

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. AND JUNIPER NETWORKS, INC.¹,

Petitioners,

v.

ORCKIT CORPORATION,

Patent Owner.

Case IPR2023-00554
U.S. Patent No. 10,652,111 B2

**PETITIONER JUNIPER NETWORKS, INC.'s
NOTICE OF APPEAL**

¹ IPR2024-00037 (Juniper Networks, Inc.) has been joined with this proceeding.

Director of the United States Patent and Trademark Office
Office of the General Counsel
United States Patent and Trademark Office
Mail Stop 8
P.O. Box 1450
Alexandria, VA 22313
efileSO@uspto.gov

**NOTICE OF APPEAL TO THE UNITED STATES
COURT OF APPEALS FOR THE FEDERAL CIRCUIT**

Petitioner Juniper Networks, Inc. (“Petitioner”) hereby provides notice of appeal to the United States Court of Appeals for the Federal Circuit pursuant to 35 U.S.C. §§ 141, 142, and 319, and 37 C.F.R. §§ 90.2 and 90.3 from the Final Written Decision of the Patent Trial and Appeal Board (“Board”) entered September 17, 2024 (Paper 43), and from all underlying findings, conclusions, orders, decisions, rulings, and opinions in IPR2023-00554. A copy of the Final Written Decision is attached as Exhibit 1.

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), Petitioner indicates that the issues on appeal include, but are not limited to: (1) the Board’s determination that claims 1-9, 12-24, and 27-31 are not unpatentable under 35 U.S.C. § 103(a) as obvious over Lin and Swenson, (2) the Board’s determination that claims 1, 5-9, 12-24, and 27-30 are not unpatentable under 35 U.S.C. § 103(a) as obvious over Shieh and Swenson, and (3) all other issues decided adversely to Petitioner in any finding, conclusion, order, decision, ruling, or opinion underlying or supporting the Final Written Decision.

Pursuant to 35 U.S.C § 142 and 37 C.F.R. § 90.2(a), Petitioner is filing a copy of this Notice of Appeal with the Director of the United States Patent and Trademark Office, and a copy of this Notice is being concurrently filed with the Patent and Trial Appeal Board. In addition, Petitioner is filing a copy of this Notice and the required docketing fees with the Clerk's Office for the United States Court of Appeals for the Federal Circuit via CM/ECF.

Dated: November 19, 2024

Respectfully submitted,

/Ken K. Fung/

Ken K. Fung (pro hac vice)

FISCH SIGLER LLP

400 Concar Drive

San Mateo, CA 94402

Phone: 650.362.8200

ken.fung@fischllp.com

Counsel for Juniper Networks, Inc.

CERTIFICATE OF SERVICE

The undersigned certifies that, on the date below, the foregoing Petitioner Juniper Network Inc.'s Notice of Appeal was:

- (1) electronically filed with the PTAB through P-TACTS
- (2) electronically filed by email sent to the following email address:

efileSO@uspto.gov for the Director of the United States Patent and Trademark Office:

Director of the United States Patent and Trademark Office
c/o Office of the Solicitor
United States Patent and Trademark Office
Mail Stop 8, P.O. Box 1450
Alexandria, VA 22314

(3) electronically filed, along with the required docket fee, in the U.S. Court of Appeals for the Federal Circuit through the Court's CM/ECF filing system

(4) served via electronic mail on the following attorneys of record for the Patent Owner listed below:

Lead Counsel	Back-up Counsel
Minghui Yang (Reg. No. 71,989) Carmichael IP, PLLC 8607 Westwood Center Drive Suite 270 Tysons, VA 22182 703.646.9248 mitch@carmichaelip.com Orckit-IPRs@Carmichaelip.com	James T. Carmichael (Reg. No. 45,306) Carmichael IP, PLLC 8607 Westwood Center Drive Suite 270 Tysons, VA 22182 703.646.9255 jim@carmichaelip.com Stephen McBride (Reg. No. 78,396) Carmichael IP, PLLC 8607 Westwood Center Drive Suite 270 Tysons, VA 22182 703.646.9247

	stevemcbride@carmichaelip.com George Stamatopoulos KOBRE & KIM LLP 800 Third Avenue New York, NY 10022 Tel: 646-658-4972 Email: George.Stamatopoulos@kobrekim.com Michael Ng KOBRE & KIM LLP 150 California Street 19th Floor San Francisco, CA 94111 Tel: 415-582-4803 Email: Michael.Ng@kobrekim.com
--	---

(5) served via electronic mail on the following attorneys of record for
Petitioner Cisco Systems, Inc. listed below:

Lead Counsel	Back-up Counsel
Jeffrey D. Blake MERCHANT & GOULD P.C. 191 Peachtree Street NE Suite 3800 Atlanta, GA 30303 Phone: 404-954-5040 Fax: 612-332-9081 jblake@merchantgould.com OrckitIPR@merchantgould.com	Andrew J. Lagatta MERCHANT & GOULD P.C. 150 South Fifth Street Suite 2200 Minneapolis, MN 55402 Phone: 612-371-5383 Fax: 612-332-9081 alagatta@merchantgould.com

Dated: November 19, 2024

/Ken K. Fung/
Name: Ken K. Fung (pro hac vice)
Counsel for Petitioner Juniper Networks, Inc.

Exhibit 1

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. AND JUNIPER NETWORKS, INC.¹,
Petitioner,

v.

ORCKIT CORPORATION,
Patent Owner.

IPR2023-00554
Patent 10,652,111 B2

Before KRISTEN L. DROESCH, NATHAN A. ENGELS, and
BRENT M. DOUGAL, *Administrative Patent Judges*.

DOUGAL, *Administrative Patent Judge*.

JUDGMENT
Determining No Challenged Claims Unpatentable
35 U.S.C. § 318(a)

¹ IPR2024-00037 (Juniper Networks, Inc.) has been joined with this proceeding.

I. INTRODUCTION

A. *Background and Summary*

Cisco Systems, Inc., later joined by Juniper Networks, Inc., (collectively, “Petitioner”) filed a Petition to institute an *inter partes* review challenging the patentability of claims 1–9, 12–24, and 27–31 (the “challenged claims”) of U.S. Patent 10,652,111 B2 (Ex. 1001, “the ’111 patent”). Paper 1 (“Petition” or “Pet.”). Orckit Corp. (“Patent Owner”) filed a Preliminary Response. Paper 6. Applying the standard set forth in 35 U.S.C. § 314(a), we instituted an *inter partes* review of all challenged claims. Paper 8 (“Dec.”).

Patent Owner filed a Response (Paper 22, “PO Resp.”), Petitioner filed a Reply (Paper 31, “Reply”), and Patent Owner filed a Sur-reply (Paper 36, “Sur-reply”). An oral hearing was held on July 9, 2024, and a copy of the transcript was entered into the record. Paper 42 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73 as to the patentability of the challenged claims. Having reviewed the arguments and supporting evidence, we determine that Petitioner has not shown by a preponderance of the evidence, that the challenged claims are unpatentable.

B. *Related Matters*

The parties identify the following related district court litigation: *Orckit Corp. v. Cisco Systems, Inc.*, No. 2:22-cv-00276 (E.D. Tex.) (“parallel district court proceeding”). Pet. 78; Paper 7, 2.

C. *The ’111 Patent*

The ’111 patent is titled “Method and System for Deep Packet Inspection in Software Defined Networks.” Ex. 1001, code (54). Deep Packet Inspection (“DPI”) is a technique for examining network

communications that can be used to extract data patterns from a data communication channel. *Id.* at 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. *Id.* at 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. *Id.* at 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.*

Figure 1 shows a method for DPI in an SDN.

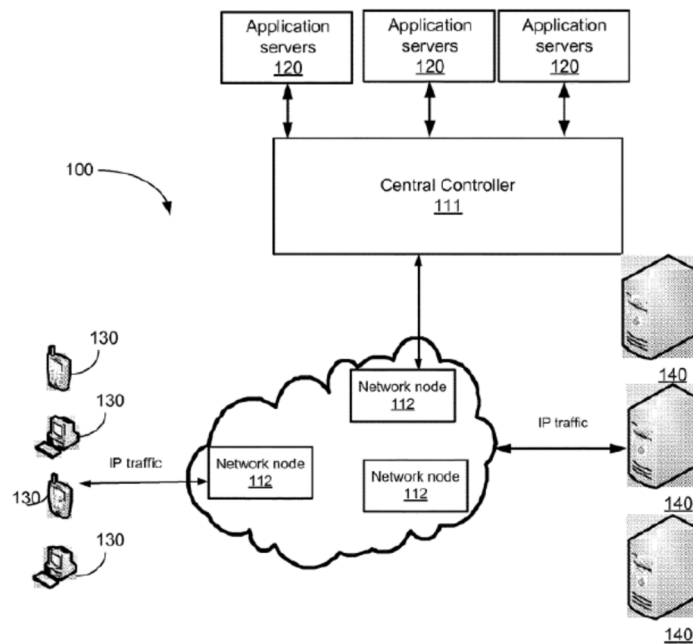


FIG. 1

In the embodiment of Figure 1, above, a network system 100 includes a controller 111 “configured to perform deep packet inspection on designated packets from designated flows or TCP sessions” by “instruct[ing] each of the network nodes 112 which of the packets and/or sessions should be directed to the controller 111 for packet inspections.” *Id.* at 4:5–11. The network node may be instructed to either redirect the packet to controller 111 or send the packet to the destination server 140. *Id.* For example, the controller may send a “probe” instruction to a network node such that, when the network node receives a packet that matches a “packet-applicable criterion,” the network node will “mirror” (i.e., send) some or all of the packet to a security component for inspection. *Id.* at 2:3–44.

D. Illustrative Claim(s)

Of the challenged claims, claim 1 is the only independent:

1. A method for use with a packet network including a network node for transporting packets between first and second entities under control of a controller that is external to the network node, the method comprising:

sending, by the controller to the network node over the packet network, an instruction and a packet-applicable criterion;

receiving, by the network node from the controller, the instruction and the criterion;

receiving, by the network node from the first entity over the packet network, a packet addressed to the second entity;

checking, by the network node, if the packet satisfies the criterion;

responsive to the packet not satisfying the criterion, sending, by the network node over the packet network, the packet to the second entity; and

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.

Ex. 1001, 10:52–11:4.

E. Evidence

Petitioner’s grounds of unpatentability rely on the following evidence:

Name	Patent Document	Exhibit
Lin	US 9,264,400 B1 (Feb.16, 2016)	1005
Swenson	US 2013/0322242 A1 (Dec. 5, 2013)	1007
Shieh	US 2013/0291088 A1 (Oct. 31, 2013)	1006

F. Asserted Grounds

Petitioner asserts the following grounds of unpatentability (Pet. 4–5), supported by the declaration of Samrat Bhattacharjee, Ph.D. (Ex. 1004):

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–9, 12–24, 27–31	103	Lin, Swenson
1, 5–9, 12–24, 27–30	103	Shieh, Swenson

II. ANALYSIS

A. Legal Standards

Petitioner bears the burden to demonstrate unpatentability. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). A claim is unpatentable as obvious if “the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (quoting 35 U.S.C. § 103(a)). We resolve the question of obviousness based

on underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the prior art and the claims; (3) the level of skill in the art; and (4) when in evidence, objective indicia of nonobviousness. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

We apply these principles to the Petition’s challenges.

B. Level of Ordinary Skill in the Art

We review the grounds of unpatentability in view of the understanding of a person of ordinary skill in the art at the time of the invention. *Id.* at 13, 17. Petitioner asserts that a person of ordinary skill in the art (POSA):

would have had a bachelor’s degree in computer science, computer engineering, or an equivalent, and two years of professional experience, and a POSA would have had a working knowledge of hardware and software for packet-switched networking. EX1004, ¶¶48-49. Lack of work experience can be remedied by additional education and vice versa. *Id.*, ¶48.

Pet. 5. “Patent Owner does not dispute Petitioner’s level of ordinary skill.”
PO Resp. 16.

We are persuaded that Petitioner’s proposal is consistent with the problems and solutions in the ’111 patent and prior art of record. We adopt Petitioner’s definition of the level of skill for the purposes of this Decision.

C. Claim Construction of “Controller”

In *inter partes* review, we construe claims using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b) (2022).

Petitioner argues that “‘controller’ should be construed to mean ‘an entity configured to perform deep packet inspection on packets.’” Pet. 5 (citing Ex. 1001, 10:52–62; Ex. 1004 ¶¶ 69–71). In support, Petitioner provides a detailed discussion of the ’111 patent specification. *See id.* at 5–7. Petitioner concludes this discussion with a statement supported by its declarant that “A POSA would have known from this description that the central controller was configured in this manner to provide DPI on redirected packets, as all of the embodiments in the ’111 Patent disclose that redirected packets are sent to the central controller for DPI.” *Id.* at 6 (citing Ex. 1004 ¶ 71; Ex. 1001, 4:8–18, 4:49–50, 8:1–5).

Patent Owner argues that in the now-dismissed parallel district court proceeding, the court “preliminarily construed the term ‘controller’ as ‘an entity that is capable of controlling deep packet inspection.’” PO Resp. 16.² “Patent Owner submits that ‘controller’ should be construed consistent with the preliminary construction in the District Court Case,” but does not explain why or address the differences between the two constructions. *Id.* at 17.

Petitioner responds that its construction “more closely aligns with the disclosure in the ’111 Patent.” Reply. 1.

Both parties agree that the ultimate analysis “remains the same” under either construction. *Id.* at 2; PO Sur-reply 2.

We likewise agree that we do not need to decide between the two constructions. At the same time, consistent with parties’ positions, we construe “controller” to mean an entity that is either 1) configured to

² Though Patent Owner does not provide a citation in support, Petitioner does not disagree that this is consistent with what occurred in the parallel district court proceeding. *See* Reply 1.

perform deep packet inspection on packets, or 2) that is capable of controlling deep packet inspection.

We determine that no other terms need to be construed. *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.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

D. 35 U.S.C. § 103 – Lin and Swenson

Petitioner argues that the combination of Lin and Swenson renders obvious the subject matter of claims 1–9, 12–24, and 27–31. Pet. 13–54. Patent Owner argues Petitioner has not demonstrated a reasonable likelihood of success in showing the claims are unpatentable. PO Resp. 19–42.

For the reasons expressed below, we determine that Petitioner has not shown that the claims are unpatentable over the combination of Lin and Swenson.

1. Claim 1

Petitioner argues that independent claim 1 is taught by the combination of Lin and Swenson. Pet. 13–33.

The method of claim 1 requires that steps be performed by a “controller.” As discussed above, we construe “controller” to mean an entity that is either 1) configured to perform deep packet inspection on packets, or 2) that is capable of controlling deep packet inspection. Both parties agree that the ultimate analysis “remains the same” under either construction. Reply 2; PO Sur-reply 2.

Both parties also agree that Lin does not teach a controller that performs or controls deep packet inspection (“DPI”). Pet. 18–19 (explaining that Lin teaches a security service (630) separate from the controller (610));

PO Resp. 20. This can be seen in Lin Figure 6, reproduced below, which the Petition relies on to show how Lin meets many of the limitations of claim 1.

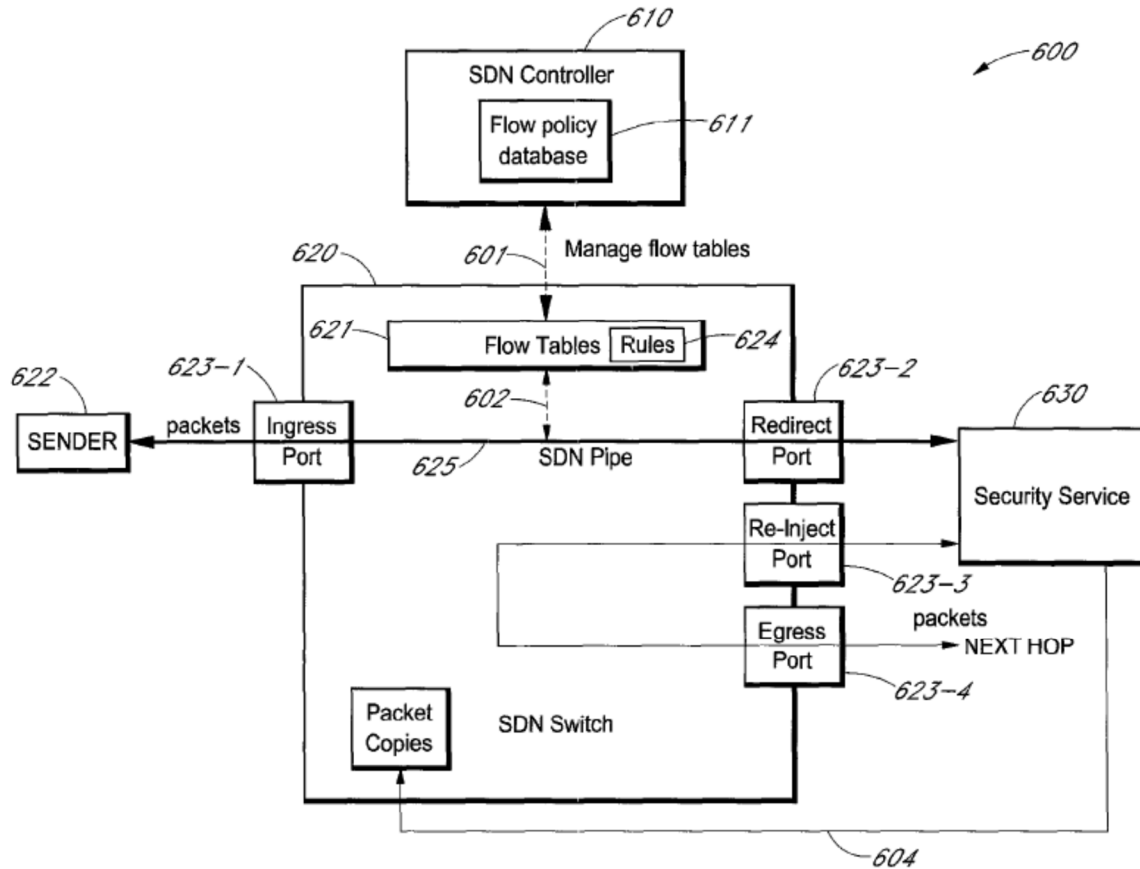


FIG. 6

Most relevant here, Petitioner relies on Lin Figure 6, above, as showing a software defined network (“SDN”) that transmits packets over the network with the use of an SDN controller (610) and an SDN switch (620) (i.e., the network node), where the packets pass between two entities (sender 622 and Next Hop) and DPI is performed on packets by the security service (630). Pet. 13–18 (citing e.g., Ex. 1005, 1:7–9, 3:11–12, 4:8–31, 4:33–67, Fig. 6; Ex. 1004 ¶¶ 75–78).

The Petition highlights that the SDN controller and switch “are logically separate components,” (*id.* at 16–17 (quoting Ex. 1005 3:51–52)) but then argues that the, also logically separate, security service and

controller would be combined (*id.* at 18–25). The Petition argues that one of skill in the art would modify Lin based on the “limited number of design options” and in view of the teachings of Swenson to obtain a controller that performs or controls DPI. *Id.* at 18–25. We start with Swenson below.

a) Lin, Modified by Swenson

The parties dispute whether Swenson teaches DPI.

Petitioner argues that Swenson teaches a flow analyzer performing deep flow inspection (“DFI”) on “a HTTP packet flow matching a particular signature.” *Id.* at 19 (citing Ex. 1007 ¶ 59). The Petition quotes Swenson as stating “the flow analyzer 312 of the network controller 140 performs a deep flow inspection to determine if the flow is worth bandwidth monitoring and/or user detection.” *Id.* (quoting Ex. 1007 ¶ 59); *see also id.* at 19–20 (citing Ex. 1007 ¶ 65 (discussing inspection of a HTTP GET request header and response payload to determine whether to monitor flow or optimize video)). Petitioner argues “that a ‘flow’ is a series of packets having a specific signature,” and therefore, according to Petitioner, DFI – “deep flow inspection” is referring to “deep packet inspection” “on one or more packets in a flow.” *Id.* at 19 (citing Ex. 1004 ¶ 80 (Declarant making a substantially identical statement)). In this manner, the Petition itself and the initial testimony of Petitioner’s declarant assert in rather conclusory fashion that DFI is the same as DPI.

Patent Owner argues with support from its declarant that DFI is not the same as DPI. PO Resp. 23–32. Both parties’ declarants agree that DPI “was a ‘well-known technique used for computer network packet filtering’ that was ‘used in enterprise security to detect various attacks.’” Ex. 1015 ¶ 29 (quoting Ex. 2025 ¶ 58). Patent Owner’s declarant provides additional detail about the “thorough inspection process” of DPI in paragraph 58,

which Petitioner’s declarant does not contest. *See* Ex. 1015 ¶ 29³. This testimony includes that “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,” and that DPI “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.” Ex. 2025 ¶ 58.

Concerning DFI, Patent Owner’s declarant argues that:

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. Flows convey information that is relevant to different aspects of network monitoring than the information conveyed by individual packets. In particular, inspection of flows conveys information about the state of the network that is not conveyed by individual packets.

Ex. 2025 ¶ 60; *see also id.* ¶ 63 (discussing Swenson, Abst., ¶¶ 3, 18). This is consistent with the teachings of Swenson.

Swenson discloses a system and method for “selectively monitoring traffic in a service provider network.” Ex. 1007, Abst. Swenson is concerned with bandwidth consumption over a network, especially in view of the high bandwidth demands required by video and media consumption. *Id.* ¶¶ 3, 5–6, 19–20. For this reason, Swenson teaches monitoring network flows and identifying large flows that can be optimized to improve network performance. *Id.* ¶¶ 18–22.

Swenson contrasts its system with “conventional inline TCP throughput monitoring devices that monitor every single data packet[]

³ Petitioner’s declarant only contests that DPI poses “certain unique challenges” as addressed in Ex. 2025 ¶ 59. Ex. 1015 ¶ 29.

transmitted and received.” *Id.* ¶ 28. This is because Swenson teaches optimizing an entire network flow, “because it is rarely possible to switch to optimized content mid-stream once non-optimized content delivery has begun.” *Id.* Swenson looks at the network flow so that the flow can be diverted, for example to optimize the network flow of a large video. *Id.* ¶ 28; *see also id.* ¶ 31 (“video is of far greater importance than all other traffic types when network congestion is considered”).

Looking at the differences between DPI and DFI in Swenson, Patent Owner’s declarant testifies that:

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. A POSA would understand 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 ¶ 62.

“[T]hat DPI and DFI are different is further supported by at least one academic article discussing combining the ‘fine-grain DPI with the coarse-grain DFI’ in a single method for ‘malicious behavior detection.’” PO Sur-reply 8 (citing Ex. 2027); *see also* Ex. 1016, 105–108 (Petitioner’s Counsel questioning Patent Owner’s declarant about this document). This article discusses DPI and DFI as separate processes consistent with the testimony of Patent Owner’s declarant and consistent with how Swenson distinguishes its process from monitoring of data packets. *See e.g.*, Ex. 2025 ¶¶ 57–67; Ex. 1007 ¶ 28. Petitioner’s argument that there are similarities between DPI and DFI (Reply 9–10) is also supported by Exhibit 2027, which discloses the

idea that DPI and DFI can be combined to provide a single method for malicious behavior detection.

We do note that Exhibit 2027 was published in 2017 (Ex. 2027, 1) while the '111 patent claims priority back to 2014 (Ex. 1001, code (60)). Thus, Exhibit 2027 is not direct evidence of the understanding of one of skill at the time of invention or filing of the application to which the '111 patent claims priority. At the same time, Exhibit 2027 does provide evidence of the understanding of one of skill in the art at least shortly thereafter. *See In re Hogan*, 559 F.2d 595, 605 & n. 17 (C.C.P.A. 1977) (Publications published after the date of invention are “evidence of the state of the art existing on the filing date of an application.”); *cf. In re Epstein*, 32 F.3d 1559, 1563, 1567 (Fed.Cir.1994) (writings dated after the filing date demonstrated the level of skill in the art at the time of the invention). Thus, Exhibit 2027 is especially relevant here, where we have no other third party or contemporary evidence supporting Petitioner’s position that Swenson’s DFI would be considered to be DPI other than the assertions of Petitioner’s declarant.

We agree with Patent Owner that DPI and DFI would have been understood to be different processes – 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. As discussed above, the testimony of Patent Owner’s declarant as to the understanding of DPI is largely uncontested. Further, the testimony of Patent Owner’s declarant as to the understanding of DFI is supported by Swenson when considered as a whole as well as supported by Exhibit 2027.

Inconsistent with our finding that DPI and DFI would have been understood to be different processes, Petitioner’s declarant argues that

independent of any “flow-related analysis” in Swenson, “[t]he DFI performed in Swenson is inspection of the payload of individual [or multiple] packets and thus would constitute DPI.” Ex. 1015 ¶ 30; *see id.* ¶ 28.

Petitioner, and Petitioner’s declarant, first rely on paragraphs 59 and 60 of Swenson in support of its position that DPI is performed. Pet. 19; Ex. 1004 ¶ 80. Swenson paragraph 59 states, for example, that “the flow inspection performed by the flow analyzer 312 may determine if the flow indeed contains large or medium object (e.g., larger than 50 kB),” but does not state that packets are inspected. Paragraph 60 similarly does not make mention of the inspection of packets. These paragraphs also do not convey any concern with what might be present in a packet, but rather are concerned with the network flow generally. Petitioner’s declarant cites these paragraphs when asserting that “‘deep flow inspection’ in Swenson refers to performing DPI on one or more packets in a flow” and that “‘flow’ is a series of packets having a specific signature,” but Petitioner’s declarant does not provide any more analysis. Ex. 1015 ¶ 28.

Petitioner’s declarant then explains that “Paragraph [0065] of Swenson discloses analysis of the ‘response payload’ of a packet. A POSA would have understood the analysis of the ‘response payload’ to be DPI by a DPI-capable controller.” *Id.* ¶ 30 (citing Ex. 1007 ¶ 65). Petitioner’s declarant then asserts that “even if the analysis involves reviewing the response payload of multiple packets, a POSA still would have considered this to be DPI because Swenson is explicitly disclosing the analysis of the payload of individual packets in a flow.” *Id.*

Similar to paragraphs 59 and 60, Swenson paragraph 65 does not mention or discuss packets or inspection of packets. Ex. 1007 ¶ 65.

Paragraph 65 discloses that “the HTTP GET request header and a portion of the response payload” are sent “to the network controller 140, which inspects the message to determine whether to monitor the flow or optimize the video.” Swenson here displays a concern for the flow and a desire to analyze the network flow, but it does not “disclose analyzing the message payload,” or provide any details of inspection of packets. Ex. 2025 ¶ 68. The assertion by Petitioner’s declarant that Swenson “discloses” analysis of packets and that this is DPI, is not supported by a preponderance of the evidence.

Further, we find the testimony of Patent Owner’s declarant more persuasive based at least on his consideration of Swenson as a whole and his more detailed analysis and explanations. For example, Patent Owner’s declarant explains in detail why, “[i]n 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:”

Furthermore, 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. The reference to a HTTP request and response “header” and “payload” are thus not references to the header and payload of a packet. A POSA would know that despite common parlance references to “HTTP packets,” HTTP does not pertain to individual packets, whereas 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). 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.

Petitioner's declarant merely responds by reiterating what was previously stated:

Swenson is explicit in stating that its inspection techniques include inspection of "a portion of the [HTTP] response payload." . . . A POSA would have understood the analysis of the "response payload" to be DPI by a DPI-capable controller, as DPI refers to monitoring the payload of a packet.

Ex. 1015 ¶ 34; *see also* Reply 8. Petitioner's declarant does not explain why mention of "response payload" means that Swenson discloses DPI and not merely inspection of the flow characteristics. Further, the assertion about what one of skill in the art would have understood is not sufficiently addressed or explained. Petitioner's declarant does testify that "DPI requires that the system must have the capability to look at the payload or body of a packet." Ex. 1015 ¶ 34. No citation is provided, and as already established, Petitioner's declarant does not contest Patent Owner's testimony that DPI requires more than this as it is a "thorough inspection process," where for example, "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." Ex. 2025 ¶ 58. Absent supporting evidence, it is unclear why merely looking at a packet could be considered DPI, even if Swenson did disclose how or whether packets are inspected.

For all of the above reasons, we determine that deep flow inspection would not be understood to be the same as deep packet inspection, and that Petitioner has not established by a preponderance of the evidence that Swenson teaches deep packet inspection or a controller configured to

perform DPI as asserted and relied on in the Petition. Thus, Petitioner has not established by a preponderance of the evidence that the combination of Lin and Swenson teaches all of the features of claim 1.

b) Limited Number of Design Options

As noted previously, the Petition also argues that one of skill in the art would modify Lin based on the “limited number of design options.” Pet. 18–19.

The Petition argues that Lin’s SDN controller and security service are both implemented on computing devices, and both are connected to the SDN switch through wires or virtual links. *Id.* at 18 (citing Ex. 1005, 5:51–55).

Thus, Petitioner argues that:

a POSA would have understood that one of the limited number of design options would have been to implement the security service as part of a controller configured to perform DPI analysis on packets, and a POSA would have had a reasonable expectation that the controller would have been successful in performing DPI analysis.

Id. at 18–19 (citing Ex. 1004 ¶ 79 (making an identical statement)). No additional discussion, explanation, or evidence on these points were provided at the Petition stage.

Patent Owner argues that:

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).

PO Resp. 21–22 (citing Ex. 2025 ¶¶ 54–55). We agree.

Though Petitioner asserts that there are a “limited number of design options” and that it would have been obvious to combine the different components of Lin, Petitioner does not establish that a controller configured to perform DPI analysis on packets was a known solution, and thus one of the limited design options. As discussed in *KSR*:

When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense. In that instance the fact that a combination was obvious to try might show that it was obvious under § 103.

KSR, 550 U.S. at 421.

Besides asserting the combination would have been “obvious to try,” Petitioner provides no other analysis or reason why one of skill in the art would have modified the teachings of Lin to obtain the claimed controller. Thus, Petitioner has not established by a preponderance of the evidence that the teachings of Lin render obvious all of the features of claim 1.

2. Claims 2–9, 12–24, 27–30

As Petitioner has not established, by a preponderance of the evidence, that Lin or the combination of Lin and Swenson renders obvious the limitations of independent claim 1, it likewise has not established the obviousness of the dependent claims.

E. 35 U.S.C. § 103 – Shieh and Swenson

Petitioner argues that the combination of Shieh and Swenson renders obvious the subject matter of claims 1, 5–9, 12–24, and 27–30. Pet. 54–73. Patent Owner argues that Petitioner’s arguments are deficient. PO Resp 42–59.

For the reasons expressed below, we determine that Petitioner has not established, by a preponderance of the evidence, that the claims are unpatentable over the combination of Shieh and Swenson.

In the below analysis, we first review Shieh, and then address the parties' arguments with respect to the claims.

1. Shieh

Shieh is titled “Cooperative Network Security Inspection.” Ex. 1006, code (54). Shieh relates to a network security system where a network access device inspects a packet received from a source node which is destined to a destination node. *Id.* at Abstr. If the network access device determines the packet needs to “undergo security processing” it “is transmitted to a security device . . . to perform content inspection.” *Id.* Alternatively, “[t]he packet is routed to the destination node without forwarding . . . to the security device.” *Id.*

2. Claim 1

Petitioner argues that independent claim 1 is taught by the combination of Shieh and Swenson. Pet. 54–66. Petitioner argues that Shieh and Swenson have similar architecture and function in similar ways. *Id.* at 55–62.

Concerning the “packet-applicable criterion,” which is relevant to almost all of the method steps, the Petition relies on Shieh for “disclos[ing] separate packet-applicable criterion to determine which packets should be forwarded to the security device pursuant to the filtering rules.” *Id.* at 62 (citing Ex. 1004 ¶ 224). The Petition then states that specific examples of packet-applicable criterion in Shieh include the identification of “TCP FIN

or TCP RST packets.” *Id.* at 63 (citing Ex. 1006⁴ ¶¶ 35, 36, 49) (emphasis omitted).

In our Institution Decision we preliminarily determined,

Petitioner’s position concerning the “packet-applicable criterion” is unclear. For example, it is unclear how identification of “TCP FIN or TCP RST packets” corresponds to the teachings surrounding filtering rules in Shieh. Further, Shieh does not appear to teach what happens to a packet in a special event such as a TCP FIN or TCP RST packet is identified. *See* Ex. 1006 ¶ 36. As discussed by Patent Owner, “Shieh discloses that packet destinations are determined by the bypass flag—which is separate from the TCP FIN or TCP RST packet.” Prelim. Resp. 19 (citing Ex. 1006 ¶¶ 36–37); *see also id.* at 19–21. The Petition asserts that they are related, but does not explain how. *See e.g.*, Pet. 62–63, 65.

As the Petition relies on identification of TCP FIN and TCP RST packets in Shieh for the “packet-applicable criterion,” we cannot say that Petitioner at this time has provided a reasonable basis for us to determine that claim 1 is unpatentable over the combination of Shieh and Swenson.

Dec. 19.

In response, Petitioner argues “the identification of ‘TCP FIN or TCP RST packets’” and the “bypass flag” were identified as *separate* examples of packet-applicable criterion in the Petition. Reply. 16–17 (citing Pet. 65–66).

We do not agree. The Petition clearly states:

For example, Shieh provides criterion specific to a particular packet being checked, such as the identification of “TCP FIN or TCP RST packets.” *Id.*, ¶[0036]; *see id.*, ¶[0035], ¶[0049]. **These correspond to the claimed packet-applicable criterion.**

⁴ The citation in the Petition uses “*id.*” in error, pointing to Ex. 1004 instead of listing Ex. 1006.

Pet. 63 (citing Ex. 1006 ¶¶ 35, 36, 49) (Bold in original); *see also id.* at 65 (“Shieh discusses the implementation of packet-applicable criterion, such as the identification of “TCP FIN or TCP RST packets.”). The Petition does not discuss the bypass rule when identifying the supposed “packet-applicable criterion” in Shieh.

The Petition does later discuss the bypass flag in a parenthetical after again discussing the “TCP FIN or TCP RST packets”:

Shieh checks whether a packet is a TCP FIN or TCP RST packet, and, responsive to the packet not satisfying this criterion, sends the packet to the destination node (i.e., the second entity). *Id.*, ¶[0036]; *see id.*, ¶[0037] (discussing whether packet should be sent to security processing device “based on a bypass flag”); EX1004, ¶¶239-242.

Pet. 65. In our Institution Decision, this is what we were referring to when we said “The Petition asserts that they (the bypass flag and the TCP FIN or TCP RST packet.”) are related, but does not explain how.” Dec. 19. The Petition only expressly relies on “check[ing] whether a packet is a TCP FIN or TCP RST packet” in this section as well. The Petition never indicates that the bypass flag is a separate embodiment of packet-applicable criterion that Petitioner intends to rely on. Thus, we decline to consider this new and untimely argument, first introduced in the Reply, that the bypass flag should be considered a packet-applicable criterion, separate from identification of a TCP FIN or TCP RST packet.

Shieh paragraph 37 describes a process of security inspection where a device (272) “determines whether [a] packet should be forwarded to [a] security device” based on “[i]f the bypass flag matches the predetermined value.” The paragraph ends stating “If there are certain events [i.e. receipt of a TCP FIN or TCP RST packet] that have been registered from security

device 273, network device 272 may notify security device 274 via path 287 upon detecting the registered events.” As can be seen, receipt of a TCP FIN or TCP RST packet does not relate to a bypass flag, which was why we determined the Petition was unclear.

Because the Petition does not discuss the bypass rule when identifying the supposed “packet-applicable criterion” in Shieh, we decline to consider this new and untimely argument that the bypass flag should be considered a packet-applicable criterion.

At the same time, we now consider Petitioner’s clarified position that identification of “TCP FIN or TCP RST packets” reads on “packet-applicable criterion,” which should be considered separately from the bypass flag. Reply 16–17.

In our Institution Decision we stated that “Shieh does not appear to teach what happens to a packet in a special event such as [when] a TCP FIN or TCP RST packet is identified.” Dec. 19 (citing Ex. 1006 ¶ 36).

Shieh paragraph 36 states:

During the bypass [security-processing] phase, the I/O function may notify the security-processing function if there are special events in the packet stream. These events could be receipt of TCP FIN or TCP RST packets, or not receiving any packets of the connection within a time threshold. The notification from I/O functions to security processing functions could help to clean up the state in the security-processing nodes.

Ex. 1006 ¶ 36; *see id.* ¶ 37 (making a similar explanation).

In response, Petitioner argues that:

A POSA would have understood this disclosure in the context of Paragraph [0035] of Shieh, which explains that “communication between I/O functions and security-processing functions [enable] packets to bypass security-processing function if there is no more need to inspect the packets of the connection.” *Id.*,

¶[0035]; EX1015, ¶50. As such, Shieh teaches using “the identification of TCP FIN or TCP RST packets” to decide whether to keep forwarding packets to the security processing device for inspection or skip the security function and send the packets to their destination.

Reply 18 (citing Ex. 1015 ¶ 50 (Petitioner’s declarant making a substantially similar statement)).

Petitioner misunderstands the teachings of Shieh. As noted above, Shieh states that a notification is sent when a TCP FIN or TCP RST packet is received to “help to clean up the state in the security-processing nodes.” Ex. 1006 ¶ 36. Shieh states that this occurs when the system is *already* in a bypass security-processing phase. *Id.* ¶¶ 35–36. This contradicts Petitioner’s assertion, as Shieh does not “teach[] using ‘the identification of TCP FIN or TCP RST packets’ to decide whether to keep forwarding packets to the security processing device for inspection or skip the security function and send the packets to their destination.”

For this reason, Petitioner has not shown by a preponderance of the evidence how identification of TCP FIN or TCP RST packets in Shieh teaches the following limitations of claim 1:

responsive to the packet not satisfying the criterion, sending, by the network node over the packet network, the packet to the second entity; and

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.

Thus, Petitioner has not established by a preponderance of the evidence that the combined teachings of Shieh and Swenson render obvious all of the features of claim 1.

3. *Claims 5–9, 12–24, 27–30*

Claims 5–9, 12–24, and 27–30 all depend from claim 1. Thus, the Petition has not established, by a preponderance of the evidence, that these claims are unpatentable over Shieh and Swenson for the same reasons as claim 1.

III. CONCLUSION

For the foregoing reasons, we determine that Petitioner has not proven, by a preponderance of the evidence, that the challenged claims are unpatentable, as summarized in the following table:

Claims	35 U.S.C. §	Reference(s) /Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1–9, 12–24, 27–31	103	Lin, Swenson		1–9, 12–24, 27–31
1, 5–9, 12– 24, 27–30	103	Shieh, Swenson		1, 5–9, 12–24, 27–30
Overall Outcome				1–9, 12–24, 27–31

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–9, 12–24, and 27–31 of U.S. Patent 10,652,111 B2 have not been shown to be unpatentable; and

FURTHER ORDERED that because this is a Final Written Decision, parties to the proceeding seeking judicial review of the Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2023-00554
Patent 10,652,111 B2

PETITIONER:

Jeffrey Blake
jblake@merchantgould.com
Daniel McDonald
dmcdonald@merchantgould.com

PATENT OWNER:

Minghui Yang
mitch@carmichaelip.com
James Carmichael
jim@carmichaelip.com
Stephen McBride
stevemcbride@carmichaelip.com