats. *See* Ex. 1001, 1:50-67. The patent explains further that routing all packets from the network nodes to the central controller had a number of drawbacks, including “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.* at 2:1-6. The inventors of the ’111 Patent recognized a need to “provide a solution that overcomes the deficiencies [of prior art SDN protocols and allowed for] efficient DPI in SDNs.” *Id.* at 2:7-9. The claims of the ’111 Patent recite methods that are directed to such a solution.

Among other elements, the sole challenged independent claim of the '111 Patent (claim 1) recites: (i) a SDN “controller” that is capable of controlling deep packet inspection<sup>1</sup> and (ii) the use of a criterion (a “packet-applicable criterion”) to determine whether packets transmitted over a SDN network should be sent to their destination or to some other entity (e.g., the controller itself) for further inspection. The remaining Challenged Claims, all of which depend from Claim 1) recite additional limitations, for example, about the criterion to be used or the specific entities to which packets should be sent in response to satisfying or not satisfying the claimed “packet-applicable criterion.”

The inventive crux of these claims was a novel SDN in which: (i) the SDN controller, unlike prior art SDN controllers (that were typically uninvolved in DPI but were dedicated to other network functions), was also capable of controlling DPI; *and* (ii) a criterion handed down by the controller to the nodes was used to intelligently determine whether and when to send packets to their destination and when to divert them for further inspection with DPI. These two elements in tandem

---

<sup>1</sup> As discussed below, the parties have advanced competing constructions for the claimed “controller.” However, Patent Owner’s arguments in this response are the same under either construction (i.e., Patent Owner’s construction as “an entity capable of controlling deep packet inspection” or Petitioner’s “entity configured to perform deep packet inspection on packets”).

were critical in the inventors' efforts to address the limitations in prior art SDNs discussed in the patent.

Petitioner has advanced two grounds challenging the patentability of the Challenged Claims: first, that the Challenged Claims are obvious over Lin in view of Swenson and, second, that the Challenged Claims are obvious over Shieh in view of Swenson. With respect to Petitioner's second ground (Shieh over Swenson), as the Institution Decision already determined, there is no reasonable basis to conclude that Shieh and Swenson invalidate any claim because Shieh and Swenson do not disclose or render obvious the claimed "packet-applicable criterion." With respect to Petitioner's first ground (Lin over Swenson), Patent Owner respectfully submits new arguments--that were not previously before the Board and are supported by the declaration of Patent Owner's expert—which show that the Challenged Claims are patentable over the Lin/Swenson combination.

As explained in detail below, among other limitations, the Lin and Swenson combination does not disclose or render obvious a controller that is capable of controlling deep packet inspection or the use of the claimed packet-applicable criterion for sending individual packets to an entity other than their original destination.

In particular, Lin discloses a less sophisticated system in which DPI is performed at a dedicated security service that is distinct from the controller and provided by “security vendors.” And, because it teaches performing DPI as part of a discrete security service, Lin does not disclose or render obvious a controller that is capable of controlling DPI.

Petitioner attempts to overcome this lack of disclosure in Lin by identifying references in Swenson to a network controller executing a technique called “deep flow inspection.” Effectively, Petitioner asserts that (i) deep flow inspection is coextensive or would otherwise render obvious deep packet inspection; and (ii) because Swenson teaches deep *flow* inspection at the controller, it also renders obvious a controller that is capable of controlling (or configured to perform, under Petitioner’s proposed construction) deep *packet* inspection. Petitioner’s assertion is incorrect if not misleading. As explained below, despite their similar-sounding names, deep *packet* inspection and deep *flow* inspection are different techniques that perform different functions. Deep packet inspection is a granular and thorough inspection of traffic at the packet level. Owing to its granularity, it is well-suited among other things to threat detection and security applications stemming, e.g., from maliciously sent packets. On the other hand, deep *flow* inspection—which is focused on traffic monitoring at the flow level—can be used for obtaining and

analyzing statistic information about data flows, but does not lend itself to inspecting data at the packet level. Indeed, Swenson discloses using deep flow inspection in connection with “the analysis of the statistic information of the data flow” to make forecasts about bandwidth in connection with facilitating user requests for content in service provider networks. Ex. 1007, Abstract. Moreover, Swenson expressly omits from its disclosure details about “security functions” so as not to “obscure the details of [its] system architecture.” Ex. 1007, [0039]. Accordingly, as also explained below, a POSA would not understand Swenson to disclose DPI at all, let alone a controller that is either capable of controlling or configured to perform DPI. In any event, even if Swenson disclosed DPI (it does not) there is no reference or teaching anywhere in the art that would provide a POSA with a reason to combine Swenson with Lin. Accordingly, Lin and Swenson do not disclose or render obvious independent claim 1.

Moreover, for reasons set forth below, the dependent claims recite additional patentable elements that are not obvious in view of Lin or Shieh and Swenson. Accordingly, Patent Owner respectfully asks that the Board issue a Final Written Decision finding all challenged claims patentable over the asserted prior art.

## **II. BACKGROUND**

### **A. Procedural History**

This proceeding is one of four IPRs filed by Petitioner against Patent Owner. The other IPRs are IPR2023-00401 (U.S. Pat. No. 7,545,740), IPR2023-00402 (U.S. Pat. No. 8,830,821) and IPR2023-00714 (U.S. Pat. No. 6,680,904). Each of the '740, '821, '111 and '904 Patents was asserted by Patent Owner against Petitioner in *Orckit Corporation v. Cisco Systems, Inc.*, Case No. 2:22-cv-00276 (E.D. Tex. July 22, 2022) (the "District Court Case"). Patent Owner and Petitioner have agreed to a jointly stipulated dismissal of the district court litigation without prejudice. Ex. 2024 [Stipulation of Dismissal].

### **B. Patent Owner**

Orckit Corporation owns the '111 patent, which originated from significant research and development by Orckit Communications Ltd. (also known as Corrigent-Systems Ltd., referred to herein as "Orckit-Corrigent").

Orckit-Corrigent was founded in 1990 in Israel by Izhak Tamir and Eric Paneth. Orckit-Corrigent's products offered networking infrastructure for the delivery of residential, business, and mobile backhauling services in packet-based networks.

By the early 2000s, Orckit-Corrigent was a pioneer in telecommunications, with revenues some years exceeding \$500M from sales to various tier 1 global telecommunications providers. Over the years, Orckit-Corrigent and its subsidiaries developed and sold products in a variety of telecommunications areas, including DSL, Packet Transport Networks (PTN), Carrier Ethernet technologies, PWE (Pseudo-Wire Emulation) technology, and Resilient Packet Ring (RPR) technology, which was developed and introduced to the market as the IEEE 802.17 Standard, part of the company's packet transport technology. In 2007, Orckit-Corrigent launched its CM4000 PTN line of products, which were purchased and deployed by telecom providers worldwide, including leading Indian carrier Bharat Sanchar Nigam Ltd. (BSNL); T-Systems (Deutsche Telekom) in Germany; Tele2, a leading Pan-European Scandinavian Service Provider; redIT (formerly MetroNet) in Mexico, and others. At one time, Orckit-Corrigent had offices in Israel, US, India, Japan, Korea, Germany, Russia, Brazil, Mexico, Thailand, and the Philippines.

Orckit-Corrigent also engaged in extensive research and development (investing over \$200M) and prosecuted an extensive patent portfolio. Many of the patents in this portfolio were practiced by its products, notably, the CM-4000 product family, which was a series of packet transport network switches (consisting of, among other products, the CM-4140, CM-4206 and CM-4314T/4314 models),

and the CM-401x portfolio of switches that included the CM-4011, CM-4012 and CM-4013 products. Ex. 2014 [Orckit-Corrigent Executive Summary].

In 2012, Orckit-Corrigent entered into debt restructuring/bankruptcy proceedings in Israel. After a series of transactions that followed the Israel proceedings, Orckit Corporation acquired a smaller set of Orckit-Corrigent's patents, including the '111 patent.

### **C. '111 Patent**

The '111 Patent is titled "Method and System for Deep Packet Inspection in Software Defined Networks." Ex. 1001, abstract. DPI is a technique for examining network communications at the packet level, which can be used to extract data patterns from a data communication channel. Ex. 1001, 1:21-25. The extracted data patterns are useful for a variety of purposes, including network security and data analytics. *Id.*

A software defined network (SDN) is a networking architecture that provides for centralized management of the nodes in a network, as opposed to the distributed architecture utilized by conventional networks. Ex. 1001, 1:30-38. For example, a SDN may utilize a controller to manage network nodes such as vSwitches. *Id.* SDN-based architectures typically decouple the data forwarding (*e.g.* data plane) from control decisions (*e.g.* control plane), such as routing, resources, and other

management functionalities. Ex. 1001, 1:39-49. The decoupling may allow the data plane and the control plane to operate on different hardware, in different runtime environments, and/or operate using different models. *Id.*

The inventors of the '111 Patent recognized that the OpenFlow protocol used by prior art did not support DPI of packets through the various networking layers. Ex. 1001, 1:50-67. This limited the ability of the OpenFlow protocol to support a number of networking features associated with DPI, including detecting security threats. *Id.* The inventors also recognized that “routing all traffic from network nodes to the central controller introduces some significant drawbacks, such as 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.* at 2:1-6. The inventors thus explain that “it would be advantageous to provide a solution that overcomes the deficiencies [in prior art SDNs] and allow[s] efficient DPI in SDNs.” *Id.* at 2:7-9. The '111 Patent proposes methods for DPI in a software defined network. Ex. 1001, 2:27-3:3. In one exemplary embodiment, a network system 100 as shown in Fig. 1 includes a controller 111 “configured to perform deep packet inspection on designated packets from designated flows or TCP sessions... the central controller 111 is further configured to instruct each of the network nodes 112 which of the packets and/or

sessions should be directed to the controller 111 for packet inspections:”

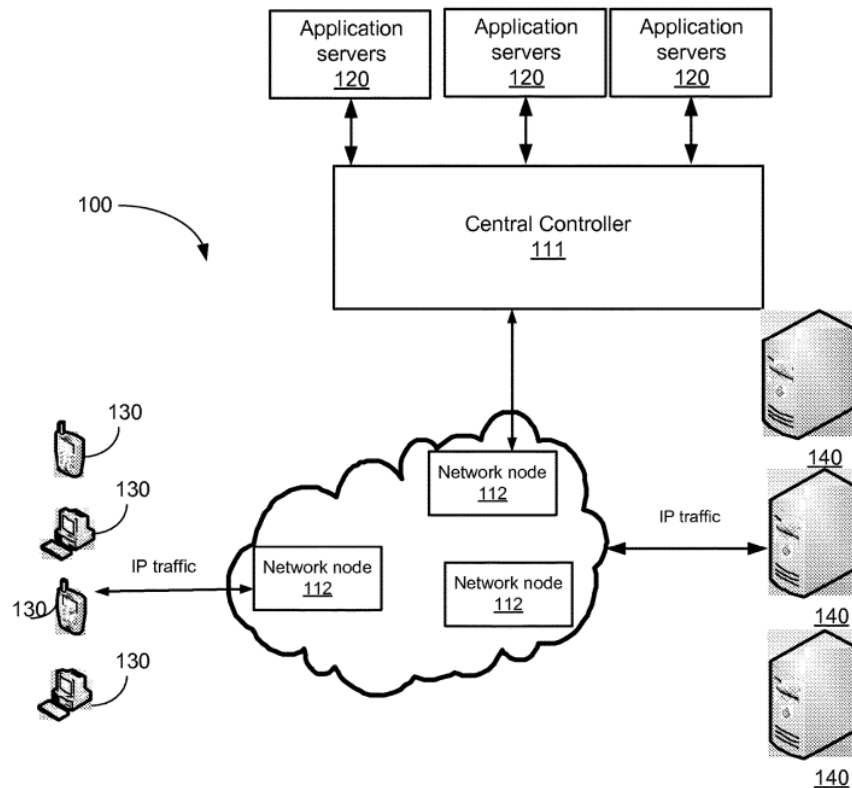


FIG. 1

Ex. 1001, 4:5-11, Fig. 1.

Controller 111 may provide instructions to the network nodes that configure the network nodes to analyze the headers of incoming packets for DPI. Ex. 1001, 4:23-37. For example, the network node may be instructed to either redirect the packet to controller 111 or send the packet to the destination server 140. *Id.* Alternatively, the controller 111 may instruct the network nodes to mirror a number

of bytes within the packet to be sent to controller 111 to perform DPI. *Id.* The TCP packet's header may include fields such as TCP FLAG SYN, TCP FLAG ACK, TCP FLAG FIN, TCP FLAG RST, which are analyzed by the network node to execute the instructions sent by the controller, which may vary depending on the contents of the TCP packet's header field. Ex. 1001, 4:23-46.

The '111 Patent has two independent claims (1 and 32) and 52 dependent claims, of which only independent claim 1 and a subset of its dependent claims are at issue in this proceeding. Consistent with the description in the '111 Patent, the claims recite a method for transporting packets based on an instruction and a packet-applicable criterion sent from a controller to a network node (claim 1) for performing DPI (claim 9).

### **1. Prosecution History**

The '111 Patent claims priority to provisional application no. 61/982,358, filed on April 22, 2014. Ex. 1001 ['111 Patent], 1:8-10. The '111 Patent was filed on April 21, 2015 as Appl. No. 15/126,288 (the "'288 Application"). *Id.*

On September 12, 2018, the Examiner issued a non-final rejection rejecting the then-pending claims under 35 U.S.C. § 103 over U.S. Pub. No. 2010/0208590 (Dolganow) and U.S. Pub. No. 2014/0052836 (Nguyen), which was made final on April 15, 2019 following an Applicant response on December 9, 2018. Ex. 1002,

170-195, 230-238, 240-263.

In response to the rejections, Applicant on May 7, 2019 amended the claims to explicitly recite that the controller “is external to the network node,” thus clarifying that the instruction and packet-applicable criterion are sent by the controller to the network node over the packet network. Ex. 1002, 148-168.

On July 8, 2019, the Examiner issued a new rejection substituting Nguyen with U.S. Pub. No. 2016/0219080 (Huang). The Examiner subsequently withdrew the rejection and allowed the claims following Applicant’s October 2, 2019 response to the Examiner’s July 8, 2019 Office Action. Ex. 1002, 15-16, 55-64. The Examiner’s January 7, 2020 Notice of Allowance credited the arguments made by Applicant’s October 2, 2019 response, including that the prior art failed to disclose “sending, by the controller to the network node over the packet network, an instruction and a packet-applicable criterion” because the prior art “only described receiving packets as part of the regular traffic to be analyzed, and are silent regarding any receiving from a controller in general, and receiving of ‘the instruction and the criterion’ in particular.” Ex. 1002, 15-16, 62-64.

The ’288 Application issued as the ’111 Patent on May 12, 2020. Ex. 1001.

#### **D. Petitioner’s Cited References and Challenged Claims**

The Petition asserts the following two grounds:

| Ground | Claims                   | Basis                                           |
|--------|--------------------------|-------------------------------------------------|
| #1     | 1-9, 12-24, and 27-31    | 35 U.S.C. § 103 (AIA)<br>over Lin and Swenson   |
| #2     | 1, 5-9, 12-24, and 27-30 | 35 U.S.C. § 103 (AIA)<br>over Shieh and Swenson |

Paper 1, i-iii. Petitioner alternatively relies on Lin or Shieh as the primary reference, and Swenson as the secondary reference in both cases.

**1. Lin (Ex. 1005)**

U.S. Patent No. 9,264,400 to Lin et al. (“Lin”) is titled “Software Defined Networking Pipe for Network Traffic Inspection” and describes a software defined networking (SDN) computer network including an SDN controller and an SDN switch. Ex. 1005, abstract. The 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. *Id.*

Specifically, Lin utilizes an SDN Controller 610 (which may be an OpenFlow Controller) that controls the behavior of the SDN computer network 600 as shown in Fig. 6:

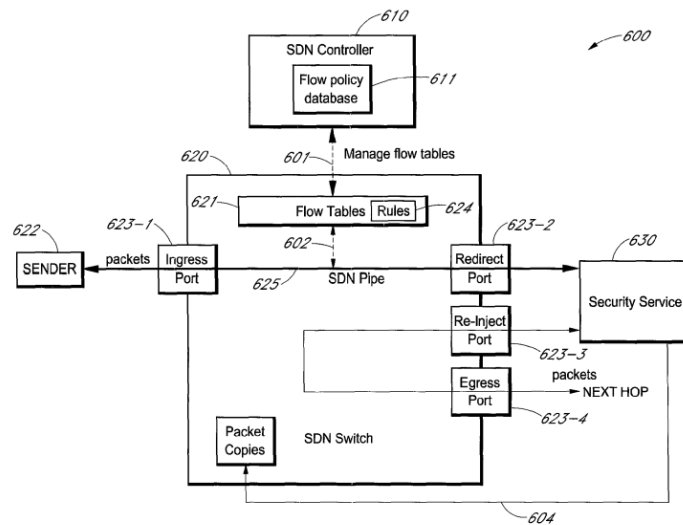


FIG. 6

Ex. 1005, 3:40-52, Fig. 6.

The SDN controller may include a flow policy database 611. *Id.* The flow policy database comprises flow policies that are enforced by the controller 610 on network traffic transmitted over the SDN computer network 600 and may specify security policies that govern transmission of packets on the network. *Id.* Flow policies in database 611 are implemented in terms of flow rules 624 that are stored in flow tables 621 of the SDN switch 620. Ex. 1005, 4:19-31. “The SDN controller 610 may insert flow rules in the flow tables 621.” Ex. 1005, 6:1-3.

## 2. Shieh (Ex. 1006)

U.S. Pat. Pub. No. 2013/0291088 to Shieh et al. (“Shieh”) is titled “Cooperative Network Security Inspection” and describes a network system

including a security device and a network access device. Ex. 1006, abstract. The network access device receives a packet from a source node of the network and determines whether the packet should be routed to a destination node or forwarded to a security device. Ex. 1006, [0037]. The network access device makes this determination based on whether a bypass flag in a session table stored on the network access device is set to a predetermined value or not. *Id.* If the bypass flag is the predetermined value, the packet is forwarded to the security device. *Id.* Otherwise, the packet is routed to the destination node. *Id.* The bypass flag may be received from the security device, such as to indicate that the security device no longer wishes to receive further packets for security inspection. Ex. 1006, [0030].

### **3. Swenson (Ex. 1007)**

U.S. Pat. Pub. No. 2013/0322242 to Swenson et al. (“Swenson”) is titled “Real-Time Network Monitoring and Subscriber Identification with an On-Demand Appliance” and describes a system and method for selectively monitoring traffic in a service provider network. Ex. 1007, abstract. A user device 110 accesses a network via a steering device 130. Ex. 1007, [0026]. A network controller 140 interfaces with steering device 130 to coordinate the monitoring and categorization of network traffic. *Id.* The network controller provides selective real-time network monitoring and subscriber identification and monitors large flows in the network, collects flow

statistics, and selects flows to be optimized. Ex. 1007, [0039-0040]. The network controller may monitor and optimize flow based on historical traffic data for the average of the bandwidth per user at a particular cell tower to estimate the amount of bandwidth or degree of congestion for the new flow based on the historical record. Ex. 1007, [0029].

#### **E. Level of Ordinary Skill**

The Institution Decision adopted Petitioner's level of ordinary skill. DI, 11-12. For purposes of this Patent Owner Response, Patent Owner does not dispute Petitioner's level of ordinary skill.

### **III. CLAIM CONSTRUCTION**

Although the Petition proposed constructions for “controller” and “instruction,” the Institution Decision “determine[d] that no terms need to be construed at this time. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’”).

Relevant to this Patent Owner Response, the Court in the District Court Case preliminarily construed the term “controller” as “an entity that is capable of controlling deep packet inspection,” and the parties submitted their proposed constructions on the papers without further argument. Notably, the parties stipulated

jointly to a dismissal of the District Court Case before the Court issued a decision on claim construction.

Patent Owner 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.” Petitioner has proposed that “controller” be construed as “an entity configured to perform deep packet inspection on packets.” As explained below, Patent Owner’s arguments are materially the same under either competing construction; thus, they do not turn on the Board resolving the parties’ dispute concerning the construction of “controller.” Accordingly, though the Board should take into account the limitations acknowledged by both parties in connection with the appropriate construction of “controller”—and whether this claim element is met or rendered obvious by Petitioner’s prior art references—it is not necessary for the Board to choose between the two competing constructions of “controller” for purposes of issuing a final written decision.

#### **IV. NO COMBINATION OF THE CITED PRIOR ART REFERENCES TEACHES OR SUGGESTS EVERY LIMITATION OF THE CLAIMS**

As discussed below, Lin and Shieh do not render independent claim 1 in light of Swenson. First, Lin and Swenson do not teach or suggest the limitation in claim 1 of a “controller” under either Petitioner’s or Patent Owner’s proposed constructions (i.e., “an entity configured to perform DPI” or “an entity capable of

performing DPI”). Lin discloses a system in which DPI is performed in a dedicated security service that is distinct from the Lin’s controller; Swenson does not disclose DPI; and a POSA would neither combine the two references nor adapt any resulting combination to practice the claimed “controller” (i.e., a controller capable of controlling DPI or configured to perform DPI). Further, Lin does not disclose the use of a single “packet-applicable criterion” in connection with sending a packet to a second entity or sending a packet to an entity that is other than the second entity; rather, Lin discloses using different conditions in connection with the claimed sending steps. Second, as the Board already found in its Institution Decision, Shieh fails to disclose or render obvious in light of Swenson the claimed “packet-applicable criterion.” Finally, as discussed below, the dependent claims are separately patentable over Lin, Shieh, and Swenson.

**A. Claim 1:<sup>2</sup> Petitioner’s First Ground Fails.**

**1. [1.0] Lin and Swenson do not disclose or render obvious the claimed controller under either Patent Owner’s or Petitioner’s proposed constructions.**

Petitioner asserts that the claimed “controller is an entity configured to perform deep packet inspection on packets” and “[t]he combination of Lin and Swenson discloses such a controller.” Pet., 18. In particular, Petitioner contends that either (i) it would have been obvious to a POSA to implement the security service of Lin as part of Lin’s controller, notwithstanding that Lin discloses the security service as a separate entity 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. As discussed below, Petitioner is wrong as to each of these assertions, because first, Lin does not disclose a controller that is configured to perform (or capable of controlling<sup>3</sup>) DPI, second, Swenson

---

<sup>2</sup> All claims at issue depend from claim 1. Thus, Patent Owner’s arguments advanced with respect to claim 1 also apply to those claims.

<sup>3</sup> As discussed *supra*, Patent Owner advances a construction for “controller” as “an entity capable of controlling deep packet inspection,” consistent with the

likewise does not disclose such a controller, and third, a POSA in any event would not have been motivated to combine Lin and Swenson to practice this limitation in the manner required by claim 1.

**a. Lin does not disclose or render obvious a controller configured to perform or capable of controlling DPI.**

Petitioner concedes that Lin does not disclose a controller that is configured to perform or capable of controlling deep packet inspection. As Petitioner admits, “Lin states that the analysis performed by *security service 630 includes DPI*.” Pet., 18. Further, as shown in the figures excerpted from Lin, the security service 630 is a separate entity from the controller 610:

---

preliminary construction of the Court in the District Court Case. Given that the arguments set forth in this response apply equally under either construction, the Board need not decide between Patent Owner’s and Petitioner’s competing constructions for present purposes.

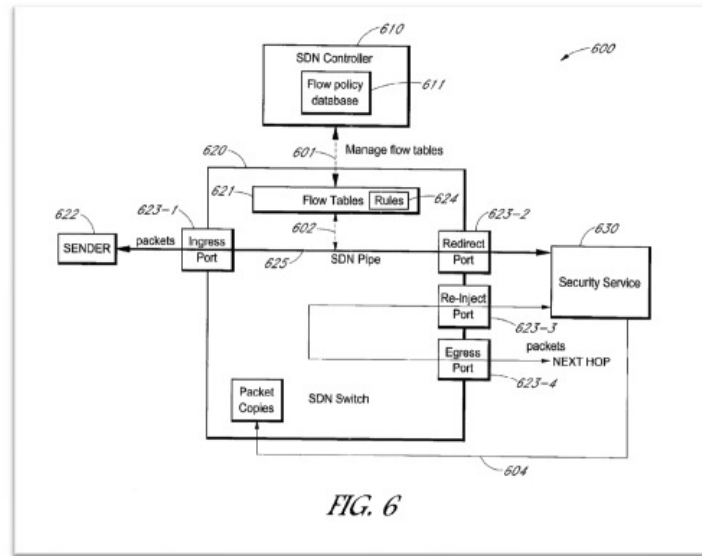


Figure 6 of Lin

Petitioner asserts that a POSA would nevertheless “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.” Pet., 18-19. Petitioner makes this assertion based on disclosures in Lin that the security service “can use 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.” Pet., 18. This assertion has no merit. Ex. 2025, ¶¶52-55.

The 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). *Id.*, ¶¶54-55. Lin itself suggests that the security service is not only a discrete network element from the controller but that specific “[n]etwork security vendors provide network security services, such as firewall or deep packet inspection (DPI)” (Ex. 1005, 3:11-12)—not the controller (or the network administrators responsible for configuring the controller). Lin also teaches that “to provide network security services, packets of network traffic are intercepted for inspection [by] plac[ing] the security service in the middle of the packet forwarding path.” *Id.* at 12-16. Lin’s disclosures that packets are routed for inspection to an entity that is entirely discrete from the controller are consistent with the ’111 patent’s teachings that the “straightforward approach of routing all traffic from network nodes to the central controller introduces some significant drawbacks, such as 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.” Ex. 1001, 2:1-5. As the ’111 Patent makes clear, it was known in the prior art that performing DPI at the controller presented material challenges and disadvantages, precisely the types of issues that

the '111 patent seeks to address. Ex. 2025, ¶¶54-55. Lin's disclosure of a security service for performing DPI that was separate from the SDN controller mirrors the disclosures in the '111 Patent about the difficulties of utilizing the controller in carrying out DPI. *Id.*

Indeed, as explained by Patent Owner's expert, the reason that security services were not—prior to the '111 patent—normally combined with a controller is 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. Ex. 2025, ¶55.

Accordingly, a POSA would not have had reason to implement the security service in Lin as part of Lin's controller, nor a reasonable expectation of success in doing so. Ex. 2025, ¶¶52-55. In any event, Petitioner and its expert have failed to identify any reason as to why a POSA would have done so.

**b. Swenson does not disclose or render obvious a controller configured to perform or capable of controlling DPI.<sup>4</sup>**

Petitioner attempts to overcome Lin's lack of disclosure of the claimed controller (i.e., an entity configured to perform or capable of performing deep packet

---

<sup>4</sup> The arguments advanced here with respect to Swenson also apply to Petitioner's second ground with respect to the Shieh/Swenson combination.

inspection, under Petitioner’s or Patent Owner’s competing constructions, respectively) by contending that Swenson “teaches the use of a controller configured to perform DPI.” Pet., 19. Petitioner’s contention is predicated upon a series of incorrect assertions concerning Swenson’s disclosure. Ex. 2025, ¶¶56-69.

Petitioner points to Swenson’s “flow analyzer 312” that performs “deep flow inspection to determine if the flow is worth bandwidth monitoring and/or user detection” to assert that a “POSA would have known that a ‘flow’ is a series of packets” and “[a]s such, it would have been obvious to a POSA that Swenson’s reference to ‘deep flow inspection’ refers to performing DPI in one or more packets in a flow.” Pet., 19. Petitioner’s assertion is incorrect if not misleading. Ex. 2025, ¶¶56-69.

As an initial matter, in contrast to Lin’s disclosure of deep *packet* inspection performed at a dedicated security service, Swenson discloses deep *flow* inspection performed in the flow analyzer of a network controller. Ex. 2025, ¶57. On their face, Lin and Swenson use different terms of art (deep packet inspection versus deep flow inspection) to disclose *different* techniques. *Id.* As Patent Owner’s expert explains, flows convey information that is relevant to different aspects of network monitoring than the information conveyed by individual packets. Ex. 2025, ¶¶60-61. In particular, inspection of flows conveys information about the state of the network

that is not conveyed by individual packets. *Id.* Thus, Petitioner’s assertion (*i.e.*, that flows contain packets, and therefore deep flow inspection is somehow synonymous or coextensive with deep packet inspection) is simply incorrect. Ex. 2025, ¶¶57-62.

A POSA would easily understand that deep *flow* inspection is simply not the same as deep *packet* inspection, that the two techniques entail material differences, and that deep packet inspection entails unique technical capabilities and challenges that distinguish it from deep flow inspection. Ex. 2025, ¶¶57-62. Accordingly, a POSA would know that (i) it would not be possible simply to combine a controller performing deep flow inspection (e.g., Swenson’s controller) with a network in which deep packet inspection is performed in a dedicated security service that is discrete from the controller (e.g., Lin’s network) to practice the claimed invention, and (ii) that Swenson’s controller is not configured to perform (or capable of controlling) deep packet inspection. Ex. 2025, ¶¶62, 64-66.

Patent Owner’s expert explains some of these differences in detail. Ex. 2025, ¶¶57-66. **Deep Packet Inspection** (or “DPI”) is well-known technique used for computer network packet filtering that may examine a packet payload (*i.e.*, the part of the packet that contains content relevant to an application, such as an email message or audio/video content) and in some instances the packet header, as a packet is transmitted through an inspection point (e.g., a node, controller, or security

device). Ex. 2025, ¶¶58-59. Networks use DPI for a number of purposes that include protocol non-compliance, viruses, spam, intrusions, or other defined criteria applicable to the packet. *Id.* On the basis of DPI, networks then decide whether particular data packets (and possibly the flows associated with those packets) should be routed to the destination to which they are addressed or some other destination, or alternatively, whether the packets should be dropped entirely. *Id.* DPI is a thorough inspection process that can be utilized for a variety of purposes, which include inspecting and managing network traffic, enforcing network security (e.g., by blocking malware or illegal content). *Id.* As Patent Owner's expert explains, DPI devices are capable of looking at Layer 2 and beyond Layer 3 of the OSI model, and can even analyze up to Layer 7. *Id.* DPI thus offers control of network traffic that goes beyond classification of packets based on header information and can be used in enterprise security to detect various attacks, including buffer overflow attacks or data leaks. *Id.*

DPI also presents certain unique challenges. Ex. 2025, ¶59. Because it is a thorough packet inspection technique, DPI requires significant processing power and may struggle with high-bandwidth networks or encrypted traffic. *Id.* Further, 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). *Id.* In such scenarios, less granular metadata analysis techniques may be deployed to overcome certain limitations of DPI by giving a more comprehensive view of the entire network, without being affected by limitations that inhere in DPI. *Id.*

On the other hand, **Deep Flow Inspection** (DFI), is a less well-known technique that—in general—refers to a type of network monitoring focused on the flow of data within the network rather than the inspection of individual packets. Ex. 2025, ¶¶60-61. Flow data typically includes information about the IP addresses, ports, and protocol types involved in a communication session, as well as metrics like the number of bytes and packets transferred. *Id.* DFI can be used for purposes like traffic analysis, network performance monitoring, and the detection of unusual or suspicious behavior patterns in network traffic. *Id.*

In summary, a POSA would have known that DPI inspects the detailed contents of individual packets in a granular, thorough manner; and, in contrast, DFI focuses on the broader patterns of network traffic flows by looking at aggregate data flow characteristics. Ex. 2025, ¶62.

This understanding—*i.e.*, that deep flow inspection is a materially different technique than deep packet inspection—is consistent with Swenson’s disclosures of a system geared toward bandwidth and user experience optimization through the use

of statistic information relating to flows, not the inspection of packet contents. Ex. 2025, ¶63. Examples of these disclosures in Swenson are excerpted below:

- The system then determines whether to monitor the data flow from the origin server to the user device. If so determined, *the system collects statistic information of the data flow* and *stores the statistic information* to a flow record in a database. The system also maps the flow record to a subscriber of the service provider network by *analyzing the statistic information of the data flow and estimates bandwidth provided to the data flow by the service provider's network based on the analysis of the statistic information of the data flow*. Ex. 1007, abstract.
- The disclosure generally relates to improving user experience on a network, and more specifically, to monitoring bandwidth consumption of the many devices connected to a given node in the network. Ex. 1007, [0003].
- Embodiments disclosed include a network controller system for real-time data gathering on the state of existing data network traffic flows and mapping flow data to respective users in the

network to predict available bandwidth and level of congestion. By gathering a history of flow statistics in the network, the network controller system establishes a relationship between base stations (or other network segments) and their capability to deliver the amount of data typically required by a particular user of the network. The very recent history of network flows can be used to predict the near future congestions in a substantially real-time fashion. Furthermore, the history of flow statistics can be used to build a long-term map of user behavior on the network, which can more effectively predict on demand data delivery requirements for the collection of users utilizing a given network access point in a consistent manner. The network controller keeps a flow state database, which groups flow data in a number of ways, such as on per station/cell tower, per subscriber, per time-of-day, or per geography area basis. As new flows are presented to the system for inspection, database can be queried to estimate the network congestion level for new flows to determine whether existing, new or future flows require

optimizations in order to maintain the desired level of user satisfaction. Ex. 1007, [0018].

Thus, as Patent Owner's expert explains, it is clear from Swenson that deep *flow* inspection is simply not the same as deep *packet* inspection. Ex. 2025, ¶¶57-66. Petitioner's assertion that flows are "series of packets having a specific signature" cannot bridge the gap between deep flow and deep packet inspection such that a POSA would glean from Swenson a controller that is configured to perform deep packet inspection. Ex. 2025, ¶66. Indeed, for the purposes of Swenson's traffic analysis, DPI would have little use due to the higher overhead it would impose upon the Swenson system as a whole. *Id.*

To shore up its assertion that Swenson discloses a controller configured to perform (or capable of controlling) DPI, Petitioner further asserts that a POSA would understand Swenson's discussion of a controller that "inspects the message" including a HTTP request header and payload portion received from a steering device "to determine whether to monitor the flow or optimize the video" to refer to "DPI by a DPI-capable controller, as DPI refers to monitoring the payload of a packet." Pet., 19. Again, this is incorrect. Ex. 2025, ¶¶67-69.

First, Swenson's disclosure of the controller analyzing a message does not require analyzing the message payload. Indeed, on its face, Swenson says nothing

of the sort; rather, Swenson says that the message is inspected without stating that the message payload is also analyzed. Ex. 2025, ¶¶67-69. Second, even assuming the message inspection did include message payload inspection, Petitioner has not explained whether and why analysis for any purpose of a payload necessarily constitutes DPI. Swenson's disclosure—which is geared toward flow monitoring rather than individual packet monitoring—nowhere suggests that the controller analyzes an individual packet payload or—even if it did—that such an analysis would constitute DPI. Ex. 2025, ¶¶67-69. Third, Swenson discloses that the steering device 130 “sends an ICAP request message 516 comprising [a] HTTP GET request header and a portion of the [HTTP] response payload to the network controller 140, which inspects the message to determine whether to monitor the flow or optimize the video.” Ex. 1007, [0065]. In the context of a HTTP GET request and response, as disclosed in Swenson, the message does not constitute a single packet but a *flow* of packets. Ex. 2025, ¶¶67-69. The reference to a HTTP request and response “header” and “payload” are thus not references to the header and payload of a packet. *Id.* Indeed, a POSA would know that despite common parlance references to “HTTP packets,” HTTP is a higher-level protocol that does not pertain to individual packets. *Id.* Rather, packet transmission is governed by the TCP protocol. HTTP utilizes TCP to exchange data such that information may be used by an end user (e.g., a

video or audio stream). *Id.* Thus, even 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 but at the flow level and thus does not constitute deep packet inspection. Ex. 2025, ¶69.

In short, Swenson does not disclose deep packet inspection, let alone a controller that performs, is capable of performing, or is capable of controlling deep packet inspection. Thus, even if a POSA were motivated to combine Swenson with Lin, the resulting combination would not practice the claimed controller.

**c. A POSA would not have combined Swenson’s controller with Lin’s or adapted such a combination to practice the claimed controller in Lin’s system in any event.**

Petitioner contends that “[a] POSA would have been motivated to combine the teachings of Lin and Swenson” to practice the claimed controller. Pet., 20. For the reasons explained below, even assuming 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), a POSA would not have combined Swenson’s controller with Lin’s system. Ex. 2025, ¶¶71-76.

Petitioner asserts that Lin and Swenson are analogous references that address the same technology and attempt to resolve the same issues relating to routing traffic in an efficient manner and conserving network resources. Pet., 20. This assertion

fails as a matter of law. Pet., 20. These generic needs—i.e., efficiency and conservation of resources—are precisely the type of generic need that the Federal Circuit has previously held insufficient to provide a motivation to combine prior art references. *See Forest Lab’ys, LLC v. Sigmapharm Lab’ys, LLC*, 918 F.3d 928, 935 (Fed. Cir. 2019) (“a generic need for more antipsychotic treatment options did not provide a motivation to combine these particular prior art elements”). Petitioner has failed to allege any specific reason for which a POSA would have combined Lin with Swenson to produce a more efficient system. And, having failed to provide such a specific reason, Petitioner’s assertions that a POSA would have combined Lin and Swenson for efficiency’s sake fails as a matter of law.

Petitioner’s assertion that each Lin and Swenson “use a central controller to provide instructions and packet-applicable criterion to network nodes to determine which packets should be redirected and which packets can be sent directly to a destination node” likewise fails. Pet., 20. As an initial matter, Petitioner does not point to any disclosures in Swenson about a packet-applicable criterion used to make packet-based routing decisions. Ex. 2025, ¶7. Accordingly, Petitioner’s argument fails for this reason alone. But even assuming Swenson disclosed a packet-applicable criterion, 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 an altogether different device in Lin (the security service). *Id.* Given that deep packet inspection as taught in Lin is much more resource-intensive than the deep flow inspection taught in Swenson, a POSA would not have been motivated to adapt Lin in accordance with Swenson to execute deep packet inspection (which Lin expressly teaches is conducted by specialized “security vendors”) in the SDN controller responsible for managing the SDN control plane. *Id.* In any event, Petitioner merely asserts that Lin and Swenson could be combined without providing any specific reason as to why a POSA *would* combine the two references. *See, e.g., Samsung Elecs. Co., Ltd. v. Elm 3DS Innovations, LLC*, 925 F.3d 1373, 1383 (Fed. Cir. 2019) (holding that in a complex field, “...specific evidence that a person of ordinary skill in the art would have reasonably expected success in combining...” prior art elements is required).

Petitioner incorrectly asserts that “[l]ike Lin, Swenson teaches that only certain packets are redirected to the controller in order to be efficient in analyzing packets of interest.” Pet., 21. This is incorrect if not misleading. Ex. 2025, ¶72 Swenson teaches forwarding an “HTTP request and a portion of the HTTP response to the network controller 140 over the ICAP client interface 404.” Ex. 1007, [0060]. But as discussed above, the disclosure referring to an HTTP request/response does

not teach routing packets for deep packet inspection; rather, it refers to directing HTTP messages—which can consist of numerous packets—to the controller for analysis of that message, rather than deep inspection of any individual packet. Ex. 2025, ¶72. Accordingly, a POSA would not glean from Swenson’s disclosure of deep flow inspection at the controller that it is also possible to conduct DPI at the controller, as Petitioner asserts. *Id.*

Petitioner further asserts that a POSA would have understood that Swenson, like Lin, could involve analyzing packets for a security function. Pet., 21. Elsewhere, Petitioner asserts that Swenson discloses “send[ing] packets to the controller for DPI.” Pet., 24. Again, these assertions are incorrect, if not misleading. Ex. 2025, ¶73. Swenson states that in “other embodiments, the network controller 140 may include additional, fewer, or different components for various applications ... [for example, conventional] components such as network interfaces, security functions, failover servers, management and network operations consoles,” which “are *not shown so as to not obscure the details of the system architecture.*” Ex. 1007, [0039] (emphasis added). On its face—and far from disclosing specific techniques for inspecting packets or security, such as DPI—Swenson expressly omits technical details pertaining to security (such as DPI or how DPI might be conducted in the context of a SDN) from its disclosure because they are *irrelevant*

to its system and would only serve to *obscure* the details of its system. Ex. 2025, ¶73.

Indeed, Swenson’s focus on high-level statistical analysis of network traffic patterns—as opposed to granular, packet-based analysis such as DPI—is evident from its disclosure that in certain embodiments “the bandwidth attained by a single flow may be sufficient to determine the capacity of the network segment(s) the flow traverses” such that a “fairly small deployment of network controller(s)” is sufficient for obtaining “an accurate detection of key network congestion points” without a “need to monitor every flow going through a network segment to detect congestions.” Ex. 1007, [0021]. It is thus evident 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. Ex. 2025, ¶74. Contrary to Petitioner’s assertions, Swenson’s acknowledgement that a controller may include conventional components for security is a far cry from disclosing a controller that is capable of DPI or that would warrant incorporation of a function as complex and taxing as DPI into another system, let alone a system such as Lin, which expressly teaches the use of a dedicated security apparatus, wholly divorced from the SDN controller, to perform DPI. *Id.*

Petitioner’s assertion that “Lin and Swenson each teach that only certain packets may need to be redirected for further processing before being sent to the destination node” (Pet., 23) is likewise misleading. As explained *supra*, Lin expressly teaches performing DPI at a dedicated security service that is divorced from the controller—which is consistent with the ’111 patent’s disclosure discussed *supra* that performing DPI at the controller was a known drawback in the prior art prior. Ex. 2025, ¶75. Further, Swenson is not focused on DPI at all, and expressly *omits* controller-based security functions like DPI. *Id.* Accordingly, other than a generic need for efficiency—which is insufficient as a matter of law to provide a motivation to combine—Petitioner has not identified anything in Lin, Swenson, or the prior art that would lead a POSA either to combine Lin and Swenson or to otherwise practice the claimed controller (i.e., a controller configured to perform or capable of controlling DPI).

Lastly, Petitioner’s assertion that a POSA would have had a reasonable expectation of success in modifying Lin to implement the disclosure of Swenson to route packets to the central controller for inspection also fails. *See* Pet., 24. Petitioner asserts—without any explanation or support—that “[i]f Swenson could be constructed to have the network nodes send packets to the central controller for security inspection, a POSA would have understood that the same arrangement could

be implemented in Lin.” Pet 24-25. But as discussed *supra*, Swenson, unlike Lin, is not directed to network security or to DPI. Ex. 2025, ¶76. Further, the ’111 patent teaches that utilizing the controller to perform security functions such as DPI was known in the art to present challenges. *See supra*. Thus, absent some other teaching (Petitioner has not identified such a teaching), a POSA would not have expected that it would be possible to practice the claimed controller in Lin by utilizing Swenson’s approach of performing deep flow inspection at the controller, particularly given that Swenson expressly states that it is not concerned with security applications, *i.e.*, the types of applications on which Lin is focused. Ex. 2025, ¶76.

In any event, 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. Performing DPI at the controller would thus be duplicative of a function already performed in Lin. Accordingly, a POSA would not be motivated to adapt Lin to provide a controller configured to perform (or capable of controlling) the resource-intensive DPI function.

Accordingly, even assuming that Swenson disclosed the claimed controller, Petitioner has failed to demonstrate that a POSA would combine Swenson and Lin to practice the claimed controller in Lin.

2. **[1.5] – [1.6]: Lin does not disclose 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.”**

Claim 1 requires (i) “receiving, by the network node from the controller, the instruction and the criterion” (*see* Pet., 30 (limitation 1.2); ’111 patent, Claim 1); (ii) “responsive to the packet not satisfying the criterion, sending, by the network node over the packet network, the packet to the second entity” (*see* Pet., 30 (limitation 1.5); ’111 patent, Claim 1); or (iii) “responsive to the packet satisfying the criterion, sending the packet, by the network node over the packet network, to an entity that is included in the instruction and is other than the second entity” (*see* Pet., 30 (limitation 1.6); ’111 patent, Claim 1). On its face, Claim 1 requires a routing decision—*i.e.*, whether to send the packet to the second entity to which it is addressed or to a different entity—based on whether the packet satisfies the criterion received “by the network node from the controller.”

As explained below, Petitioner incorrectly asserts that two separate criteria 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 (*i.e.*, based on whether that criterion is satisfied or not satisfied). Ex. 2025, ¶¶77-83.

Petitioner first points to the condition used by Lin’s “bypass flow rules” as the criterion responsive to which Lin’s SDN switch sends the packet to the second entity. Pet., 31. In particular, Petitioner cites Lin’s Table 3 (reproduced as annotated by Petitioner below), in which “the bottom two rows are bypass flow rules for all packets:”

| TABLE 3          |     |        |              |              |     |               |       |
|------------------|-----|--------|--------------|--------------|-----|---------------|-------|
| IN_PORT          | ... | IP src | TCP src port | TCP dst port | ... | Action        | Count |
| Ingress_port_ID  | *   | *      | *            | 80           | *   | Redirect port | 10    |
| Redirect_port_ID | *   | *      | 80           | *            | *   | Ingress port  | 10    |
| Ingress_port_ID  | *   | *      | *            | *            | *   | Egress port   | 130   |
| Egress_port_ID   | *   | *      | *            | *            | *   | Ingress port  | 130   |

**Table 3 of Lin (Annotated)**

A POSA would understand from Lin’s disclosure that the bypass flow rules are set such that “packets bypass the SDN pipe, and are accordingly not inspected by the security service 630” if they do not indicate a TCP source or destination port. Ex. 2025, ¶79.

Petitioner incorrectly asserts that this same criterion is used in connection with “sending the packet, by the network node over the packet network, to an entity that is included in the instruction and is other than the second entity.” Pet., 32-33. In the same example given in Table 3, Lin makes clear that a different criterion is used in

connection with sending packets to its security service. Ex. 2025, ¶80. As Lin explains, “the top two rows are redirect flow rules for redirecting HTTP packets to the security service 630 for inspection,” and the criterion employed in connection with the “redirect flow rules” is the packet’s specific TCP source or destination address, in this example (shown in Petitioner’s annotated Table 3), port 80:

| TABLE 3          |     |        |              |              |     |               |       |
|------------------|-----|--------|--------------|--------------|-----|---------------|-------|
| IN_PORT          | ... | IP src | TCP src port | TCP dst port | ... | Action        | Count |
| Ingress_port_ID  | *   | *      | *            | 80           | *   | Redirect port | 10    |
| Redirect_port_ID | *   | *      | 80           | *            | *   | Ingress port  | 10    |
| Ingress_port_ID  | *   | *      | *            | *            | *   | Egress port   | 130   |
| Egress_port_ID   | *   | *      | *            | *            | *   | Ingress port  | 130   |

**Table 3 of Lin (Annotated)**

Critically, Lin does not teach how a packet is sent if either the bypass flow rule and redirect flow rule conditions are both not satisfied. Ex. 2025, ¶82. Rather, Lin’s rule tables only govern how a packet is sent if a particular condition is satisfied, as is evident from Lin’s discussion of the importance of rule priority in its table. Ex. 1005, 8:1-17. That is, Lin teaches that conditions are executed only if they are stated explicitly and does not teach actions to be taken on a packet if conditions are not satisfied or not explicitly stated. Ex. 2025, ¶82.

A POSA would immediately understand that Lin uses two different criteria: one criterion for sending a packet to the security service (which Petitioner identifies as the claimed “entity that is other than the second entity”) and a separate criterion for sending the packet to the second entity. Ex. 2025, ¶83. Lin’s conditions are thus different than the claimed “packet-applicable criterion” (and the step of sending the packet to different entities in response to satisfying or not satisfying that criterion) in claim 1. Accordingly, and given that Petitioner has not asserted that this limitation is somehow rendered obvious by Lin or any other asserted reference, ground 1 fails for this reason alone.

**B. Claim 1:<sup>5</sup> Petitioner’s Ground 2 fails**

- 1. 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.**

As the Institution Decision already determined, there is no reasonable basis to conclude that Shieh and Swenson invalidate any claim because Swenson does not disclose a “packet-applicable criterion.” Paper 8, 18-19.

---

<sup>5</sup> All claims at issue depend from claim 1. Thus, Patent Owner’s arguments advanced with respect to claim 1 also apply to those claims.

Petitioner asserts that the claimed packet-applicable criterion corresponds to Shieh disclosure of “the identification of ‘TCP FIN or TCP RST packets’” that Petitioner alleges is used to “determine which packets should be forwarded to the security device pursuant to the filtering rules.” Pet., 62-63. Petitioner’s assertion is incorrect. Ex. 2025, ¶¶84-89.

First, as Petitioner concedes, “Shieh does not state whether these criterion [sic] are sent from a controller to the network access devices.” Paper 1, 62. To overcome this deficiency, Petitioner asserts that “a POSA would have understood that the packet-applicable criterion would be sent from a controller to one or more network access devices.” *Id.* In support, the Petition cites paragraph 224 of the Bhattacharjee Declaration, which simply repeats this assertion verbatim without any underlying factual support and thus is entitled to little weight. *Xerox Corp. et al. v. Bytemark, Inc.*, IPR2022-00624, Paper 12 (PTAB Feb. 10, 2023). Petitioner and its expert offer no explanation for how a POSA would modify Shieh to send a TCP FIN or TCP TST packet—which Shieh describes as being sent by the network source node and received by the network switch as part of the “packet stream” (Ex. 1006, [0036])—from the controller to the network switch. There likewise is no explanation for why a TCP FIN or TCP TST packet would originate from the controller as required by Petitioner’s modification rather than from a source node as

disclosed by Shieh. Again, there is simply no evidence, besides Petitioner's conclusory arguments and Petitioner's expert's conclusory testimony, that it would have been obvious to do so.

Second, 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. Ex. 2025, ¶¶87-89. Claim 1 states that the packet is sent to different destinations based on whether or not the criterion is satisfied. In contrast, Shieh discloses that packet destinations are determined by the bypass flag stored in the session table of the network switch, which the Petition has not alleged to be a packet-applicable criterion in element 1.1. Ex. 1007, [0037]; Paper 1, 62-63.

Shieh clearly discloses that the bypass flag used to determine destination addresses is separate from the TCP FIN or TCP RST packet that the Petition alleges is the packet-applicable criterion. *Compare* Ex. 1006, [0037] ("[D]evice 272 may look up in its session table such as the one as shown in FIG. 5 to determine whether a bypass flag has been set to a predetermined value. If the bypass flag matches the predetermined value, the packet is forwarded to the security device 273 via path 282;

otherwise, the packet is routed to destination node 274.”) with Ex. 1006, [0036] (“During 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...”).

The Petition conflates the TCP FIN and TCP RST packets, which Shieh discloses are “special events in the packet stream” that produce notifications to the security-processing function (Ex. 1006, [0029]), with the bypass flag stored in the session table of the network switch that flags packets to be sent to the security device for inspection (Ex. 1006, [0030], [0037]). Ex. 2025, ¶¶87-89. Shieh explicitly teaches that (i) the bypass flag is stored in the session table of the network switch (Ex. 1007, [0037]) (“device 272 may look up in its session table such as the one as shown in FIG. 5 to determine whether a bypass flag has been set to a predetermined value. If the bypass flag matches the predetermined value, the packet is forwarded to security device 273 via path 282; otherwise, the packet is routed to destination node 274”)); and (ii) the TCP FIN and TCP RST are packets received by the network switch from the source node. Ex. 1006, [0031, 0036] (“[W]hen a security-processing function (e.g., processing node 211A) receives the packets, it does the security inspection and security policy enforcement...During 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...”). Shieh thus makes clear that the bypass flag is different from the TCP FIN or TCP RST packets. Ex. 2025, ¶¶87-89. Given that the Petition alleges that the claimed actions are taken based on the flags—rather than the TCP FIN or TCP RST packets, which the Petition alleges are the criterion—the Petition has failed to allege that packet destinations are determined in response to the criterion being met, as required by the claims.

Thus, the Petition has not demonstrated that Shieh discloses sending a packet-applicable criterion.<sup>6</sup> Accordingly, the Board should find that Claim 1 is patentable over Shieh and Swenson.

**C. Claim 3: The prior art does not disclose sending the packet to an entity that is other than the second entity *and* to the controller**

Claim 1 recites a series of steps that are performed in the order written. *Mformation Tech. v. Research in Motion Ltd.*, 764 F.3d 1392, 1398-99 (Fed. Cir. 2014) (holding that claim language, as a matter of logic and grammar, “requires that the steps be performed in the order written”). The controller must send the instruction and packet-applicable criterion (the first element) before the network

---

<sup>6</sup> In addition, for similar reasons as those set forth in connection with Lin and Swenson, Shieh in combination with Swenson does not disclose or render obvious the claimed controller.

node receives it (the second element). The network node must receive the criterion (the second element) before it checks whether the packet satisfies the criterion (the third element). The fourth element is “*responsive* to the packet not satisfying the criterion” while the fifth element is “*responsive* to the packet satisfying the criterion”; thus, elements four and five must occur after the third, checking, element. Dependent claim 3 then requires an additional step of “sending the packet...to the second entity and to the controller,” in addition to the five steps of claim 1. Thus, the Petition must show two separate steps “responsive to the packet satisfying the criterion” in the prior art combination: (1) “sending the packet...to an entity that is included in the instruction and is other than the second entity” and (2) “sending the packet...to the second entity and to the controller.”

The Petition has not shown that the prior art performs these two separate steps in the order recited. Ex. 2025, ¶¶90-94. The Petition states that Lin sends the packet to an entity that is other than the second entity on the basis of Lin’s disclosure that the packet is sent to the security device: “Lin states that, if a packet satisfies this criterion (i.e., the packet indicates that port 80 is the source or destination port), then the SDN switch (which corresponds to the claimed network node) sends the packet over the packet network to the security device (which corresponds to the claimed entity that is included in the instruction and is other than the second entity).” Pet.,

32. But the Petition also asserts that Lin sends the packet to the controller based on the same disclosure of sending the packet to the security device: “Lin teaches that the mirror instruction instructs that ‘the SDN switch 620 may be configured to copy packets that are redirected to the security service 630 for inspection’ and to ‘forward the copied packets to their destinations.’ As discussed above for Element [1.6], it would have been obvious to implement the security service 630 in Lin as part of the controller; thus, the original packet would be sent to the controller by the SDN switch and a copy of the packet is sent to the destination node.” Pet., 35-36 (citations omitted). Thus, the Petition at most asserts that Lin sends a packet once to the controller (as discussed *supra*, Lin does not contain such a disclosure). Ex. 2025, ¶¶90-94. Even if it were true, Petitioner’s assertion is insufficient to satisfy an order of steps that separately sends the packet (1) to an entity other than the second entity *and* (2) to the controller as required by claims 1 and 3. See *Mformation*, 764 F.3d at 1398-99.

**D. Claims 4 and 5:<sup>7</sup> The prior art does not disclose sending the packet to an entity that is other than the second entity *and* to the controller**

Petitioner's theory with respect to claims 4 and 5 fail for the same reason as for claim 3. In addition to the step of "sending the packet...to an entity that...is other than the second entity" as in claim 1, both claims 4 and 5 require the further step of "sending the packet to the controller." Ex. 2025, ¶95. The Petition, however, relies on the assertion that the packets is sent to the controller once to assert that two required steps are met: sending the packet to the controller (which as discussed *supra*, is not disclosed by Lin) *and* sending the packet to an entity that is other than the second entity. This is insufficient to satisfy an order of steps that separately sends the packet (1) to an entity other than the second entity and (2) to the controller. *See Mformation*, 764 F.3d at 1398-99.

---

<sup>7</sup> Claims 6, 7, and 9 depend from claim 5. Thus, Patent Owner's arguments advanced with respect to claim 5 also apply to those claims. Further, claims 12-15 depend from claim 9. Thus, the arguments advanced with respect to claim 9 also apply to those claims.

**E. Claim 6: The prior art does not disclose storing *the packet* by the controller in a memory**

Claim 6 requires that a *packet* or a portion of a *packet* be stored in a memory. The Petition alleges claim 6 is obvious over Swenson because “Swenson discloses a flow cache memory 322.” Pet., 40, 66. Petitioner’s argument is flawed because it once again conflates a packet and a flow. Ex. 2025, ¶¶96-102. As explained in Section IV(A)(a)(ii), a POSA would understand that a packet is an individual, granular unit of data whereas a flow is an aggregate of the data traffic and not granularized to any individual packet. Thus, as explained above, deep packet inspection refers to examining a packet payload whereas deep flow inspection refers to monitoring the flow of data.

This distinction is important here because Swenson’s flow cache memory 322 is directed to caching *flow* data and not individual packets or portions of packets as the Petition alleges. Ex. 2025, ¶¶96-102. According to the Petition, Swenson paragraph 73 describes storing a portion of a packet: “In discussing Figure 7, Swenson states that the flow cache entry stores at least a portion of the received packet, including at least the IP address of the received packet. *Id.*, ¶[0073] (discussing Figure 7).” Pet., 40. Contrary to Petitioner’s representations, however, Swenson paragraph 73 (fully reproduced as follows) says nothing about caching

packets—instead, it explicitly states that it stores “flow cache entries indexed by a hash”:

FIG. 7 is a block diagram illustrating one embodiment of an example of internal components of the flow cache. The flow cache map 700 comprises a plurality of flow cache entries, such as flow cache entries 710 and 712 indexed by a hash. Not shown in the example diagram is a possible linked list behind each flow cache entry which allows chaining of flow cache entries for a given hash index. The hash into the flow cache may be based on source IP address, MAC address, subscriber ID, or other identifier indicative of a given subscriber, group of subscribers or subscriber's device.

Ex. 1007, [0073]. While the Petition alleges that the flow cache memory stores “the IP address of the received packet,” Swenson paragraph 73 (upon which Petitioner relies for this assertion) does not state that the IP address is stored in the cache—rather, it states that the “source IP address, MAC address, subscriber ID, or other identifier” are a basis for a hash index to retrieve the flow cache entries stored in the cache. Nothing in paragraph 73 states an IP address is stored in the flow cache memory. Rather, paragraph 76 states that the flow cache memory stores a list of flows associated with subscriber IDs and flow statistics such as the number of bytes in either direction. Ex. 1007, [0076]. Paragraph 84 then states that the MAC address

or TCP source port is the address or source port of the flow—not the payload of an individual packet.

A POSA would understand from these disclosures that Swenson’s flow cache stores flow data and not packets or portions of a packet. Ex. 2025, ¶¶96-102. The addresses cited by the Petition correspond to a source of a flow, and Swenson contains no disclosure that any packet or portion of a packet is stored in the flow cache. *Id.*

**F. Claim 7:<sup>8</sup> The prior art does not disclose sending “a portion of the packet” as claimed**

Claim 7 requires “sending a portion of the packet...to the controller.” A POSA would understand that a portion of a packet is less than the whole packet; thus, claim 7 requires sending less than a whole packet to the controller. Ex. 2025, ¶¶103-107.

The Petition alleges that “Swenson teaches that the network node sends a portion of a packet to the controller” because “Swenson discloses that...the steering device 130 forwards the HTTP request and a portion of the HTTP response to the network controller 140.” Pet., 40. Petitioner’s argument fails however because it

---

<sup>8</sup> Claim 8 depends from claim 7. Thus, Patent Owner’s arguments advanced with respect to claim 7 also apply to that claims.

conflates a portion of a packet as claimed and a portion of an HTTP request or response. Ex. 2025, ¶¶103-107. A POSA would understand that a packet is an individual, granular unit of data. *Id.* A POSA would further understand that an HTTP request or response is not a single packet but rather many packets. *Id.* Thus, a portion of an HTTP request or response still comprises multiple packets—not a portion of a packet. *Id.*

This is supported by Swenson itself, which describes the steering device as routing “portions of network traffic” (i.e., a series of packets), rather than a portion of an individual packet:

The steering device interface 316 interacts with an external routing appliance, such as the steering device 130 to divert **portions of the network traffic (e.g., large object network flows)**...

Ex. 1007, [0045].

Even more tellingly, the Petition consistently states that Swenson sends “a portion of a HTTP response”:

The 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.” A POSA would have understood that the steering device corresponds to at least part of the claimed network node, and the signature that is compared to the

HTTP packet flow corresponds to the claimed criterion. Further, a POSA would have understood that, responsive to the HTTP packet flow satisfying that criterion, the steering device applies an instruction pursuant to which **a portion of a HTTP request or a portion of a HTTP response** is sent to the network controller.

Pet., 40-41 (citations omitted). The Petition never alleges that a portion of an HTTP response is a portion of a packet—because it is not true.

Swenson unambiguously describes routing portions of HTTP requests or responses, which are portions of network traffic and not portions of an individual packet. Ex. 2025, ¶¶106-107. Each of Swenson’s portions of HTTP requests, portions of HTTP responses, or portions of network traffic themselves comprise multiple packets and are not portions of packets. *Id.* Thus, Swenson does not suggest sending less than a whole packet to the controller as claimed.

**G. Claim 16:<sup>9</sup> The 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”**

---

<sup>9</sup> Claim 17 depends from claim 16. Thus, Patent Owner’s arguments advanced with respect to claim 16 also apply to that claim.

Claim 16 requires “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.” The Petition does not allege that Lin or Shieh discloses distinct header and payload fields, or that the header comprises one or more flag bits—implicitly admitting that they do not disclose the claimed features. Pet., 45, 68. Without these disclosures, Lin and Shieh cannot suggest that the packet-applicable criterion is a set flag bit.

Instead, the Petition alleges without evidentiary support that a “POSA would have known that a packet includes distinct header and payload fields” and “it would have been well-known to a POSA that the header field includes one or more flag bits.” *Id.* This is an improper attempt to use a POSA’s common knowledge to supply a wholly missing claim limitation without evidentiary support or satisfying the “searching” standard required by the Federal Circuit, and should be rejected. *See DSS Tech. Mgmt. Inc. v. Apple Inc.*, 885 F.3d 1367, 1377 (Fed. Cir. 2018) (The Board may not “rel[y] on ‘ordinary creativity’ ‘as a wholesale substitute for reasoned analysis and evidentiary support’ ‘when dealing with a limitation missing from the prior art references specified’”); *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 851 F.3d 1270, 1274-1275 (Fed. Cir. 2017) (expert may not “fill in missing limitations” by alleging that a person of ordinary skill in the art would

envision them). As the Federal Circuit has repeatedly held, “references to ‘common sense’—whether to supply a motivation to combine or a missing limitation—cannot be used as a wholesale substitute for reasoned analysis and evidentiary support, especially when dealing with a limitation missing from the prior art references specified...In cases in which ‘common sense’ is used to supply a missing limitation, as distinct from a motivation to combine, moreover, our search for a reasoned basis for resort to common sense must be searching.” *Arendi SARL v. Apple Inc.*, 832 F.3d 1355, 1362-63 (Fed. Cir. 2016).

Here, even more egregiously, the Petition suggests that, because headers including flag bits were known, a POSA could have used them as a condition in Lin or Shieh—despite neither reference mentioning flag bits at all. This argument is not supported with “reasoned analysis and evidentiary support.” *Id.* at 1362. The Petition has not produced any supporting evidence that header fields are known to comprise flag bits at the time of invention. Furthermore, even assuming header fields were known to comprise flag bits, no evidence exists to suggest that a POSA would apply them to Lin or Shieh in the manner claimed. Ex. 2025, ¶¶108-110.

The Petition does not allege that the missing features are “unusually simple and the technology particularly straightforward” or provide “reasoned analysis and evidentiary support” to justify gap-filling the missing limitation. *Arendi*, 832 F.3d at

1362. Indeed, the Petitioner does not address *Arendi* at all. Petitioner however cannot satisfy their burden under *Arendi* simply with a generic allegation that a POSA would know to apply flag bits in header fields to Lin or Shieh. *Id.*

**H. Claim 30: The prior art does not disclose “receiving...one or more additional packets” as claimed**

Finally, claim 30 requires “receiving...one or more additional packets,” “checking...if any one of the one or more additional packets satisfies the criterion,” and “sending...the additional packet to the second entity” “responsive to an additional packet not satisfying the criterion” or “sending the additional packet in response to the instruction” “responsive to the additional packet satisfying the criterion.” The Petition alleges claim 30 is obvious based on Lin’s teaching “that its method can be applied to ‘any packet received by the SDN switch’” or Shieh’s statement that “its method can be applied to ‘subsequent packets of a particular session.’” Pet., 53, 73. Neither of these teachings, however, are disclosures to perform the steps of claim 30 on “one or more additional packets.” Ex. 2025, ¶¶111-117.

Contrary to the Petition, paragraph 29 of Shieh actually states that the security device informs the network access device that all subsequent packets of the session are forwarded for inspection: “Alternatively, a security device may inform a network access device that subsequent packets of a particular session should be forwarded

from the network access device for security inspection.” Ex. 1006, [0029]. Thus, rather than checking whether the additional packet satisfies the criterion and then sending the additional packet to the “second entity” or to the “entity that is included in the instruction” depending on the criterion, Shieh teaches that *all* packets are forwarded to the same destination (the security device) for inspection. Ex. 2025, ¶¶115-117. Paragraph 29 does not disclose the “subsequent packets of a particular session” are subject to checking if 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. *Id.*

Likewise, contrary to the Petition, Lin states that any packet received at ingress port 623-1 will be forwarded to redirect port 623-2 and any packet received at redirect port 623-2 will be forwarded to ingress port 623-1:

After the redirect flow rules for creating the SDN pipe are inserted in the flow tables 621, any packet received by the SDN switch 620 in the ingress port 623-1 will be identified as to be forwarded to the redirect port 623-2, and any packet received by the SDN switch 620 in the redirect port 623-2 will be identified as to be forwarded to the ingress port 623-1 (see arrow 602). This allows the security service 630 to receive from the redirect port 623-2 all outgoing packets sent by the sender component 622 to the ingress port 623-1.

Ex. 1005, 6:40-48. Just like for Shieh above, this passage of Lin treats *all* packets identically without consideration of any criterion: if a packet is received at ingress port 623-1, it is forwarded to redirect port 623-2, and if a packet is received at redirect port 623-2, it is forwarded to ingress port 623-1.<sup>10</sup> Ex. 2025, ¶¶112-114. The destination of the packets disclosed in this passage does not change between the “second entity” and the “entity that is included in the instruction” depending on whether the additional packet satisfies the criterion, as required by the claim.

For these reasons, neither Lin nor Shieh perform the steps of claim 30 on “one or more additional packets.”

## V. CONCLUSION

For the reasons set forth above, Petitioner has not met its burden of proving claims 1-9, 12-24, and 27-31 of the ‘111 Patent are unpatentable by a preponderance of the evidence. The Board should therefore issue a final written decision finding claims 1-9, 12-24, and 27-31 not unpatentable.

---

<sup>10</sup> Since claim 30 requires the packets be “receiv[ed], by the network node from the first entity . . .,” packets received by Lin’s redirect port cannot meet the claim language.

Date: January 15, 2024

Respectfully submitted,

/Minghui Yang/

Minghui Yang  
Reg. No. 71,989  
Counsel for Patent Owner  
CARMICHAEL IP, PLLC  
8607 Westwood Center Drive  
Suite 270  
Tysons, VA 22182  
Email: mitch@carmichaelip.com  
Telephone: (703) 646-9248

**CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITS**

This Patent Owner's Response ("POR") consists of 12,427 words, excluding table of contents, table of authorities, certificate of service, this certificate, or table of exhibits. The POR complies with the type-volume limitation of 14,000 words as mandated in 37 C.F.R. § 42.24. In preparing this certificate, counsel has relied on the word count of the word-processing system used to prepare the paper (Microsoft Word).

Dated: January 15, 2024

/Minghui Yang/  
Minghui Yang  
*Counsel for Patent Owner*

**CERTIFICATE OF SERVICE**

The undersigned hereby certifies that the following documents were served  
by electronic service, by agreement between the parties, on the date below:

**PATENT OWNER'S RESPONSE  
EXHIBIT 2024-2027**

The names and email addresses of the parties being served are as follows:

Jeffrey D. Blake      [jblake@merchantgould.com](mailto:jblake@merchantgould.com)  
[OrckitIPR@merchantgould.com](mailto:OrckitIPR@merchantgould.com)

Respectfully submitted,

/Minghui Yang/

Date: January 15, 2024