

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CLOUDFLARE, INC.,
Petitioner,

v.

PACSEC3, LLC.,
Patent Owner.

IPR2023-00544
Patent 7,523,497 B2

Before KRISTEN L. DROESCH, GREGG I. ANDERSON, and
MICAHEL T. CYGAN, *Administrative Patent Judges*.

ANDERSON, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Cloudflare, Inc., (“Petitioner”) filed a Petition requesting *inter partes* review of claims 7–12 of U.S. Patent No. 7,523,497 B2 (Ex. 1001, “the ’497 patent”). Paper 2, 1 (“Pet.”). Pacsec3, LLC, (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

We have authority under 35 U.S.C. § 314. Upon considering the record developed thus far, for reasons discussed below, we institute *inter partes* review.

II. BACKGROUND

A. *Real Parties in Interest*

Petitioner states it is the real party in interest. Pet. 94. Patent Owner asserts it is the real party in interest. Paper 3, 2 (Patent Owner’s Mandatory Notices).

B. *Related Matters*

Both parties list one pending lawsuit filed by Patent Owner asserting the ’497 patent against Petitioner in the Western District of Texas captioned *PacSec3, LLC v Cloudflare, Inc.*, 6:22-cv-00129 (W.D. Tex.). Pet. 94; Paper 3, 2. Both parties list another twenty (20) lawsuits filed against third parties where Patent Owner asserts infringement of the ’497 patent. Pet. 94–95; Paper 3, 2–3. Patent Owner discloses that eight (8) of the twenty listed lawsuits have been dismissed.¹ Paper 3, 2–3.

The parties also list a pending reexamination of the ’497 patent Control No. 90/014,746, currently on appeal to the Board.² Pet. 95;

¹ Petitioner lists the eight dismissed lawsuits without noting they have been dismissed. Pet. 94–95.

² The Examiner finds claims 7 and 10 not unpatentable over Maher (US Patent No.7,058,974) and Savage (*see* Section II.E below), in a Notice of

IPR2023-00544

Patent 7,523,497 B2

Paper 3, 3; *see also* Ex. 1003 (Reexamination Application No. 90/014,746).

However, an Ex Parte Reexamination Certificate issued May 22, 2023, and there is no indication that the case continues to be on Appeal to the Board.

See Ex. 3002.

The parties also list another *inter partes* review proceeding involving the '497 patent, IPR2022-01230, *Splunk Inc. v. PacSec3, LLC* (“'1230 IPR”), which was terminated due to settlement prior to any institution decision. *See* '1230 IPR, Paper 8 (Termination Decision).

C. The '497 Patent

The application for the '497 patent was filed on May 7, 2004, as U.S. Patent Application No. 10/841,064 ('064 application). Ex. 1001 at code (22). The '064 application is a continuation of U.S. Patent Application No. 09/715,813 filed November 16, 2000 which issued as U.S. Patent No. 6,789,190 on September 7, 2004. *Id.* at code (63), 1:6–8.

1. Background Technology

The '497 patent “pertains to network data transmission controls” and to “minimizing the effects of packet flooding attacks directed against computers or routers connected to a network.”³ Ex. 1001, 1:11–15. The primary objective of the '497 patent is to “defend against ‘packet flooding attacks’ in which an attacker tries to use up all the bandwidth to the victim by sending data of little or no value (at least to the victim), thereby making

Intent to Issue a Reexamination Certificate on May 1, 2023 (Ex. 3001, 1); *see also* Ex. 3002 (“Ex Parte Reexamination Certificate,” US 7,523,497 C1).

³ Wetherall (*see* Section II.E below), as well as other prior art relied on, relate to “regulating network traffic in a computer network, such as defending against denial-of-service (‘DoS’) attacks against the network.” Ex. 1004 ¶ 56 (citing Ex. 1006 (Wetherall), 1:52–55).

more valuable communication with the victim slow or unreliable.” *Id.* at 2:6–10.

One way to deal with such attacks is to allocate resources in the network. Ex. 1001, 2:15–18. “Well-behaved users” request reasonable of bandwidth while “attackers request unreasonable amounts,” resulting in an unfair allocation. *Id.* at 2:16–18. A “first come first served” approach allocates most of the resource to the attackers whereas a “fair” allocation would “reduce the impact of an attacker to that of a normal user.” *Id.* at 2:18–22.

2. The network control method of the '497 patent

The '497 patent describes and claims “[a] packet flooding defense system for a network” which includes “a plurality of host computers, routers, communication lines and transmitted data packets.” Ex. 1001, 3:30–34. Data packets received at a host computer are classified by “associating a maximum acceptable processing rate with each class of data packet received at the computer.” *Id.* at 3:46–48.

Figure 1 is reproduced below.

Figure 1

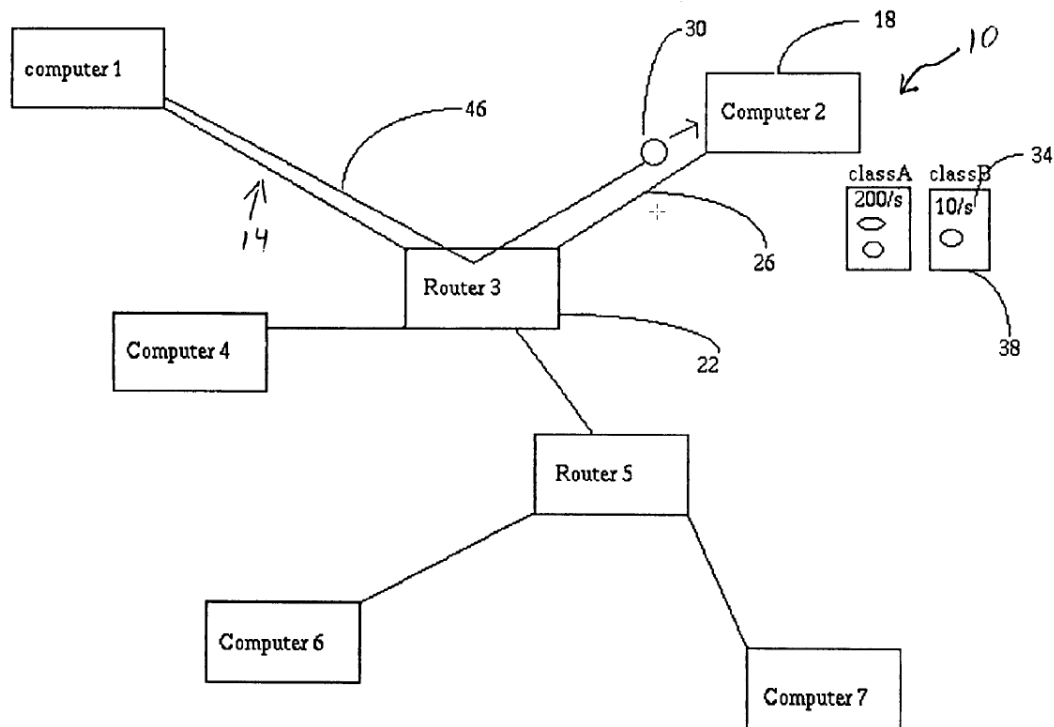


Figure 1 is a schematic view of one embodiment illustrating the association of maximum acceptable processing rates for each class of packet received at a computer.

Ex. 1001, 5:28–32. As shown in Figure 1, the packet flooding defense system network 14 includes “a plurality of host computers 18, routers 22, communication lines 26 and transmitted data packets 30.” *Id.* at 6:14–16. Data packets 30 received at the host computer 18 are associated with a “maximum acceptable processing rate 34 with each class 38 of data packet 30 received at the computer 18.” *Id.* at 6:16–20. The computer determines “the path 46 by which the packets 30 came to the computer 18.” *Id.* at 6:20–23. Using the path information, the computer “allocate[s] the processing rate for each class 38 in a desired way among the places from which packets 30 are transmitted.” *Id.* at 6:23–25.

D. Illustrative Claim

Claims 7–12 of the '497 patent are challenged. Pet. 6. Claims 7, 8, 10, and 11 are independent method claims. Claims 9 and 12 depend from claims 8 and 11 respectively. Claim 7 is illustrative and is reproduced below.

7. [Preamble]⁴ A method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said method comprising the steps of::

[7.A] determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer;

[7.B] classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;

[7.C] associating a maximum acceptable processing rate with each class of data packet received at said host computer; and

[7.D] allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.

Ex. 1001, 9:45–61.

⁴ Petitioner uses the claim number followed by “[Preamble]” for the preamble or capital letters for the claim limitations. *See* Pet. 14 ([Preamble]), 16 ([A]). Patent Owner adopts Petitioner’s format but adds the claim number. *See* Prelim. Resp. 15 (7[B]). We place the claim number with a capital letter for the limitation inside the brackets as the format for this Decision.

E. Evidence of Record

This proceeding relies on the following prior art references and expert testimony:

Wetherall, US Patent No. 6,801,503 B1, issued October 5, 2004 (Ex. 1006, “Wetherall”);

Doeppner, *Using Router Stamping to Identify the Source of IP Packets*, CCS ’00, Athens, Greece, Copyright 2000 (Ex. 1007, “Doeppner”);

Savage, *Practical Network Support for IP Traceback*, SIGCOMM’00, Stockholm, Sweden, Copyright 2000 (Ex. 1008, “Savage”);

Cheriton, US Patent No. 7,120,931 B1, issued October 10, 2006 (Ex. 1009, “Cheriton”); and

Petitioner relies on the Declaration of Dr. Kevin Jeffay in Support of Petition for *Inter Partes* Review of U.S. Patent No. 7,523,497 (Ex. 1004, “Jeffay Declaration”).

F. Asserted Grounds

Petitioner asserts the following grounds. Pet. 6.

Claim(s) Challenged	35 U.S.C.⁵ §	Reference(s)/Basis
7–12	103	Wetherall, Doeppner
7–12	103	Wetherall, Savage
7–12	103	Cheriton, Doeppner
7–12	103	Cheriton, Savage

⁵ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-129, 125 Stat. 284, 285–288 (2011), revised 35 U.S.C. § 103 effective March 16, 2013. Because the challenged patent was filed prior to March 16, 2013, we refer to the pre-AIA version of the statute. The findings and analysis in this Decision would be the same under the AIA version.

III. PATENTABILITY ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner proposes that a person of ordinary skill in the art as of the priority date of the '497 patent “would have had a B.S. degree and a Masters degree in Computer Science, Computer Engineering, or an equivalent field, as well as one to two years of academic or industry experience in computer networking or comparable industry experience.” Pet. 5 (citing Ex. 1004 ¶ 53). Patent Owner does not propose a level of ordinary skill nor does it comment on Petitioner’s proposal.

Petitioner’s proposal is consistent with the level of ordinary skill in the art reflected by the asserted prior art. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). On this record, the level of ordinary skill is neither in dispute nor dispositive of any challenge. For purposes of this Decision, we apply Petitioner’s articulation.

B. Claim Construction

In an *inter partes* review, a claim shall be construed 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 (2019); *see also Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

Petitioner asserts no term requires construction. Pet. 5. Patent Owner “submits that the terms of the ’497 Patent are clear on their face” but proposes that the term “path” should be construed. Prelim. Resp. 5.

1. “*path*” (claims 7 and 10)

Patent Owner proposes “path” be construed as follows:

Both the ordinary meaning and the specification of the ’497 patent show that a “path” must include a link such as a series of routers, a “path” must not comprise only source and destination.

Prelim. Resp. 6.

Claim 7 recites in pertinent part recites “determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; *said path comprising all routers in said network via which said packets are routed to said computer.*” See Section II.D above (Limitation [7.A]). Patent Owner cites the italicized language as part of its evidence supporting its proposed construction. Prelim. Resp. 6.

Patent Owner also argues the specification supports that “routers” or some physical “link” must be included in the path. Patent Owner quotes the following from the Specification.

Routers will supply data about the forwarding path of the packets that arrive at a site. . . . In this invention a path (which is not controlled by the attacker) is used to determine the actual direction of the packet flow towards the victim.

Prelim. Resp. 6 (quoting Ex. 1001, 2:54–55, 3:62–64).

Patent Owner also cites supporting extrinsic evidence. Patent Owner argues “source” and “destination” are the beginning and end of the “path” but the “path” includes a “series of routers” or physical “links” along its

journey. Prelim. Resp. 5 (citing Ex. 2001,⁶ 394 (“In communications, a link between two nodes in a network.”). Patent Owner also cites extrinsic evidence as showing “[t]he sequence of communication links and packet switches traversed by a packet from the sending end system to the receiving end system is known as a route or path through the network.” *Id.* at 5–6 (quoting Ex. 2002,⁷ 4). Patent Owner cites additional evidence from Exhibit 2002 that

a packet starts in a host (the source), passes through a series of routers, and ends its journey in another host (the destination). As a packet travels from one node (host or router) to the subsequent node (host or router) along this path, the packet suffers from several types of delays at each node along the path.

Id. (quoting Ex. 2002 at 35–36).

At this time, Petitioner has not requested an opportunity to dispute Patent Owner’s proposal. We refer to our discussion below regarding Petitioner’s showing for Limitation [7.A]. *See* Section III.D.4 below. We preliminarily construe “path” to mean “a network connection between a source and destination that includes a series of routers.”

2. *Remaining Terms*

The parties are cautioned that arguments not timely raised are forfeit. In other words, if a party raises a claim construction issue at a final hearing, it may be too late. In general, the parties should review the record developed during trial for possible claim construction issues. Pending further development of the record, we proceed on the plain and ordinary

⁶ Microsoft Corp., MICROSOFT COMPUTER DICTIONARY, 5th Ed. 2002.

⁷ Kurose, *Computer Networking-A Top-Down Approach* (Pearson Education, Inc. 6th Ed. 2013).

meaning to a person of ordinary skill in the art as to all remaining claim terms.

C. *Legal Standard for Obviousness*

A patent claim is invalid as obvious if the differences between the claimed subject matter 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.” 35 U.S.C. § 103(a).

The ultimate determination of obviousness is a question of law, but that determination is based on underlying factual findings. . . . The underlying factual findings include (1) “the scope and content of the prior art,” (2) “differences between the prior art and the claims at issue,” (3) “the level of ordinary skill in the pertinent art,” and (4) the presence of secondary considerations of nonobviousness such “as commercial success, long felt but unsolved needs, failure of others,” and unexpected results.

In re Nuvasive, Inc., 842 F.3d 1376, 1381 (Fed. Cir. 2016) (citing *inter alia* *Graham v. John Deere Co. of Kan. City*, 383 U.S. 1, 17–18 (1966)).

“To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). Furthermore, in assessing the prior art, the Board must consider whether a person of ordinary skill would have been motivated to combine the prior art to achieve the claimed invention. *Nuvasive*, 842 F.3d at 1381.

As the Federal Circuit found, in quoting from the Supreme Court’s decision in *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418–419 (2007),

“because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known,” “it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does.”

Personal Web Techs., LLC v. Apple, Inc., 848 F.3d 987, 991–92 (Fed. Cir. 2017).

D. Claims 7–12 as Obvious over Wetherall and Doeppner

Petitioner alleges claims 7–12 would have been obvious over Wetherall and Doeppner. Pet. 7–44. Petitioner also relies on the Jeffay Declaration. Ex. 1004 ¶¶ 55–140.

On this record, Petitioner has sufficiently shown the subject matter of claims 7–10 would have been obvious over Wetherall and Doeppner. The showing made for claims 11 and 12 is in question. Below we briefly summarize the argument and evidence as to those limitations which are contested by Patent Owner.

1. Wetherall (Ex. 1006)

Wetherall describes a method and system for “regulating network traffic destined for a network node, such as a server, to facilitate ensuring the quality of service provided by the network to the network node and the parties interacting with it, such as a client.” Ex.1006, 1:44–48. Wetherall’s method “may also be used to block selected network traffic destined for a network node, thereby protecting the network node from denial of service attacks.” *Id.* at 1:52–55.

In Wetherall, an example computer network 100 includes a server 110 coupled to routers 106a-106h, which delivers data packets between

clients 108a, 108b and the server. *Ex.* 1006, 3:27–32. Network 110 is also provided with “director 102 to manage network traffic routing within network 100 to ensure a desired not-to-exceed network traffic profile of server 110 is adhered to.” *Id.* at 3:47–51. In one embodiment, the desired not-to-exceed network traffic profile is specified using one or more metrics, and preferably by network traffic types. *Id.* at 3:51–53. For example, at most 10% each of the incoming bandwidth to be used for TCP synchronize (SYN) packets and for domain name system (DNS) packets, with remaining incoming bandwidth to be used by other TCP traffic. *Id.* at 3:53–57.

Director 102 manages network traffic routing within network 100 by regulating and de-regulating network traffic routing by routing devices 106 a-106 h. *Ex.* 1006, 3:60–62. Examples of regulation include, but are not limited to, rate limiting the excess traffic, decreasing priority of the excess traffic, and re-routing the excess traffic. *Id.* at 3:62–65.

In operation, director 102 is first provided with a desired “not-to-exceed” network traffic profile of server 110, and a topology and routing map of network 100. *Ex.* 1006, 6:4–7. Director 102 receives network traffic reports on the network traffic routed through routing devices 106a-106h. *Id.* at 6:22–24, Fig. 1.

Figure 1 is reproduced below.

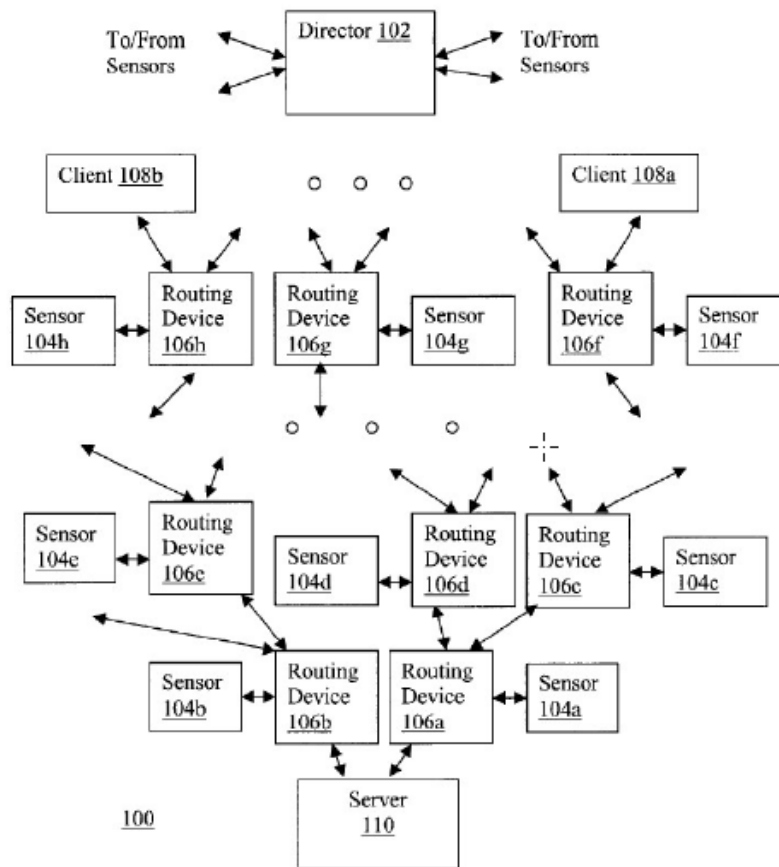


Figure 1

Figure 1 illustrates a network 100 to be managed for a network node 110 including a number of routing devices 106a-106h coupled to each other and to server 110.

Ex. 1006, 3:28–31. The routing devices 106 are “for routing network traffics, including network traffics destined for server 110, such as those originated from clients 108a-108b.” *Id.* at 3:31–33. The network has a “director 102 to manage network traffic routing within network 100 to ensure a desired not-to-exceed network traffic profile of server 110 is adhered to.” *Id.* at 3:47–51.

Figure 2 of Wetherall is reproduced below.

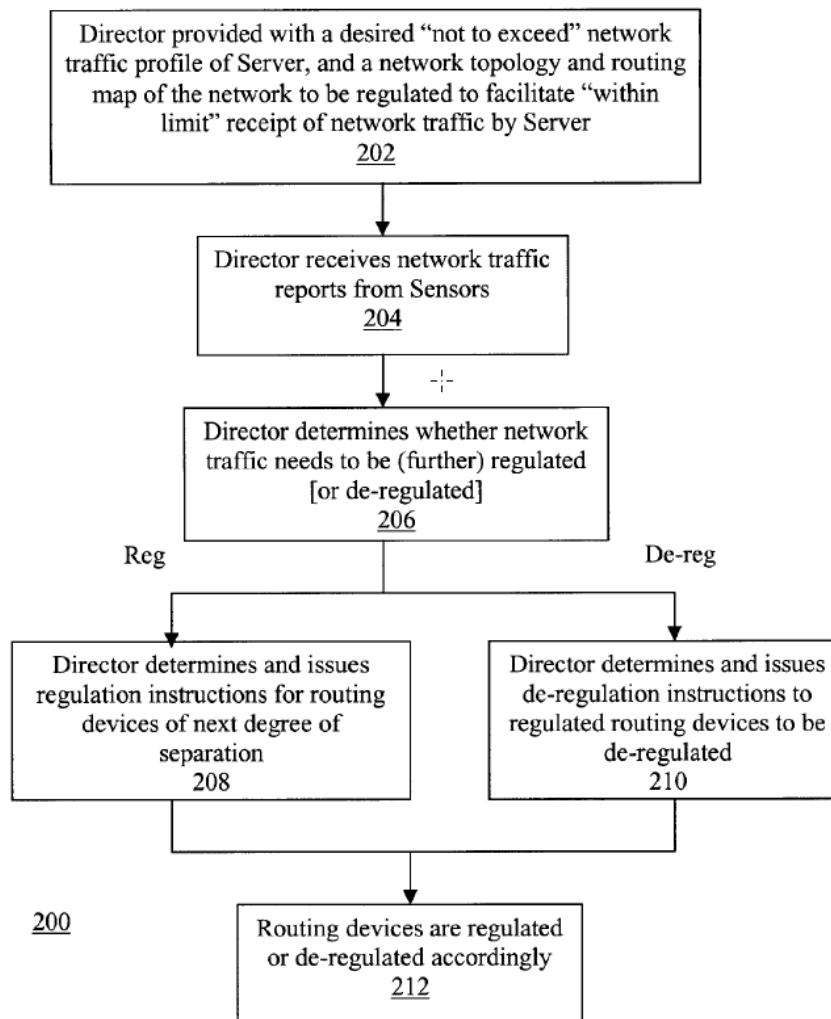


Figure 2

Figure 2 illustrates a method view of how a director regulates network traffic for a network node.

Ex. 1006, 2:21–27. At block 202, the “director 102 is first provided with a desired ‘not-to-exceed’ network traffic profile of server 110, and a topology and routing map of network 100.” Ex. 1006, 6:4–7. At block 204 the reported data includes various statistics and “characteristic” information describing the network traffic routed through the ingress/egress interfaces of routing devices 106a-106h. *Id.* at 6:26–29. For example, the reported data

includes destination information or network traffic types. *Id.* at 6:29–34. In addition to the TCP SYN and DSN packets, “network traffic types may further include Web, Real Networks, Secure Web.” *Id.* at 6:34–36. “Other TCP, [o]ther user datagram protocol (UDP), internet control message protocol (ICMP), TCP packets with acknowledge (ACK) set, TCP packets without SYN set, and so forth.” *Id.* at 6:37–40. “In general, any information carried as part of the packets may be used as typing criteria to divide the network traffic into different traffic types.” *Id.* at 6:40–42. Generally, “whatever data are necessary to support the employment of the desired ‘not-to-exceed’ metrics” is included. *Id.* at 6:47–48.

Still referring to Figure 2:

At block 206, in response to the receipt of the reported data, director 102 automatically determines whether network traffic routing in network 100 needs to be (further) regulated or de-regulated (using the received data, and the limits and operating margins specified in the earlier described desired “not-to-exceed” network traffic profile). . . . [R]egulation/de-regulation is advantageously performed in a progressive manner, thus if regulation (or further regulation) is needed, at block 208, director 102 determines the regulation to be imposed on the routing devices of the next degree of separation (along the reverse direction the routing paths traversed by the packets to reach the network node).

Id. at 6:49–62.

Continuing with the method illustrated in Figure 2, “if regulation is already in effect on both the ingress and egress interfaces of routing devices 106a-106b, further regulation is determined for routing devices 106c-106e with two degrees of separation from server 110.” Ex. 1006, 7:1–5. “On the other hand, . . . if de-regulation (or further de-regulation) is needed, at block 210, director 102 determines de-regulation for the ‘outermost’ regulated

subset.” *Id.* at 7:7–11. “At block 212, director 102 issues the regulation/deregulation instructions to routing devices 106a-106h to be regulated/de-regulated.” *Id.* at 7:58–60.

2. Doeppner⁸ (Ex. 1007)

Doeppner discloses a “router stamping” method that identifies the source of Denial of Service attacks. Ex.1007, 1⁹ (Abs.). A router “stamps” a data packet with an IP address corresponding to the previous router. *Id.* at 1–2.

Figure 1 of Doeppner (compressed) is reproduced below.

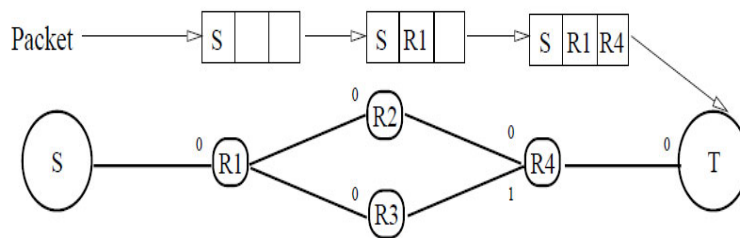


Figure 1: The packet travels from *S* to *T* via routers *R*₁, *R*₂ and *R*₄. Each router records the IP address of its predecessor before it forwards the packet.

Ex. 1007, 3. As illustrated in Figure 1:

[A] packet is sent from *S* to *T*. When *R*₁ processes the packet, it records *S*’s IP address in the first available slot and forwards the packet to *R*₂. *R*₂ records *R*₁’s address in the second slot and forwards the packet to *R*₄, which in turn records *R*₂’s address in the third slot and forwards the packet to *T*.

⁸ Petitioner alleges Doeppner is prior art under 35 U.S.C.

§ 102(a). Pet. 11–12. At this stage of the proceeding Patent Owner does not contest the allegation. For purposes of this Decision we find Doeppner is prior art.

⁹ Page references are to page numbers for the exhibit, which is how Petitioner cites to Doeppner. See Pet. 10 (“Summary of Doeppner”).

In case *T* does not trust the source address in the IP header, it can verify the source of the packet: assuming that routers' entries are accurate, *T* looks at the recorded route that the packet has traveled.

Id. at 2.

Doeppner explains that the packet stamps can be used to determine the source of a DoS attack on a network, so that packets from that source can be filtered out while leaving other data packets untouched. Ex. 1007, 4–5. Likely sources of an attack are identified by “looking for routers that had little incoming traffic, as evidenced by the absence of their stamps, while their neighbors recorded a large amount of traffic.” *Id.* at 5.2. One such filter can drop only packets that “come from the compromised area.” *Id.* at 7.2.

3. *Claim 7*

Petitioner alleges four reasons Wetherall and Doeppner are combinable. Pet. 12–14. Patent Owner does not dispute that a person of ordinary skill in the art would have had reason to combine Wetherall and Doeppner. We preliminarily find the reasons provided by Petitioner are sufficient and summarize the reasons below.

The first reason asserted by Petitioner is that the two references are in the same field of endeavor. Pet. 12 (citing Ex. 1004 ¶ 66). The second reason is that Doeppner teaches that packet source address information cannot be trusted because the packet header information can be manipulated or “spoofed” by the attacker. *Id.* at 12–13 (citing Ex. 1007, 184). Petitioner alleges this problem would have motivated a person of ordinary skill in the art to improve Wetherall, which does not provide a solution to the problem, by targeting attack traffic, rather than legitimate traffic. *Id.* at 13 (citing

Ex. 1007, 184; Ex. 1006, 6:40-48; 1004 ¶¶ 67–68). The third reason is that “Doeppner invites the combination with Wetherall by expressly suggesting that, upon identifying the source of attack packets, those packets can be isolated and filtered.” *Id.* at 13 (citing Ex. 1007, 186–188; 1006, 1:44–2:14; Ex. 1004 ¶ 69). The fourth reason Petitioner advances is that “Wetherall’s and Doeppner’s teachings are implemented on analogous computer components, such as computer networks with host computers, routers, and communication lines.” *Id.* at 13–14 (citing Ex. 1007, 187; Ex. 1004 ¶¶ 70–71).

We turn to Petitioner’s showings regarding the limitations of claim 7. Limitation 7 [Preamble] recites “[a] method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets.” If considered a limitation, Petitioner argues the preamble is shown because “Wetherall notes that its method of ‘regulating network traffic’ is used to ‘block selected network traffic destined for a network node, thereby protecting the network node from denial of service attacks.’” Pet. 14–15 (citing Ex. 1006, 1:44–55, 3:9–15, 3:23–39, 9:60–64, 10:1–7, Figs. 1 (reproduced above), 8; Ex. 1004 ¶¶ 72–73).

Petitioner adds that “Doeppner discloses using ‘router stamping’ techniques to ‘implement a successful defense against a *DoS* attack.’” Pet. 15 (citing Ex. 1007, 184, 186–187). Petitioner argues Doeppner, like Wetherall, shows a network “with host computers, routers, communication lines, and transmitted data packets.” *Id.* at 16 (citing; Ex. 1004 ¶ 74).

Limitation [7.A] recites “determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via

which said packets are routed to said computer.” Petitioner argues Doeppner teaches “router stamping.” Pet. 16 (citing Ex. 1007, 184–185; Ex. 1004 ¶ 75). Petitioner contends the router stamping is a “packet mark” which tracks malicious IP packets in a DoS attack. *Id.* at 16 (citing Ex. 1007, 185 (algorithm); Ex. 1004 ¶ 75).

Petitioner relies, in part, on Doeppner’s Figure 2 (reduced to fit page) is reproduced below.

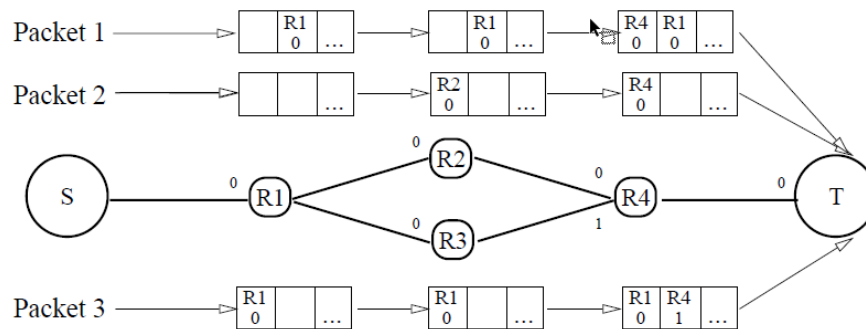


Figure 2: Packets 1, 2, 3 travel from *S* to *T*. They are processed by *R*₁, *R*₂, *R*₃ and *R*₄ which implement Router Stamping.

Pet. 17 (reproducing Ex. 1007, Fig. 2). Petitioner notes that the stamp of Doeppner includes “the IP address of the router and the interface on which the packet was received.” *Id.* (quoting Ex. 1007, 185, Fig. 2 (routers implementing router stamping); Ex. 1004 ¶¶ 76–77). In conclusion, Petitioner argues host computer *T*, the destination of the packets in Figure 2 of Doeppner (*see also* Ex. 1007, Fig. 1 above), “can determine the paths by which attack packets arrived at *T*, based on packet marks.” *Id.* (citing Ex. 1007, 187; Ex. 1004 ¶ 78).

Limitation [7.B] recites “classifying data packets received at said host computer into wanted data packets and unwanted data packets by path.” Part of Petitioner’s showing for Limitation [7.A] is relevant to this limitation. Limitation [7.A] includes the first appearance of “path.” We

therefore consider the showing for Limitation [7.A] in regard to meeting our preliminary construction of “path.”

In connection with Limitation [7.A], Petitioner argues that “[i]n a packet flooding attack, host computer T can determine the paths by which attack packets arrived at T, based on packet marks” and the amount of traffic. Pet. 17 (citing Ex. 1007, 187; Ex. 1004 ¶ 78). According to Petitioner, “[t]his determination can be made by ‘looking for routers that had little incoming traffic, as evidenced by the absence of their stamps, while their neighbors recorded a large amount of traffic from this node.’” *Id.* at 17–18 (citing Ex. 1007, 187, Fig. 2; Ex. 1004 ¶¶ 78–79). Referring to Figure 2 above and a probability calculation at Doeppner’s page 187 that a particular router is a source of “malicious packets,” Petitioner argues that the “path comprises all routers in said network via which said packets are routed to said computer.” *Id.* at 18 (citing Ex. 1007, 187 (probability calculation), Fig. 2; Ex. 1004 ¶¶ 78–79). Petitioner also contends the paths between routers, R1-R2-R4 and R1-R3-R4, are “all routers via which the packets are routed from source S to host computer T.” *Id.* (citing Ex. 1004 ¶ 79).

Specifically, with respect to Limitation [7.B], Petitioner’s showing continues noting Wetherall’s teaching of regulating network traffic by “rate limiting” based on the “not-to-exceed” step is described in connection with Wetherall’s Figure 1. Pet. 18 (citing Ex. 1006, 3:47–53, 3:60–65). Relying on the Jeffay Declaration, Petitioner contends that the “not-to-exceed” limits bandwidth based on traffic type. *Id.* (citing Ex. 1004 ¶ 80 (citing Ex. 1006, 3:47–53, 3:62–65)). Petitioner points to Wetherall’s Figure 2 as dividing traffic into two “traffic types,” i.e., “Reg” and “De-reg,” in which the regulation is applied to “routing devices of next degree of separation [from

the server].” *Id.* at 19 (citing Ex. 1006, Fig. 2 (annotated)). According to Petitioner, Wetherall’s division of traffic into traffic types, and “limiting only the packets sent by an attacker, these unwanted packets will only ‘minimally interfere[] with the legitimate or desirable traffic.’” *Id.* at 19–20 (citing Ex. 1006, 7:48–52; Ex. 1004 ¶ 82). Petitioner then argues “Wetherall thus *teaches classifying data packets into wanted data packets* (legitimate or desirable traffic) *and unwanted data packets* (attack traffic), and rate-limiting the attack packets differently than the legitimate packets.” *Id.* at 20 (citing Ex. 1004 ¶ 82). Petitioner also argues that Wetherall teaches that the packets are received at the server 110 of the host computer. *Id.* (citing Ex. 1006, 7:28–36; Ex. 1004 ¶ 83); *see also* Ex. 1006, Fig. 1, server 110 (reproduced above).

As to that portion of Limitation [7.B] reciting classification of wanted and unwanted packets by “path,” Petitioner argues source and destination indicating the start and end of a packet’s path as meeting the claim language. Pet. 20 (citing Ex. 1006, 6:42–45; Ex. 1004 ¶ 84). Further, it is argued that a person of ordinary skill would have understood that “classifying data packets by source and destination addresses to meet classifying those data packets by *path*.” *Id.* (citing Ex. 1004 ¶ 84). In making the allegation regarding “path,” Petitioner relies on Patent Owner’s infringement contentions in the other litigation that “deep packet inspection” is based on “source and destination of the packet.” *Id.* at 20–21, n.2 (citing Ex. 1010,¹⁰ 5).

¹⁰ “Patent Owner’s Infringement Contentions in litigation of same ’497 patent.” Pet. vi. The contentions appear to be from the “Splunk” lawsuit, which we understand to have been dismissed. *See* Ex. 1010, 2 (“Splunk® Enterprise”); *see also* Paper 3, 2 (listing Splunk lawsuit).

Petitioner also contends Doeppner teaches Limitation [7.B]. Pet. 21–22 (citing Ex. 1007, 186–188; Ex. 1004 ¶ 85). Petitioner notes that Doeppner teaches the classification into wanted and unwanted packets based on a “path” being “information about source and destination” and the application of filters to classify data packets, as taught by Doeppner. *Id.* at 21–22, n.3 (citing Ex. 1007, 188; Ex. 1010, 4 (infringement contentions in Splunk lawsuit)).

Patent Owner disputes Petitioner has shown Limitation [7.B] based on the construction of “path.” *See* Pet. 20 (Petitioner’s showing citing Ex. 1006, 6:42–45; Ex. 1004 ¶ 84). Patent Owner argues that Petitioner’s showing is based on “path” being construed as “specific source and destination address combinations in the packet header indicating the start and end of “the packet’s path in a network.” Prelim. Resp. 15 (citing Ex. 1006, 6:42–45; Ex. 1004 ¶ 84).

On this record, we are not persuaded by Patent Owner’s argument. First, Petitioner’s “source and destination” argument is advanced based on its understanding of Patent Owner’s infringement contentions. Second, as detailed above in connection with both Limitations [7.A] and [7.B], Petitioner’s arguments encompass a “path” that includes “a series of routers.” *See* Pet. 18 (“path comprises all routers in said network via which said packets are routed to said computer.”). We also note that in describing Doeppner, Petitioner contends the “data packet’s path can then be determined based on packet marks.” *Id.* at 10 (citing Ex. 1007, 187, Fig. 1 (reproduced above)). We decline to limit Petitioner’s showing regarding “path” when the showing as a whole meets our preliminary construction of “path” and Petitioner’s construction was based on what it anticipated from Patent Owner’s known litigation positions.

Limitation [7.C] recites “associating a maximum acceptable processing rate with each class of data packet received at said host computer.” Petitioner argues Wetherall teaches this limitation by disclosing that “packets are rate-limited to adhere to a ‘not-to-exceed’ network traffic profile of server 110,’ which is specified ‘preferably by network traffic types.’” Pet. 22–23 (citing Ex. 1006, 3:47–53, 6:4–7, Fig. 2 (annotated); Ex. 1004 ¶ 86). Petitioner adds that Wetherall “can specify, e.g., a maximum bandwidth, number of packets per second, or number of flows per second.” *Id.* at 23 (citing Ex. 1006, 3:51–57, 4:33–44, 6:7–12; Ex. 1004 ¶ 87). Petitioner concludes that a person of ordinary skill in the art would have understood “these metrics to meet the claimed maximum acceptable processing rate.” *Id.* (citing Ex. 1004 ¶ 87).

For that portion of Limitation [7.C] reciting “maximum acceptable processing rates” and “associates the rates with each class of data packet received at said host computer” Petitioner cites Wetherall Figure 7c. Pet. 24 (citing Ex. 1006, 9:30–41, Fig. 7c (annotated); Ex. 1004 ¶ 88). Petitioner notes specifically that columns 725a-725n and 726a-726n of Figure 7c are “for storing the network traffic types, and their corresponding ‘not-to-exceed’ limits,’ for the ‘various servers.’” *Id.* (citing Ex. 1006, 9:30–41, Fig. 7c (annotated)).

Limitation [7.D] recites “allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.” Petitioner cites Wetherall as teaching that “a notice is generated if ‘network traffics of the particular type have reached or surpassed the margin of the ‘not-to-exceed’ limit.’” Pet. 24 (quoting Ex. 1006, 8:52–55; Ex. 1004, ¶ 89). Wetherall is cited for teaching instructions are provided to routers to

be “regulated” as to “rate limiting the excess traffic.” *Id.* at 25 (citing Ex. 1006, 3:62–65, 8:65–9:1; Ex. 1004 ¶ 89).

Petitioner also argues Doeppner teaches Limitation [7.D]. Pet. 25. Petitioner argues that when a router is identified as a “possible source of malicious attacks” a filter is replaced on all routers connected to the filter. *Id.* (citing Ex. 1007, 188; Ex. 1004 ¶ 90).

Petitioner has shown sufficiently all limitations of claim 7 are taught by the combination of Wetherall and Doeppner. Accordingly, Petitioner has shown a reasonable likelihood that claim 7 would have been obvious over Wetherall and Doeppner.¹¹

4. Claims 8 and 9

Petitioner’s showing for independent claim 8 relies on similar arguments and evidence as alleged in connection with claim 7. *Compare* Pet. 18–22 (Limitation [7.B] (“classifying data packets . . . by path”)) *with* Pet. 26–27 (Limitation [8.A] (“classifying data packet . . . routed to said computer.”)). Limitation [8.A] recites “classifying data packets received at a host computer into wanted data packets and unwanted data packets; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer.” Petitioner relies on its “source and destination” argument discussed above in connection with Limitation [7.B]. Pet. 26.

¹¹ Having decided to institute trial on claim 7 as obvious over Wetherall and Doeppner, we proceed to trial on all claims challenged under all grounds. *SAS Inst. v. Iancu*, 138 S. Ct. 1348, 1356 (U.S. 2018). We analyze “the strengths and weaknesses of all challenges in the petition in order to provide guidance to the parties for the upcoming trial.” Patent Trial and Appeal Board Consolidated Trial Practice Guide November 2019, 64.

Patent Owner argues the classification of Doeppner is based only on source, and not destination. Prelim. Resp. 20 (citing Petitioner’s showing at Pet. 21). Patent Owner concludes that “[i]t is clear that the criterion of ‘classifying data packets’ in Doeppner is the source of the packets, not the destination address of the packets as required by claim 8 of the ‘497 Patent.” Prelim. Resp. 21. Petitioner relies primarily on Wetherall, not Doeppner. *See* Pet. 18–20.

Patent Owner seemingly equates the source and destination argument Petitioner makes to the showing regarding “path.” *See* Prelim. Resp. 20 (citing Pet. 20). However, the “path” term is absent from Limitation [8.A]. Regardless, Patent Owner’s argument regarding Doeppner’s teaching will be moot if Wetherall is shown to teach Limitation [8.A]. Preliminarily, we find Petitioner’s showing is sufficient for Limitation [8.A].

Claim 9 depends from claim 8. Patent Owner relies on its arguments for claim 8 to assert claim 9 has not been shown. Prelim. Resp. 29.

On this record, Petitioner has sufficiently shown all limitations of claims 8 and 9 are taught by the combination of Wetherall and Doeppner.

5. Claim 10

Patent Owner’s arguments for independent claim 10 are the same as those made for claim 7 and Limitation [7.B]. Prelim. Resp. 23. We refer to our prior analysis of Limitation [7.B]. *See* Section III.D.3 above.

On this record, Petitioner has sufficiently shown all limitations of claim 10 are taught by the combination of Wetherall and Doeppner.

6. Claims 11 and 12

Patent Owner’s arguments for independent claim 11 are the same as those made for claim 8 and Limitation [7.B]. Prelim. Resp. 25. Limitation [11.C] does differ and is argued as not being shown in the Petition. *Id.* at 26.

Limitation [11.C] recites “determining by said first router of the rate at which data packets of each class are transmitted from a second router to said first router.”

Petitioner relies on its showing for claims 7 and 8 for claim 11. Pet. 40–43 (citing Pet. 12–43 (showing for claim 7)). Limitation [11.C] recites “determining by said first router of the rate at which data packets of each class are transmitted from a second router to said first router.” Petitioner relies on its showing for Limitation [8.C] and the Jeffay Declaration. *Id.* at 42 (citing Pet. 27–28 (Limitation [8.C]; Ex. 1004 ¶¶ 98–99); Ex. 1004 ¶ 131 (Limitation [11.C])).

Patent Owner argues Limitation [11.C] differs from Limitation [8.C] and Wetherall and Doeppner do not teach “the rate at which data packets of each class transmitted from a second router to said first router **is determined by the first router.**” Prelim. Resp. 26. Patent Owner argues that Petitioner’s showing for Limitation [8.C] is insufficient because there is no showing of the bolded language. *Id.* at 25 (summarizing Petitioner’s showing for Limitation [8.C], 26 (no showing of “rate . . . determined by the first router”)).

As to Limitation [8.C], the Jeffay Declaration states a person of ordinary skill would understand that “various statistics and ‘characteristic’ information” would include “determined data rates and other network traffic data.” Ex. 1004 ¶ 98. The Jeffay Declaration also states the “determined rates” would “be transmitted from a router to the host computer.” *Id.* ¶ 99. There is no evidence on this record supporting that assertion. Neither of the above citations, nor the citation to paragraph 131 of the Jeffay Declaration, show the determination is made by a first of two claimed routers.

Petitioner equates the “host computer” of claim 8 to a “second router” of claim 11. *See* Pet. 40. How this architecture might meet Limitation [11.C] is left for trial.

Claim 12 depends from claim 11. Patent Owner relies on its arguments for claim 11 to assert claim 12 has not been shown. Prelim. Resp. 26.

On this record, we question whether Petitioner has sufficiently shown all limitations of claims 11 and 12 are taught by the combination of Wetherall and Doeppner.

7. Conclusion

Petitioner has shown a reasonable likelihood that claims 7–10 would have been obvious over Wetherall and Doeppner. We question whether Petitioner has sufficiently shown the combination teaches all the limitations of claims 11 and 12.

E. Claims 7–12 as Obvious over Wetherall and Savage

Petitioner alleges claims 7–12 would have been obvious over Wetherall and Savage. Pet. 44–59. Petitioner also relies on the Jeffay Declaration. Ex. 1004 ¶¶ 141–197.

Petitioner has sufficiently shown the subject matter of claims 7–10 would have been obvious over Wetherall and Savage. The showing made for claims 11 and 12 is in question. Below we briefly summarize the argument and evidence as to those limitations which are contested by Patent Owner.

1. Wetherall (Ex. 1006)

Wetherall was described in Section III.D.1 above.

2. *Savage*¹² (Ex. 1008)

Savage describes a technique for tracing anonymous packet flooding attacks on the Internet back towards their source. Ex. 1008, 1¹³ (Abs.)

Fig. 1 of Savage is shown below.

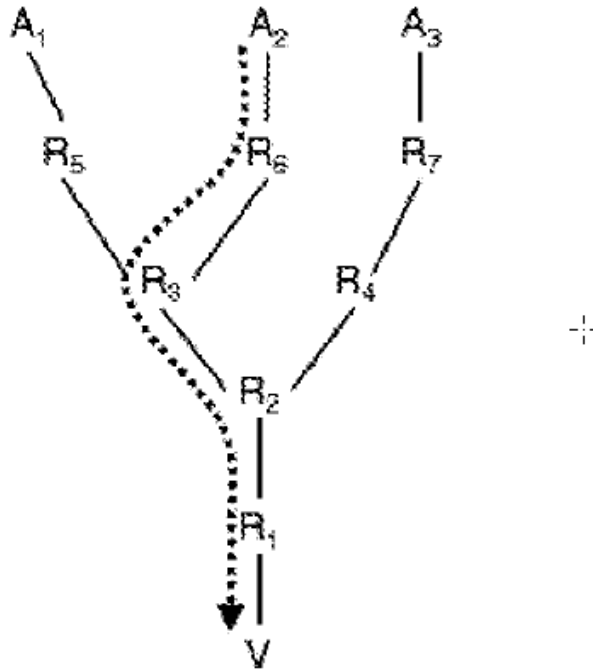


Figure 1 is a network as seen from the perspective of a victim (V). Ex. 1008, 298 (Fig. 1). In Figure 1, routers are shown as R₁ through R₇, attackers are shown as A₁ through A₃ and a particular attack path shown in dotted line. *Id.* (Section 3.1).

In order to determine the attack path and the associated attack origin for each attacker, Savage provides a marking algorithm including two

¹² Petitioner alleges Savage is prior art under 35 U.S.C. § 102(a). Pet. 46–47. At this stage of the proceeding Patent Owner does not contest the allegation. For purposes of this Decision we find Savage is prior art.

¹³ Page references are to Petitioner’s page numbers.

methods. Ex. 1008, 298. The first method (node append algorithm) is to “append each node’s address to the end of the packet as it travels through the network from attacker to victim.” *Id.* at 299. “[E]very packet received by the victim arrives with a complete ordered list of the routers it traversed a built-in attack path.” *Id.*

The second method includes a node sampling algorithm and edge sampling algorithm. Ex. 1008, 299. As to node sampling algorithm, “[u]pon receiving a packet, each router chooses to write its address in the node field with some probability *p*.” *Id.* “After enough packets have been sent, the victim will have received at least one sample for every router in the attack path.” *Id.* “Although it might seem impossible to reconstruct an ordered path given only an unordered collection of node samples, it turns out that with a sufficient number of trials, the order can be deduced from the relative number of samples per node.” *Id.* The algorithm of Savage attempts to determine the approximate origin of attack traffic. *Id.* at 304.

3. Claim 7

Petitioner provides four reasons a person of ordinary skill in the art would have combined Wetherall and Savage. Pet. 47–48. The reasons are either the same or similar to those discussed in the Wetherall and Doeppner combination and are not disputed by Patent Owner at this time. We find the reasons sufficient.

As with the Wetherall and Doeppner combination,¹⁴ Patent Owner contests Petitioner’s showing regarding Limitation [7.B] as failing to

¹⁴ The Examiner in the reexamination determined that Savage did not teach Limitation [7.B]. *See* Ex. 3001, 3–4. Because we determine that Wetherall teaches it, our determination is not inconsistent with the reexamination certificate finding claim 7 not unpatentable over Maher and Savage.

disclose “classifying data packets . . . by path.” Prelim. Resp. 27.

Petitioner relies on Wetherall, not Savage, for Limitation [7.B]. Pet. 51 (citing Pet. 18–22).

Savage is not a part of Petitioner’s showing for Limitation [7.B]. We addressed Wetherall as disclosing Limitation [7.B] above in connection with the Wetherall and Doeppner ground. *See* Section III.D.3 above. Because of the Examiner’s determination that Savage did not teach claim 7, we find questions surrounding this ground that will be further addressed during trial.

4. Claims 8 and 9

Patent Owner disputes that the Wetherall and Savage combination teach Limitation [8.A]. Prelim. Resp. 28–29. Patent Owner does not make any specific argument beyond a denial. *Id.* Petitioner relies on Savage for Limitation [8.A]. Pet. 52–53 (citing Ex. 1008, 297–298, Fig. 1 (reproduced above; Ex. 1004 ¶¶ 165–166)). On this record, Patent Owner’s denial is not sufficient.

Claim 9 depends from claim 8. Patent Owner relies on its arguments for claim 8 to assert claim 9 has not been shown. Prelim. Resp. 29.

On this record, Petitioner has sufficiently shown all limitations of claims 8 and 9 are taught by the combination of Wetherall and Savage.

5. Claim 10

Patent Owner’s arguments for independent claim 10 are the same as those made for claim 7 and Limitation [7.B]. Prelim. Resp. 29. We refer to our prior analysis of Limitation [7.B]. *See* Section III.D.3 above. Patent Owner does not make a separate argument based on the combination of Wetherall and Savage.

Petitioner relies on its showing regarding claim 7, which is alleged to be analogous. Pet. 54.

On this record, Petitioner has sufficiently shown all limitations of claim 10 are taught by the combination of Wetherall and Savage.

6. Claims 11 and 12

Patent Owner's denials, without further argument, that either Wetherall or Savage teach Limitation [11.C]. Prelim. Resp. 30. Petitioner relies on its showing for Limitation [8.B]. Pet. 57 (citing Pet. 40–43; Ex. 1004 ¶ 189). Paragraph 189 of the Jeffay Declaration does not show the determination is recited in Limitation [11.C] is made by a first of two claimed routers.

Claim 12 depends from claim 11. Patent Owner relies on its arguments for claim 11 to assert claim 12 has not been shown. Prelim. Resp. 30.

On this record, we question whether Petitioner has sufficiently shown all limitations of claims 11 and 12 are taught by the combination of Wetherall and Savage.

7. Conclusion

Petitioner has shown a reasonable likelihood that claims 7–10 would have been obvious over Wetherall and Savage. We question whether Petitioner has sufficiently shown the combination teaches all the limitations of claims 11 and 12.

F. Obviousness of Claims 7–12 over Cheriton and Doeppner

Petitioner alleges claims 7–12 would have been obvious over Cheriton and Doeppner or Savage. Pet. 61–81. Petitioner also relies on the Jeffay Declaration. Ex. 1004 ¶¶ 198–258.

1. Cheriton (Ex. 1009)

Cheriton discloses a method and system for generating filters based on analyzed flow data. Ex. 1009, 2:20–21. The method comprises separating

the data into different network flows, analyzing at least one of the network flows, and detecting potentially harmful network flows. *Id.* at 2:21–24.

Figure 4 of Cheriton is reproduced below.

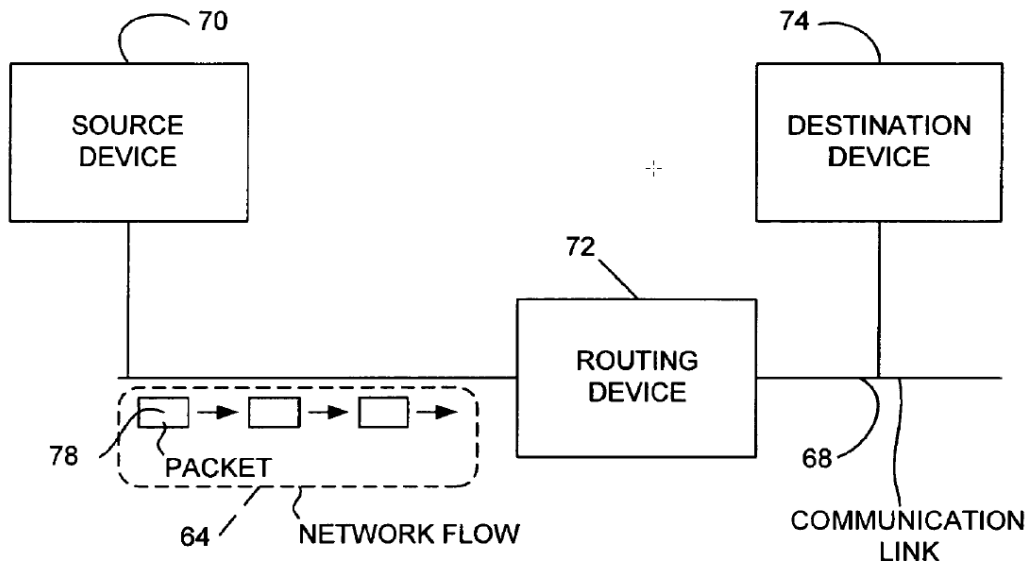


Fig. 4

Figure 4 is a diagram of a network illustrating network flow on a communication link.

Ex. 1009, 3:12–13. Figure 4 “shows a network flow 64 on communication link 68 connecting a source device 70, a routing device 72 and a destination device 74.” *Id.* at 5:40–42. “The source device 70 may be the attacker 20, the routing device may be the ISP router 14 or firewall 12, and the destination device may be one of the plurality of servers 16.” *Id.* at 5:46–49. “The routing device 72 may include specific hardware constructed or programmed for performing process steps described below, a general purpose processor operating under program control.” *Id.* at 5:52–55.

A network flow from an attacker in a DoS attack can be classified as harmful based on the number of packets or an unusual distribution of the

packets, which indicates a particular source is involved in the attack.

Ex. 1009, 7:12–15. That network flow can be filtered such that “only the destructive packets received from the actual attacker are dropped.” *Id.* at 7:23–24. Filters can be implemented in a router, or in a firewall between the router and host computer. *Id.* at 3:38–40.

2. Doeppner (Ex. 1007)

Doeppner is described in Section III.D.2 above.

3. Claim 7

Petitioner provides four reasons a person of ordinary skill in the art would have combined Cheriton and Doeppner. Pet. 61–63. The reasons are either the same or similar to those discussed in the Wetherall and Doeppner combination and are not disputed by Patent Owner at this time. We find the reasons sufficient.

Patent Owner disputes that Cheriton and Doeppner teach Limitation [7.B]. Prelim. Resp. 31. Patent Owner argues Petitioner’s argument and evidence are based on equating “source and destination addresses” in Cheriton with “path” in the ’497 patent. *Id.* (citing Pet. 64–67). Accordingly, Patent Owner argues our preliminary construction of “path” is not met. *Id.* at 32. Petitioner argues the “classification is *by path* (i.e., from the source device to the destination device).” Pet. 67 (citing Ex. 1004 ¶ 214).

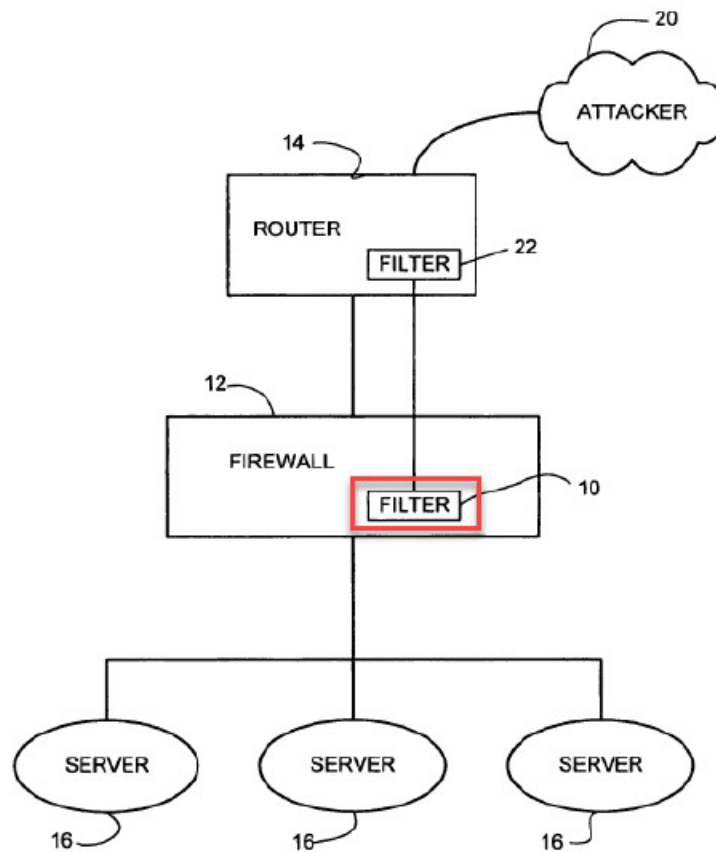
However, we do not find the showing is limited to “source and destination.” Petitioner also alleges a person of ordinary skill in the art “would recognize that the data packets are *received at said host computer* at least because the ACL classifier classifies ‘received packets 78,’ which are transmitted to and received by destination device 74, the host computer, via communication link 68, as shown in Fig. 4.” Pet. 66–67 (citing Ex. 1009,

5:40–44, 6:9–20, 6:38–42, Fig. 4; Ex. 1004 ¶ 213). The showing regarding Limitation [7.B], specifically Cheriton’s Figure 4, meets our preliminary construction of “path.” *See id.* at 66 (citing Ex. 1009, Fig. 4); *see also* Section III.B.1 above (“path” construction). The illustrated “communication link” of Figure 4 also shows a “routing device 72.”

4. Claims 8 and 9

Patent Owner disputes that the Petitioner has shown Limitation [8.C], “determining the rate at which data packets of each class are transmitted from a router to said computer.” Prelim. Resp. 32–35. Patent Owner argues that “Cheriton identities source of potentially harmful data package and limits the transmission rate of the identified sources.” *Id.* at 34 (citing Ex. 1009, 5:28–29, 6:66–7:24, 8:37–34). According to Patent Owner, Cheriton doesn’t need “to determine the rate at which data packets of each class are transmitted from a router to said computer.” *Id.* at 34–35.

Petitioner argues Cheriton teaches that “flows classified by ACL [Access Control List] classifier 80 can be analyzed by a flow analyzer 122.” Pet. 69 (citing Ex. -1009, 7:9–12, Fig. 6; Ex. 1004 ¶ 222). Figure 1 is annotated by Petitioner and is reproduced below.



Cheriton Figure 1 annotated is a diagram illustrating a firewall located between a router and a plurality of servers with an attacker sending data into the router.

Pet. 71; Ex. 1009, 3:3–5. Petitioner argues Figure 1 annotated shows a “rate at which data packets are transmitted.” *Id.* (citing Ex. 1009, 8:7–14, Fig. 1 (annotated); Ex. 1004 ¶ 224). The flow analyzer “monitors statistics associated with the aggregate filters 10.” Ex. 1009, 7:58–59. Petitioner argues the statistics monitored include the rate at which data packets are transmitted and detection of anomalies, including “rate of packets.” Pet. 71 (citing Ex. 1009, 8:7–14, 8:23–27; Ex. 1004 ¶ 224).

On this record, we preliminarily find Petitioner has sufficiently shown Cheriton teaches Limitation [8.C]. In making this finding we give weight to

the Jeffay Declaration. During trial, Patent Owner may develop further argument and evidence regarding its argument that Cheriton does not classify packets by determining the “rate” at which data packets are transmitted.

Claim 9 depends from claim 8. Patent Owner relies on its arguments for claim 8 to assert that claim 9 has not been shown. Prelim. Resp. 35.

On this record, Petitioner has sufficiently shown all limitations of claims 8 and 9 are taught by the combination of Cheriton and Doeppner.

5. Claim 10

Patent Owner’s arguments for independent claim 10 are the same as those made for claim 8. Prelim. Resp. 35. We refer to our prior analysis of Limitation [7.B]. *See* Section III.F.4 above.

Petitioner relies on its showing regarding claim 7, which is alleged to be analogous. Pet. 75.

On this record, Petitioner has sufficiently shown the subject matter of claim 10 is taught by the combination of Cheriton and Doeppner.

6. Claims 11 and 12

Petitioner relies on its showing for claim 8 to meet all the limitations of claim 11. Pet. 79–80. Patent Owner argues the combination of “Cheriton and Doeppner does not teach limiting transmission rate of routers, while limitations 11[B] -11[E] [all] relate to limitation of transmission rate of routers.” Prelim. Resp. 36. We question Petitioner’s showing of the determination rate recited in Limitation [11.C] is made by a first of two claimed routers.

Claim 12 depends from claim 11. Patent Owner relies on its arguments for claim 11 to assert that claim 12 has not been shown. Prelim. Resp. 37.

On this record, we question whether Petitioner has sufficiently shown all limitations of claims 11 and 12 are taught by the combination of Cheriton and Doeppner.

7. Conclusion

Petitioner has shown a reasonable likelihood that claims 7–10 would have been obvious over Cheriton and Doeppner. We question whether Petitioner has sufficiently shown the combination teaches all the limitations of claims 11 and 12.

G. Obviousness of Claims 7–12 over Cheriton and Savage

Petitioner alleges claims 7–12 would have been obvious over Cheriton and Doeppner or Savage. Pet. 81–89. Petitioner also relies on the Jeffay Declaration. Ex. 1004 ¶¶ 259–302.

1. Cheriton (Ex. 1006)

Cheriton was described in Section III.F.1 above.

2. Savage (Ex. 1008)

Savage is described in Section III.E.2 above.

3. Claim 7

Petitioner provides four reasons a person of ordinary skill in the art would have combined Cheriton and Savage. Pet. 81–83. The reasons are either the same or similar to those discussed in the Wetherall and Doeppner combination and are not disputed by Patent Owner at this time. We find the reasons sufficient.

Patent Owner denies that Cheriton and Savage teach Limitation [7.B]. Prelim. Resp. 37. We preliminarily determine Petitioner has sufficiently shown the subject matter of claim 7 is taught by the combination of Cheriton and Savage. Pet. 81–83.

4. Claims 8 and 9

Patent Owner denies, without any corresponding persuasive argument, that Cheriton and Savage teach Limitations [8.C], [8.D], and [8.E]. Prelim. Resp. 37. Patent Owner specifically denies that Savage teaches “limiting transmission rate of routers.” *Id.* We preliminarily determine Petitioner has sufficiently shown the subject matter of claim 8 is taught by the combination of Cheriton and Savage. Pet. 84–85.

Claim 9 depends from claim 8. Patent Owner relies on its arguments for claim 8 to assert claim 9 has not been shown. Prelim. Resp. 38.

On this record, Petitioner has sufficiently shown all limitations of claims 8 and 9 are taught by the combination of Cheriton and Savage.

5. Claim 10

Patent Owner denies that Cheriton and Savage teach Limitation [10.B]. Prelim. Resp. 38. We preliminarily determine Petitioner has sufficiently shown the subject matter of claim 10 is taught by the combination of Cheriton and Savage. Pet. 86–87.

On this record, Petitioner has sufficiently shown all limitations of claim 10 is taught by the combination of Cheriton and Savage.

6. Claims 11 and 12

Petitioner relies on its showing for claim 8 to meet all the limitations of claim 11. Pet. 87–88. Patent Owner argues “[Cheriton and] Savage do not teach limiting transmission rate of routers, while limitations 11[B] - 11[E] are relate to limitation of transmission rate of routers.” Prelim. Resp. 38. We question Petitioner’s showing of the determination rate recited in Limitation [11.C] is made by a first of two claimed routers.

Claim 12 depends from claim 11. Patent Owner relies on its arguments for claim 11 to assert that claim 12 has not been shown. Prelim. Resp. 38.

On this record, we question whether Petitioner has sufficiently shown that all the limitations of claims 11 and 12 are taught by the combination of Cheriton and Savage.

7. Conclusion

Petitioner has shown a reasonable likelihood that claims 7–10 would have been obvious over Cheriton and Savage. We question whether Petitioner has sufficiently shown that the combination teaches all the limitations of claims 11 and 12.

IV. CONCLUSION

As explained above, we determine that Petitioner has established a reasonable likelihood of prevailing in its challenge to at least one claim of the '497 patent. Thus, we institute an *inter partes* review of all challenged claims on all asserted grounds. *See SAS Inst.*, 138 S. Ct. at 1356.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that *inter partes* review is *instituted* with respect to all claims and all grounds of unpatentability raised in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(a), *inter partes* review of the '497 patent is hereby instituted commencing on the entry date of this Order, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial.

IPR2023-00544
Patent 7,523,497 B2
PETITIONER:

Craig Tolliver
John Heuton
CHARHON CALLAHAN ROBSON & GARZA, PLLC
ctolliver@ccrglaw.com
jheuton@ccrglaw.com

PATENT OWNER:

Jacob B. Henry
William P. Ramey, III
RAMEY LLP
jhenry@rameyfirm.com
wramey@rameyfirm.com