

Patent No. 7,523,497
Petition For *Inter Partes* Review

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CLOUDFLARE, INC.
Petitioner,

v.

PACSEC3, LLC
Patent Owner.

Patent No. 7,523,497

Inter Partes Review No. IPR2023-00544

PETITION FOR *INTER PARTES* REVIEW

UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42.100 *et seq.*

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. SUMMARY OF THE '497 PATENT	1
A. Background of the '497 patent	1
1. Problems identified in the prior art	1
2. Limiting bandwidth for unwanted packets	2
B. Prosecution History of the '497 patent	3
C. <i>Ex Parte</i> Reexamination	4
D. Level of Ordinary Skill	5
III. CLAIM CONSTRUCTION	5
IV. PRECISE REASONS FOR RELIEF REQUESTED	6
V. WETHERALL IN VIEW OF DOEPPNER OR SAVAGE RENDERS OBVIOUS CLAIMS 7-12	7
A. Summary of Wetherall	7
B. Ground 1: Claims 7-12 are Obvious in View of Wetherall and Doeppner	10
1. Summary of Doeppner	10
2. Doeppner is § 102(a) prior art to the '497 patent	11
3. Claim 7	12
4. Claim 8	26
5. Claim 9	31
6. Claim 10	33
7. Claim 11	40
8. Claim 12	43
C. Ground 2: Claims 7-12 are Obvious in View of Wetherall and Savage	44
1. Summary of Savage	44
2. Savage is § 102(a) prior art to the '497 patent	46
3. Claim 7	47

TABLE OF CONTENTS
(continued)

	Page
4. Claim 8.....	51
5. Claim 9.....	54
6. Claim 10.....	54
7. Claim 11.....	57
8. Claim 12.....	58
VI. CHERITON IN VIEW OF DOEPPNER OR SAVAGE RENDERS	
OBVIOUS CLAIMS 7-12	59
A. Summary of Cheriton	59
B. Ground 3: Claims 7-12 are Obvious in View of Cheriton and Doeppner	61
1. Claim 7	61
2. Claim 8.....	69
3. Claim 9.....	73
4. Claim 10.....	75
5. Claim 11.....	79
6. Claim 12.....	80
C. Ground 4: Claims 7-12 are Obvious in View of Cheriton and Savage.....	81
1. Claim 7.....	81
2. Claim 8.....	84
3. Claim 9.....	85
4. Claim 10.....	86
5. Claim 11.....	87
6. Claim 12.....	88
VII. DISCRETIONARY DENIAL WOULD BE INAPPROPRIATE AND	
IMPROPER	89
A. District Court Litigation.....	89

TABLE OF CONTENTS
(continued)

	Page
B. <i>Ex Parte</i> Reexamination.....	92
VIII. NOTICES AND STATEMENTS.....	94
IX. CONCLUSION.....	97

TABLE OF AUTHORITIES

	Page(s)
 Cases	
<i>Acceleration Bay, LLC v. Activision Blizzard, Inc.</i> , 908 F.3d 765 (Fed. Cir. 2018)	11
<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH</i> , IPR2019-01469, Paper 6 (Feb. 13, 2020) (designated precedential on March 24, 2020).....	92
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (designated precedential on May 5, 2020).....	90-91
<i>Apple Inc. v. Jawbone Innovations, LLC</i> , IPR2022-01084, Paper 9 (PTAB December 16, 2022)	91
<i>Beckman Coulter, Inc. v. Sirigen II Ltd.</i> , IPR2022-01203, Paper 12 (PTAB January 6, 2023)	90
<i>In re Hall</i> , 781 F.2d 897 (Fed. Cir. 1986)	11
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	5
 Statutes	
35 U.S.C. § 102	5
35 U.S.C. § 102(a)	12, 47
35 U.S.C. § 102(e)	7, 59
35 U.S.C. § 103	5, 6
35 U.S.C. § 314	89
35 U.S.C. §§ 311-319	6

35 U.S.C. § 325(d)	92
--------------------------	----

Other Authorities

37 C.F.R. § 42.8(b)(1).....	94
37 C.F.R. § 42.8(b)(2).....	94
37 C.F.R. § 42.8(b)(3).....	96
37 C.F.R. § 42.8(b)(4).....	96
37 C.F.R. § 42.15(a).....	97
37 C.F.R. § 42.100 <i>et seq.</i>	6
37 C.F.R. § 42.104(a).....	96
37 C.F.R. § 42.104(b)	6
37 C.F.R. § 42.104(b)(4).....	7
Vidal, K., <i>Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation</i> (USPTO June 21, 2022).....	91

EXHIBIT LIST

Exhibit Description	Exhibit #
U.S. Patent No. 7,523,497 to Cohen (“the ’497 patent”)	EX-1001
Prosecution History of U.S. Patent No. 7,523,497	EX-1002
Prosecution History of <i>Ex Parte</i> Reexamination Control No. 90/014,746	EX-1003
Declaration of Kevin Jeffay in Support of Petition for <i>Inter Partes</i> Review of U.S. Patent No. 7,523,497	EX-1004
<i>Curriculum Vitae</i> of Kevin Jeffay	EX-1005
U.S. Patent No. 6,801,503 to Wetherall <i>et al.</i> (“Wetherall”)	EX-1006
Doeppner, T., <i>et al.</i> , “Using Router Stamping to Identify the Source of IP Packets” (November 1, 2000) (“Doeppner”)	EX-1007
Savage, S., <i>et al.</i> , “Practical Network Support for IP Traceback” (“Savage”)	EX-1008
U.S. Patent No. 7,120,931 to Cheriton (“Cheriton”)	EX-1009
Patent Owner’s Infringement Contentions in litigation of same ’497 patent	EX-1010
Declaration of Scott Delman dated June 8, 2022	EX-1011
Declaration of Scott Delman dated April 1, 2021	EX-1012
[Reserved]	EX-1013
Song, D., <i>et al.</i> , “Advanced and Authenticated Marking Schemes for IP Traceback,” Report No. UCB/CSD-00-1107, University of California, Berkeley (June 2000)	EX-1014

Exhibit Description	Exhibit #
U.S. Patent No. 6,839,321 to Chiruvolu	EX-1015
U.S. Publication No. 2003/0118029 to Maher III <i>et al.</i>	EX-1016
U.S. Patent No. 6,904,529 to Swander	EX-1017
U.S. Patent No. 6,385,170 to Chiu <i>et al.</i>	EX-1018
U.S. Patent No. 6,934,256 to Jacobson <i>et al.</i>	EX-1019
U.S. Patent No. 7,027,393 to Cheriton	EX-1020
“RFC 1009 – Requirements for Internet Gateways” Braden <i>et al.</i>	EX-1021
U.S. Patent No. 6,115,357 to Packer <i>et al.</i>	EX-1022
U.S. Patent No. 6,412,000 to Riddle <i>et al.</i>	EX-1023
U.S. Patent No. 5,581,559 to Crayford <i>et al.</i>	EX-1024
U.S. Patent No. 6,044,402 to Jacobson <i>et al.</i>	EX-1025
U.S. Patent No. 5,455,865 to Perlman	EX-1026
U.S. Patent No. 5,353,353 to Vijeh <i>et al.</i>	EX-1027
U.S. Patent No. 5,850,515 to Lo <i>et al.</i>	EX-1028
U.S. Patent No. 5,367,523 to Chang <i>et al.</i>	EX-1029
U.S. Patent No. 7,058,974 to Maher III <i>et al.</i>	EX-1030
U.S. Patent No. 6,725,378 to Schuba <i>et al.</i>	EX-1031
U.S. Patent No. 7,058,015 to Wetherall <i>et al.</i>	EX-1032
U.S. Patent No. 6,889,181 to Kerr <i>et al.</i>	EX-1033

Exhibit Description	Exhibit #
Wayback Machine archive of http://www.ccs2000.org/	EX-1034
Wayback Machine archive of http://www.acm.org/sigcomm/sigcomm2000/conf/techprog.htm	EX-1035
ACM SIGCOMM Conference 2000 Preliminary Technical Program	EX-1036
Standing Order Governing Proceedings (Judge Alan D. Albright, United States District Court for the Western District of Texas, Waco Division)	EX-1037
Current docket in <i>PacSec3, LLC v. Cloudflare, Inc.</i> , Case No. 6:22-cv-00129 (W.D. Tex.)	EX-1038
Current docket in <i>PacSec3, LLC v. Darktrace, PLC</i> , Case No. 6:22-cv-00126 (W.D. Tex.)	EX-1039

I. INTRODUCTION

Petitioner Cloudflare, Inc. (“Cloudflare”) petitions for *inter partes* review of claims 7-12 of U.S. Patent No. 7,523,497 (“the ’497 patent” (EX-1001)). The ’497 patent is directed to minimizing the effects of packet flooding attacks against computers or routers connected to a network. The challenged claims do not present any patentable improvement over the prior art, as set forth in this Petition and in the supporting Declaration of Dr. Kevin Jeffay (EX-1004).

Petitioner requests that the Board institute *inter partes* review of the ’497 patent and cancel the claims at the conclusion of the instituted proceeding.

II. SUMMARY OF THE ’497 PATENT

A. Background of the ’497 patent

1. Problems identified in the prior art

According to the ’497 patent, its “primary objective” 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. . . thereby making more valuable communication with the victim slow or unreliable.” (EX-1001, 2:6-10.) In such attacks, it can be assumed that the attacker “will never cooperate” with the victim. (EX-1001, 1:65-67.) For example, the attacker may falsify packet data, such as source address information. (EX-1001, 2:3-5.) Thus, network control techniques

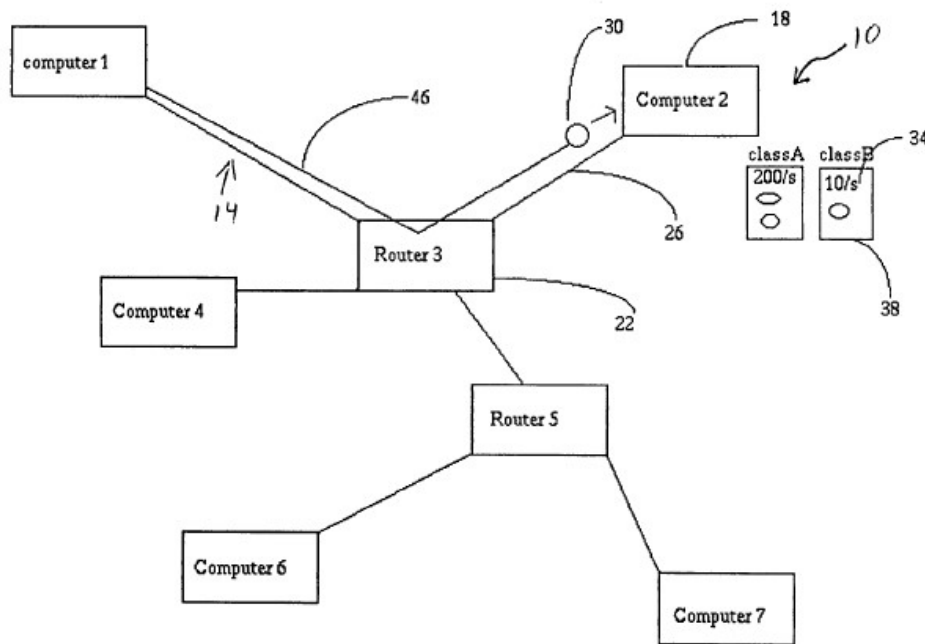
that rely on packets to contain accurate information are poorly suited to packet flooding attacks. (EX-1004, ¶45.)

2. Limiting bandwidth for unwanted packets

Data packets in a network can be classified as “wanted packets” or “unwanted packets”; unwanted packets are supplied by an attacker in a packet flooding attack, and wanted packets are legitimate network traffic. (EX-1001, 2:54-3:12.) Network bandwidth can be limited (e.g., by transmission rate) for unwanted packets, freeing resources for legitimate traffic. (EX-1001, 3:4-23, 6:16-20; EX-1004, ¶46.)

Wanted packets and unwanted packets can be identified based on a path that a packet takes to a host computer. For example, with respect to Fig. 1 (below), “Means are also provided for the computer 18 to find information for packets 30 it receives regarding the path 46 by which the packets 30 came to the computer 18. Thus, the computer 18 can use the information to allocate the processing rate for each class 38 in a desired way among the places from which packets 30 are transmitted.” (EX-1001, 6:12-25.)

Figure 1



(EX-1001, Fig. 1.)

Routers in a computer network can be utilized to identify unwanted packets and to limit their transmission rate. For example, “cooperating routers will limit the rate at which they forward packets to places that so request,” which is “useful for limiting the bandwidth used by ‘unwanted’ packets.” (EX-1001, 3:4-8.) Allocating bandwidth by path can be performed “via packet marks provided by routers leading up to the victim.” (EX-1001, 3:64-66.)

B. Prosecution History of the '497 patent

The application that became the '497 patent is a continuation filed on May 7, 2004, claiming priority to an application filed on November 16, 2000. For this

Petition, Petitioner assumed a priority date of November 16, 2000 for the challenged claims.

After amendment, the claims were allowed because the Examiner believed “path information forwarding along the entire path to the victim, said path information encompassing the entire path through the associated routers, and subsequent use of said information to effect filtering via allocation of packet processing rate” to be novel over the prior art. (EX-1002, 31-32.) As set forth in this Petition, however, the prior art does in fact disclose all limitations of the challenged claims.

C. *Ex Parte* Reexamination

On May 3, 2021, Unified Patents, LLC submitted a request for *ex parte* reexamination (Control No. 90/014,746) of claims 1, 4, 7, 10, 13, and 16 of the ’497 patent. (EX-1003, 321.) (Unified Patents is unaffiliated with Petitioner and uninvolved in this Petition.) On June 17, 2021, the USPTO granted the reexamination request. (EX-1003, 270-283.) In the Order, the USPTO found a substantial new question of patentability based on three prior art references: Savage, Schuba, and Maher. (EX-1003, 273.)

In a Non-Final Office Action dated Nov. 12, 2021, and again in a Final Office Action dated March 16, 2022, the USPTO rejected claims 1, 4, 13, and 16 under §

102; rejected claim 7 under § 103; and confirmed claim 10 as patentable. (EX-1003, 153-184.) The reexamination is on appeal to the Patent Trial and Appeal Board.

D. Level of Ordinary Skill

Based on the disclosure of the '497 patent and a priority date of November 16, 2000, a person of ordinary skill in the art ("POSITA") 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. (EX-1004, ¶53.)

III. CLAIM CONSTRUCTION

The Board construes claims under *Phillips*, giving claims their ordinary and customary meaning in light of the specification. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315-17 (Fed. Cir. 2005). Petitioner does not believe any claim construction is necessary for this Petition.

The '497 patent is the subject of litigation as discussed in Section VII. Patent Owner's lawsuit against Petitioner is at the earliest stages, and no infringement contentions have been exchanged. For this Petition, Petitioner has sought to apply (without concession and where applicable) its understanding of Patent Owner's interpretation of claim scope based on its publicly available infringement contentions applying the '497 patent against other parties.

IV. PRECISE REASONS FOR RELIEF REQUESTED

Pursuant to 35 U.S.C. §§ 311-319 and 37 C.F.R. § 42.100 *et seq.* (including § 42.104(b)), Petitioner requests cancellation of claims 7-12 of the '497 patent based on the following references and the accompanying Declaration of Dr. Kevin Jeffay (EX-1004).

Prior Art Reference	Abbreviation
U.S. Patent No. 6,801,503 to Wetherall <i>et al.</i>	Wetherall (EX-1006)
Doeppner, T., <i>et al.</i> , “Using Router Stamping to Identify the Source of IP Packets” (November 1, 2000)	Doeppner (EX-1007)
Savage, S., <i>et al.</i> , “Practical Network Support for IP Traceback”	Savage (EX-1008)
U.S. Patent No. 7,120,931 to Cheriton	Cheriton (EX-1009)

The statutory grounds for the challenge of each claim are set forth below. The statutory citations are pre-AIA based on a priority date of November 16, 2000.

Ground	35 U.S.C. §	Claims(s)	Prior Art Reference(s)
1	103	7-12	Wetherall, Doeppner
2	103	7-12	Wetherall, Savage
3	103	7-12	Cheriton, Doeppner
4	103	7-12	Cheriton, Savage

Below, Petitioner discusses why the challenged claims are unpatentable, including by specifying how and where the prior art satisfies each limitation of each challenged claim, per 37 C.F.R. § 42.104(b)(4).¹ Petitioner's showing establishes a reasonable likelihood that it will prevail on each ground of invalidity as to each challenged claim.

V. WETHERALL IN VIEW OF DOEPPNER OR SAVAGE RENDERS OBVIOUS CLAIMS 7-12

A. Summary of Wetherall

Wetherall is a U.S. patent filed on Oct. 9, 2000 that issued on Oct. 5, 2004. It is prior art to the '497 patent under at least 35 U.S.C. § 102(e).

Wetherall relates to regulating network traffic in a computer network, such as defending against denial-of-service (“DoS”) attacks against the network. (EX-1006, 1:52-55.) In Wetherall, an example computer network 100 includes a server 110 coupled to routers 106a-106h, which deliver data packets between clients 108a, 108b and the server. (EX-1006, 3:27-32, Fig. 1; EX-1004, ¶56.)

¹ Petitioner also shows how each claim preamble is satisfied, but does not concede that any preamble is limiting.

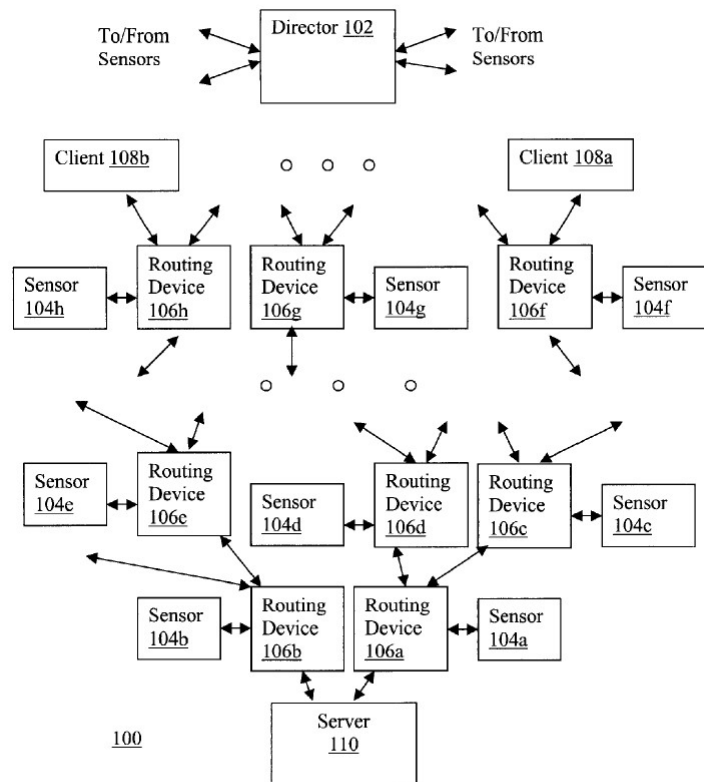


Figure 1

(EX-1006, Fig. 1.)

Director 102 manages data packet traffic. The director receives network traffic data from sensors 104a-104h, which may be incorporated within the routers. (EX-1006, 4:57-62; EX-1004, ¶57.) Director 102 provides regulation instructions to the routers based on the network traffic data and on a “not-to-exceed” network traffic profile. (EX-1006, 3:60-62, 4:62-66; EX-1004, ¶57.) The routers can execute the regulation instructions by “rate limiting” network traffic in accordance with the profile, which can specify bandwidth limits for particular types of network traffic. (EX-1006, 3:47-53, 3:62-65; EX-1004, ¶57.)

In Wetherall, the traffic data can be used to divide the traffic into different types. (EX-1006, 6:22-48; EX-1004, ¶58.) For example, data packets can be divided into traffic types based on source and destination address information in the packets; the routers can then regulate (e.g., rate limit) the data packets independently for each type as shown in exemplary Fig. 2 below. (EX-1006, 6:40-48; EX-1004, ¶58.)

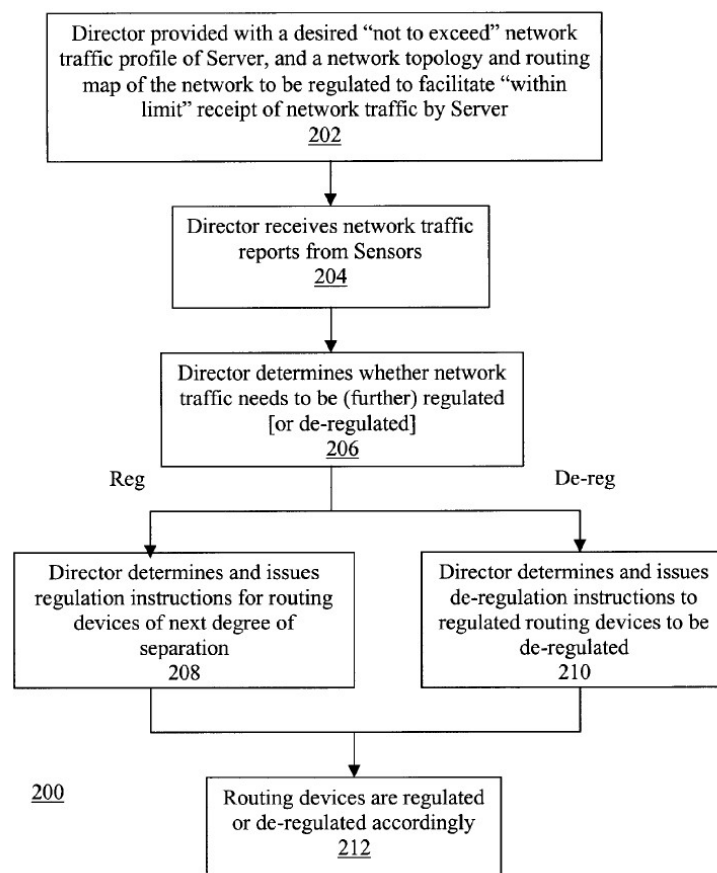


Figure 2

(EX-1006, Fig. 2.)

Packets of a specific type (e.g., packets having particular source/destination addresses) thus can be rate-limited, such that an attacker's packets will "minimally

interfere[] with the legitimate or desirable traffic.” (EX-1006, 7:48-52; EX-1004, ¶59.)

B. Ground 1: Claims 7-12 are Obvious in View of Wetherall and Doeppner

1. Summary of Doeppner

Doeppner is a printed publication that was publicly accessible in the United States at least by November 1, 2000 as discussed below.

Doeppner relates to defending against DoS attacks on a computer network. (EX-1007, 184.) Doeppner describes “router stamping” techniques that identify the path (e.g., source and destination) of a data packet. (EX-1007, 184-185.) In Doeppner, a router “stamps” a data packet with an IP address corresponding to the previous router, such as shown in Fig. 1. (EX-1007, 184-185, Fig. 1.) The data packet’s path can then be determined based on packet marks. (EX-1007, 187.)

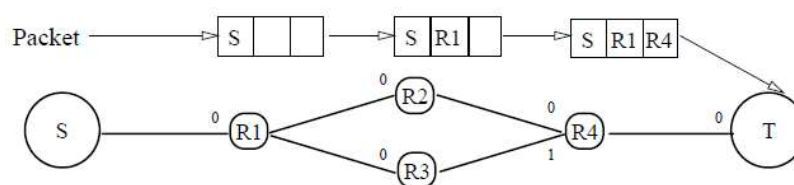


Figure 1: The packet travels from *S* to *T* via routers *R*₁, *R*₂ and *R*₄. Each router records the IP address of its predecessor before it forwards the packet.

(EX-1007, Fig. 1.)

In some embodiments, the packet marks are applied deterministically (i.e., every router in a path marks a packet with the forwarding router’s IP address). (EX-

1007, 185, Fig. 1; EX-1004, ¶63.) The packet marks can also be applied probabilistically. (EX-1007, 185, Fig. 1.)

Doeppner explains that the packet marks 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, 187-188; EX-1004, ¶64.) One such filter can drop only packets that “come from the compromised area.” (EX-1007, 188; EX-1004, ¶64.)

2. Doeppner is § 102(a) prior art to the ’497 patent

“Public accessibility” is “the touchstone in determining whether a reference constitutes a printed publication.” *In re Hall*, 781 F.2d 897, 899 (Fed. Cir. 1986) (internal quotations omitted). A reference is considered “publicly accessible” if it was “disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.” *Acceleration Bay, LLC v. Activision Blizzard, Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018) (internal citation omitted). Doeppner was published by the Association for Computing Machinery (ACM), in its ordinary course of business, in connection with its well-known and public CCS ’00 conference. (EX-1011, ¶¶5-7; EX-1004, ¶61.) The June 8, 2022 declaration of Scott Delman explains that Doeppner was made available to the general public on an unrestricted basis by at least November 1, 2000, which precedes the ’497 patent’s priority date. (EX-1011,

¶11; EX-1004, ¶61.) The archived copy of the CCS '00 website corroborates this publication date by identifying Doeppner as an “accepted paper” for CCS '00. (EX-1034, 2; EX-1004, ¶61.) Doeppner itself indicates it was presented at CCS '00 and published. (EX-1007, 184; EX-1004, ¶60.) As Dr. Kevin Jeffay states, ACM has long published the proceedings of conferences such as CCS '00, including the presented papers, and made those proceedings available to the public. (EX-1004, ¶61.) And Doeppner’s formatting is consistent with Dr. Jeffay’s experiences with ACM publications for ACM conferences. (EX-1004, ¶61.)

Accordingly, Doeppner was publicly accessible to the POSITA at least by November 1, 2000. (EX-1004, ¶¶60-61.) It is thus prior art under at least 35 U.S.C. § 102(a).

3. Claim 7

Wetherall in combination with Doeppner meets each limitation of claim 7. The references would have been readily combinable by a POSITA.

First, Wetherall and Doeppner belong to the same field of endeavor (computer network traffic management) and are directed to the same problem (defending against DoS attacks, including packet flooding attacks, against a network). (EX-1004, ¶66.)

Second, a POSITA would have been motivated to combine Doeppner with Wetherall to solve a problem identified in Doeppner. In a DoS attack, the source

address in a packet header cannot be trusted, because header data can be manipulated (“spoofed”) by the attacker; and a DoS defense system that relies on header data can inadvertently penalize legitimate traffic. (EX-1007, 184; EX-1004, ¶67.) This is analogous to a problem identified in the ’497 patent. (EX-1001, 1:63-2:5; EX-1004, ¶67.)

Wetherall, by itself, offers no solution to this problem. (EX-1004, ¶68.) A POSITA would have been motivated to apply Doeppner’s solution for source tracing (which can identify an attacker’s source even when packet header data has been falsified) to Wetherall’s teachings of rate-limiting traffic based on, *e.g.*, its source and destination addresses. (EX-1007, 184; EX-1006, 6:40-48; EX-1004, ¶68.) The POSITA would have realized a technical advantage: improving Wetherall’s system by more precisely targeting attack traffic, rather than legitimate traffic. (EX-1004, ¶68.)

Third, Doeppner invites combination with Wetherall by expressly suggesting that, upon identifying the source of attack packets, those packets can be isolated and filtered. (EX-1007, 186-188; EX-1004, ¶69.) Wetherall teaches techniques for isolating and filtering the packets. (*See, e.g.*, EX-1006, 1:44-2:14; EX-1004, ¶69.)

Fourth, Wetherall’s and Doeppner’s teachings are implemented on analogous computer components, such as computer networks with host computers, routers, and communication lines. (EX-1004, ¶70.) Doeppner “can be used in conjunction with”

other defense measures, such as in Wetherall. (EX-1007, 189.) Doeppner's teachings are "inexpensive to implement and maintain," permit a "variety of modifications," can cooperate with "poorly maintained, noncompliant, or compromised systems," and offer "flexibility in selecting the tools." (EX-1007, 188-189; EX-1004, ¶71.) Doeppner's implementations were thus well known, inexpensive, fault tolerant, and adaptable. (EX-1007, 188; EX-1004, ¶71.) The combination of Doeppner with Wetherall thus would have yielded predictable results with a reasonable expectation of success. (EX-1004, ¶71.)

a. [Preamble] *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:*

The preamble is taught by Wetherall in view of Doeppner. 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." (EX-1006, 1:44-55.) DoS attacks include packet flooding attacks. (EX-1004, ¶72; EX-1001, Abstract.)

Example network 100 in Wetherall shows a plurality of host computers (e.g., server 110) and routers (e.g., routing devices 106a-106h). (EX-1006, 3:9-15, 3:23-39, 9:60-64, Fig. 1, Fig. 8.) Communication lines are disclosed at least by routing devices 106a-106h being "coupled to each other and to server 110" in example

network 100, and by communications interfaces 810 and system bus 812 for example host computer system 800. (EX-1006, 3:23-39, 10:1-7, Fig. 8; EX-1004, ¶73.) These communication lines are for “routing network traffics”—that is, “transmitted data packets.” (EX-1006, 3:23-39, 10:1-10; EX-1004, ¶73.)

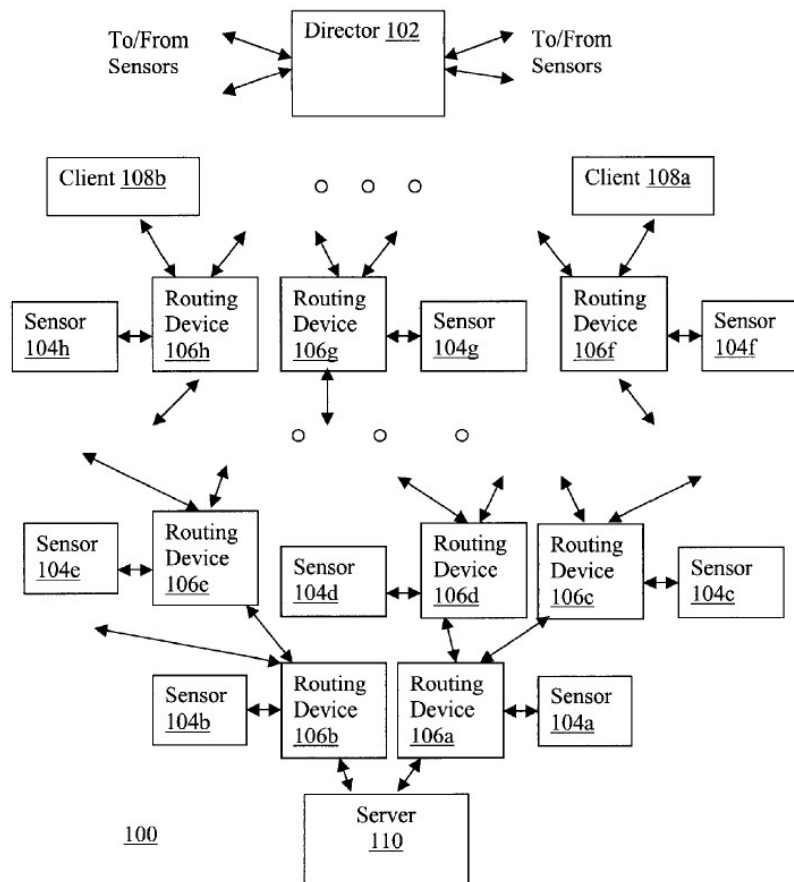


Figure 1

(EX-1006, Fig. 1.)

Additionally, Doeppner discloses using “router stamping” techniques to “implement a successful defense against a *DoS* attack.” (EX-1007, 184, 186-187.)

Like Wetherall, Doeppner's disclosures apply to computer networks, such as the Internet, with host computers, routers, communication lines, and transmitted data packets. (EX-1004, ¶74.)

- b. ***[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;***

Wetherall in view of Doeppner teaches this element. For example, Doeppner describes "router stamping" to "track or to trace the flood of malicious IP packets" in a DoS attack. (EX-1007, 184; EX-1004, ¶75.) A router in a network receives a packet from a forwarding router and can mark the packet by writing a "stamp" into the packet's IP header. (EX-1007, 185; EX-1004, ¶75.) The stamp includes "the IP address of the router and the interface on which the packet was received." (EX-1007, 185; EX-1004, ¶75.) In some embodiments, each router applies a stamp according to a probability:

Each compliant router R_i implements the following algorithm:

1. For each packet routed through R_i
2. $x \leftarrow$ random number between 0 and 1
3. if $x < sp$
4. R_i places its *stamp* into slot $\lfloor x/p \rfloor$
5. R_i routes the packet

(EX-1007, 185; EX-1004, ¶75.)

Fig. 2 shows routers R1, R2, R3, and R4 marking packets in transit from source S to host computer T, according to the algorithm above:

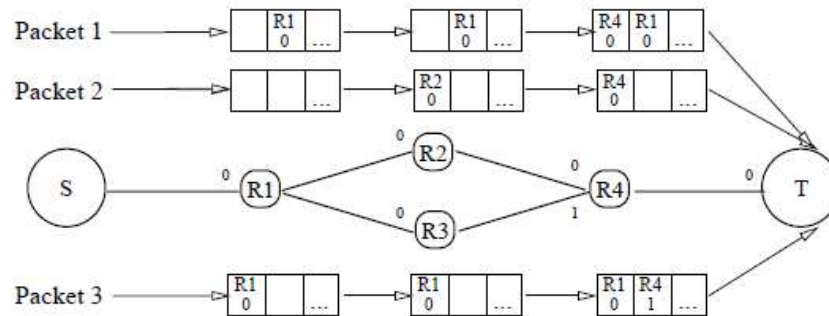


Figure 2: Packets 1, 2, 3 travel from S to T. They are processed by R1, R2, R3 and R4 which implement Router Stamping.

(EX-1007, 185, Fig. 2; EX-1004, ¶76.)

The packet marks applied by the routers in Fig. 2 meet the claimed *packet marks provided by routers leading to said host computer* at least because they are marks (i.e., IP addresses of forwarding routers) inserted into the packet by routers (i.e., routers R1, R2, R3, and R4) leading to said host computer (i.e., T). (EX-1004, ¶77.)

In a packet flooding attack, host computer T can determine the paths by which attack packets arrived at T, based on packet marks. (EX-1007, 187; EX-1004, ¶78.) This 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,” such as:

1. For each R_i
2. $x \leftarrow$ the number of packets with R_i 's stamps
3. $y \leftarrow 0$
4. For each neighbor of R_i , R_j
5. $y \leftarrow y +$ the number of packets routed to R_j
 from R_i that bear the stamps of R_j
6. If $y \gg x$
7. R_i is probably a source of malicious packets

(EX-1007, 187; EX-1004, ¶78.)

By applying this packet marking information to a “map” of routers in a network, such as shown in Fig. 2, a *path by which data packets arrive at a host computer* (e.g., R1-R2-R4; R1-R3-R4) can be determined *via packet marks provided by routers leading to said host computer*. (EX-1004, ¶79.) The path *comprises all routers in said network via which said packets are routed to said computer*: in the above example, the paths R1-R2-R4 and R1-R3-R4 include all routers via which the packets are routed from source S to host computer T. (EX-1004, ¶79.)

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

Wetherall in view of Doeppner teaches this element. For example, in Wetherall, a “director” can manage data packet traffic by instructing routers to regulate network traffic. (EX-1006, 3:60-62; EX-1004, ¶80.) This includes “rate limiting” the traffic according to a “not-to-exceed” network traffic profile that specifies bandwidth limits for particular traffic types. (EX-1006, 3:47-53, 3:62-65; EX-1004, ¶80.)

In Wetherall, routers include sensors that provide network data used to divide the network traffic into traffic types, so the routers can independently limit packets of each type as shown below. (EX-1006, 5:15-18, 6:22-48; EX-1004, ¶81.)

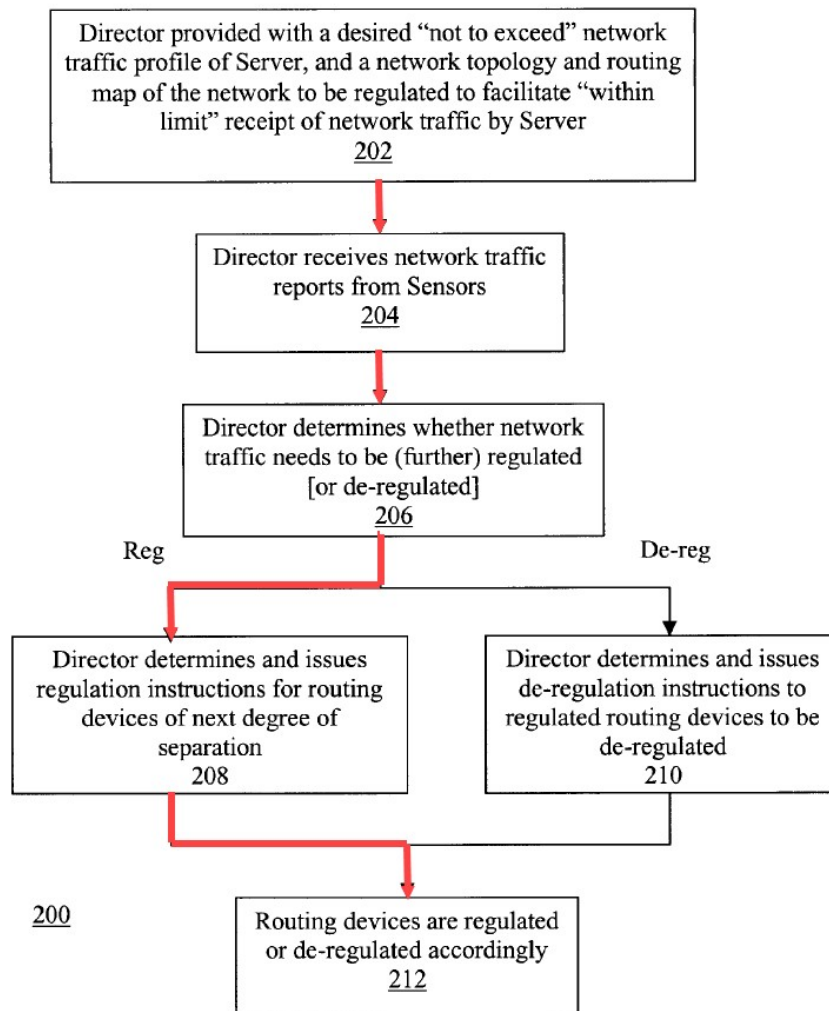


Figure 2

(EX-1006, Fig. 2 (annotated).)

By dividing network 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.” (EX-1006, 7:48-52; EX-1004, ¶82.) 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. (EX-1004, ¶82.)

The classified data packets include data packets *received at the host computer* (e.g., server 110). Wetherall describes regulating the rate of data received at “ingress interface of server 110” from the “egress interfaces of routing devices 106a and 106b,” such that the rate does not exceed the host’s limitations for a particular network traffic type. (EX-1006, 7:28-36; EX-1004, ¶83.)

Packets are classified as wanted data packets and unwanted data packets *by path*. In Wetherall, “any information carried as part of the packets may be used as typing criteria to divide the network traffic into different traffic types.” (EX-1006, 6:40-42.) This includes “specific source and destination address combinations,” which are packet header data indicating a start and end of the packet’s path in a network. (EX-1006, 6:42-45; EX-1004, ¶84.) A POSITA would understand classifying data packets by source and destination addresses to meet classifying those data packets *by path*.² (EX-1004, ¶84.)

² In its infringement contentions for the ’497 patent in a lawsuit against another party, Patent Owner cited for this claim limitation a document describing deep packet

Further, Doeppner teaches “identify[ing] and isolat[ing] problem-causing packets” in a DoS attack. (EX-1007, 186; EX-1004, ¶85.) In Doeppner, once the source of a DoS attack is determined as described for element 7[A], network traffic can be classified and filtered accordingly. (EX-1007, 187-188; EX-1004, ¶85.) For example, packets originating from source R_x and having host computer T as their destination can be blocked by routers in a network. (EX-1007, 187-188; EX-1004, ¶85.) These are *unwanted packets* associated with the DoS attack. (EX-1004, ¶85.) Meanwhile, packets not having that path (*wanted packets*) are left uninterrupted. (EX-1007, 187-188; EX-1004, ¶85.) Doeppner provides an algorithm for classifying and filtering packets:

1. While T is under attack
2. Administrator of T identifies R_x as a possible source of the malicious packets
2. Administrator of T uses the method described in Section 6.1 to verify that the stamps identifying R_x are not being forged
3. Administrator of T places a filter on all routers connected to R_x . The routers drop all packets whose destination is T and were forwarded to them by R_x

inspection that “provides information about the *source and destination* of the packet.” (EX-1010, 5 (emphasis added).)

(EX-1007, 188.)³

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

Wetherall in view of Doeppner teaches this element. In Wetherall, as shown below, 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.” (EX-1006, 3:47-53, 6:4-7; EX-1004, ¶86.)

³ In its infringement contentions against another party, Patent Owner appears to assert that *classifying data packets received at said host computer into wanted data packets and unwanted data packets by path* is met by “apply[ing] filters” to network traffic, such as in Doeppner. (EX-1010, 4.)

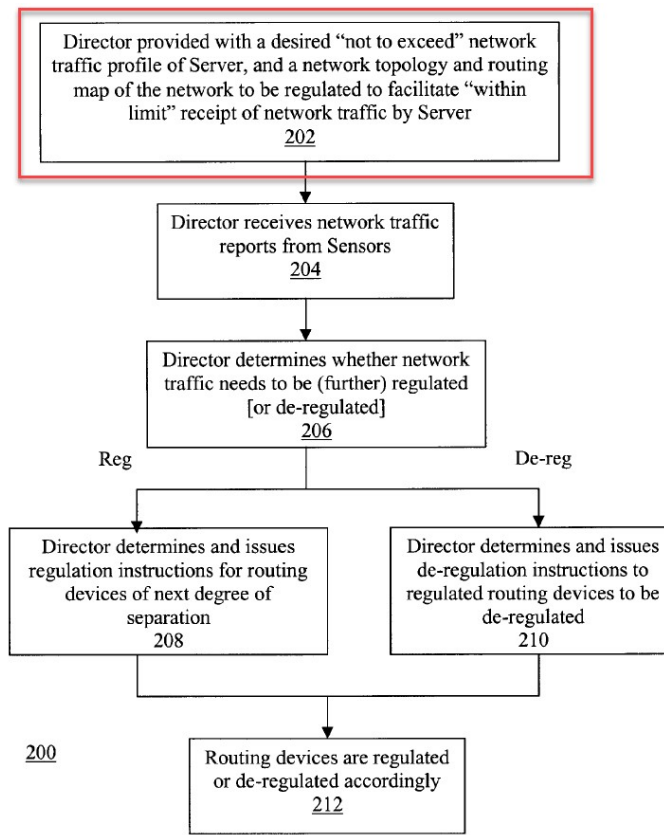


Figure 2

(EX-1006, Fig. 2 (annotated).)

The profile can specify, e.g., a maximum bandwidth, number of packets per second, or number of flows per second. (EX-1006, 3:51-57, 4:33-44, 6:7-12; EX-1004, ¶87.) A POSITA would understand these metrics to meet the claimed *maximum acceptable processing rate*. (EX-1004, ¶87.) For example, the '497 patent describes that "the rate of data packet transmissions received at the computer," such as specified in the not-to-exceed profile, "is kept below the maximum acceptable processing rate." (EX-1001, 3:56-58; *see also* EX-1006, 6:7-12, 7:28-36; EX-1004, ¶87.)

Fig. 7c of Wetherall illustrates table 720 “specifying the desired ‘not-to-exceed’ network traffic profile for a number of network traffic types for a number of servers” and including “columns 725a-725n and 726a-726n for storing the network traffic types, and their corresponding ‘not-to-exceed’ limits,” for the “various servers.” (EX-1006, 9:30-41.) Columns 726a and 726n annotated below provide *maximum acceptable processing rates* (limits), and the table *associates the rates with each class of data packet received at said host computer* (725a, 725n):

720

Server ID <u>722</u>	IP Addr <u>724</u>	Traffic Type 1 <u>725a</u>	Limit for Traffic Type 1 <u>726a</u>	...	...	Traffic Type 2 <u>725n</u>	Limit for Traffic Type n <u>726n</u>	Other Data <u>728</u>

Figure 7c

(EX-1006, Fig. 7c (annotated); EX-1004, ¶88.)

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

Wetherall in view of Doeppner teaches this element. In Wetherall, a notice is generated if “network traffics of the particular type have reached or surpassed the margin of the ‘not-to-exceed’ limit.” (EX-1006, 8:52-55; EX-1004, ¶89.) The traffic types in Wetherall include *unwanted data packets* as described above. (EX-

1004, ¶89.) Regulation instructions are provided to routers to be “regulated accordingly,” including by “*rate limiting* the excess traffic”. (EX-1006, 3:62-65, 8:65-9:1; EX-1004, ¶89.)⁴ “[I]f an ingress interface of server 110 has a bandwidth of z Mbps,” the egress interfaces of two routers “feeding this ingress interface” may be “rate limited” such that their combined bandwidth does not exceed the bandwidth limit z . (EX-1006, 7:28-36; EX-1004, ¶89.)

In Doeppner, unwanted data packets from a malicious source can be “filtered,” such as by dropping packets from that source to host computer T :

1. While T is under attack
2. Administrator of T identifies R_x as a possible source of the malicious packets
2. Administrator of T uses the method described in Section 6.1 to verify that the stamps identifying R_x are not being forged
3. Administrator of T places a filter on all routers connected to R_x . The routers drop all packets whose destination is T and were forwarded to them by R_x

(EX-1007, 188; EX-1004, ¶90.)

A POSITA would understand “drop all packets” to mean reducing a processing rate of those unwanted packets to zero, which is *less than or equal to* any *maximum acceptable processing rate for unwanted data packets*, at least because a maximum acceptable processing rate cannot be less than zero. (EX-1004, ¶91.)

⁴ All emphases herein added unless otherwise noted.

4. Claim 8

Wetherall in combination with Doeppner renders obvious each limitation of claim 8. A POSITA would have been motivated to combine Wetherall with Doeppner as described in V.B.3.

- a. ***[Preamble] 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:***

The preamble is taught by Wetherall in view of Doeppner as described above for the identical preamble of claim 7.

- b. ***[A] 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;***

This element is taught by Wetherall in view of Doeppner as described above for element 7[B].

Further, Fig. 2 of Doeppner shows a network with data packets 1, 2, and 3 routed from source S to host computer T:

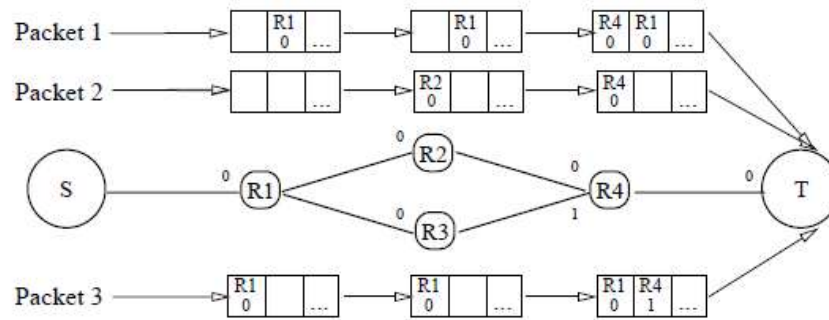


Figure 2: Packets 1, 2, 3 travel from S to T. They are processed by R₁, R₂, R₃ and R₄ which implement Router Stamping.

(EX-1007, 185; EX-1004, ¶95.)

The data packets are routed from S to T via routers R₁, R₂, R₃, and R₄. (EX-1007, 185; EX-1004, ¶96.) Packet 1 and packet 2 are routed to T from routers R₁, R₂, and R₄. (EX-1007, 185; EX-1004, ¶96.) Packet 3 is routed to T from routers R₁, R₃, and R₄. (EX-1007, 185; EX-1004, ¶96.) Accordingly, data packets 1, 2, and 3 comprise *data packets from all routers* (i.e., R₁, R₂, R₃, R₄) *in said network via which said data packets are routed to said computer* (i.e., T). (EX-1004, ¶96.)

- c. **[B] associating a maximum acceptable processing rate with each class of data packet received at said computer;**

This element is taught by Wetherall in view of Doeppner as described above for element 7[C].

- d. **[C] determining the rate at which data packets of each class are transmitted from a router to said computer;**

This element is taught by Wetherall in view of Doeppner. In Wetherall, routers monitor and report network traffic including “various statistics and

‘characteristic’ information describing the network traffic,” which a POSITA would understand to include determined data rates and other network traffic data. (EX-1006, 4:57-62, 6:26-29; EX-1004, ¶98.)

The reported data may also include, e.g., “volume of data with specific source and destination address combinations,” and “whatever data are necessary to support the employment of the desired ‘not-to-exceed’ metrics.” (EX-1006, 6:42-48.) A POSITA would understand this to include determined rates at which data packets of each class (e.g., packets having paths corresponding to the specific source and destination address combinations) are transmitted from a router to the host computer. (EX-1004, ¶99.)

- e. ***[D] receiving a maximum acceptable transmission rate for data packets being transmitted to said computer in said router; and***

This element is taught by Wetherall in view of Doeppner. For example, in Wetherall, sensors 104a-104h (which may be integrated within routing devices 106a-106h) use the commands “show interface rate-limit” and “rate-limit” to execute their rate-limiting instructions as described above. (EX-1006, 5:28-31; EX-1004, ¶100.) As Wetherall indicates, these commands were “known in the art,” were described in “product literatures from routing device manufacturers,” and thus would have been understood by the POSITA to provide maximum acceptable

transmission rates for packets transmitted to the host computer. (EX-1006, 5:25-34; EX-1004, ¶100.)

- f. [E] *controlling the rate of transmission of data packets from said router to said computer by said router so that data packet transmissions received at said computer are kept below the maximum acceptable processing rate for each data packet class; and*

This element is taught by Wetherall in view of Doeppner. In Wetherall, regulation instructions include instructions for routers to perform “rate limiting” of the network traffic. (EX-1006, 3:60-65; EX-1004, ¶101.) Chart 710 shows, for routers 712, “the regulations (i.e.,) bandwidth allocation, *rate limit* etc.) currently imposed on the various interfaces of the routing devices *for the various network traffic types* of the network nodes.” (EX-1006, 9:42-54; EX-1004, ¶101.)

710

Routing Device ID 712	IP Addr 713	Inter-face 714	Network Node 715	Regulation on Traffic Type 1 716a	...	Regulation on Traffic Type n 716n	Other Data 718

Figure 7b

(EX-1006, Fig. 7b (annotated).)

Routers 106a and 106b are coupled to server 110 and control transmission of data packets to server 110:

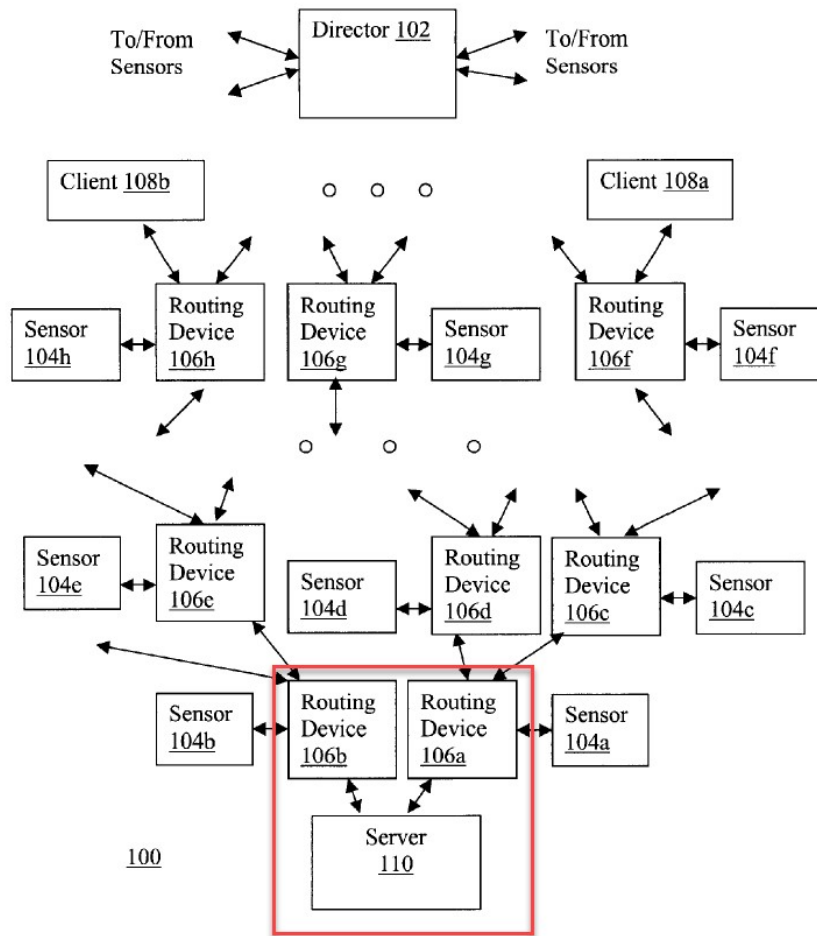


Figure 1

(EX-1006, 3:27-32, Fig. 1 (annotated); EX-1004, ¶102.)

As described above, data packets are rate-limited to adhere to a “not-to-exceed” network traffic profile, which specifies rate limits such as number of packets per second. (EX-1006, 3:60-65, 6:7-12, Fig. 7b; *see also* EX-1006, 7:28-40; EX-1004, ¶103.) The routers thus regulate data packet transmissions to the host computer such that they *are kept below the maximum acceptable processing rate for each data packet class*. (EX-1006, 6:7-12; EX-1004, ¶103.)

g. [F] *freeing a portion of the network providing data packet transmission to said computer.*

This element is taught by Wetherall in view of Doeppner. The '497 patent provides:

[T]he rate of data packet transmissions received at the computer is kept below the maximum acceptable processing rate for each data packet class by the control of the rate of transmission of data packets from the router, *thereby freeing a portion of the network providing data packet transmission to the computer.*

(EX-1001, 3:56-61.)

As described above for element 8[E], Wetherall in view of Doeppner teaches that “data packet transmissions received at said computer are kept below the maximum acceptable processing rate for each data packet class,” by “controlling the rate of transmission of data packets from the router to the computer.” (EX-1004, ¶105.) According to the '497 patent, this limiting of data packet transmissions “thereby” results in *freeing a portion of the network providing data packet transmission to the computer.* (EX-1004, ¶105.)

5. Claim 9

Wetherall in combination with Doeppner renders obvious each limitation of claim 9. A POSITA would have been motivated to combine Wetherall with Doeppner to meet the limitations of claim 9 as described above in V.B.3.

- a. **[Preamble] *A method as described in claim 8, in which:***

Wetherall in view of Doeppner teaches a method described in claim 8 as described above for claim 8.

- b. **[A] *said router receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and***

Wetherall in view of Doeppner teaches this element as described above for 8[D] and 8[E]. For example, Fig. 7b of Wetherall shows regulations, including rate limits, “for the various network traffic types of the network nodes.” (EX-1006, 9:42-54; EX-1004, ¶108.)

710

Routing Device ID <u>712</u>	IP Addr <u>713</u>	Inter- face <u>714</u>	Network Node <u>715</u>	Regulation on Traffic Type 1 <u>716a</u>	...	Regulation on Traffic Type n <u>716n</u>	Other Data <u>718</u>

Figure 7b

(EX-1006, Fig. 7b (annotated).)

Thus, the maximum acceptable transmission rate is for *each class* of data packet. (EX-1004, ¶109.)

c. **[B] *said router controls the rate of transmission of each class of data packet to said computer.***

Wetherall in view of Doeppner teaches this element as described above for 8[E].

6. Claim 10

Wetherall in combination with Doeppner renders obvious each limitation of claim 10. A POSITA would have been motivated to combine Wetherall with Doeppner to meet the limitations of claim 10 as described above for claim 7.

Claim 10 includes limitations analogous to claim 7. In claim 10, packets are received by a *router* instead of by a *host computer*, and the method recites a *transmission rate* instead of a *processing rate*. As explained above, Wetherall in view of Doeppner teaches the limitations of claim 7, in which data packets are received by a host computer. These teachings also apply to claim 10. (EX-1004, ¶112.)

For example, in Wetherall, data packets are received at a host computer (e.g., server 110) from a source (e.g., client 108a or 108b) in a computer network 100 that includes multiple routers (e.g., routers 106a-106h). (EX-1006, 3:28-39, Fig. 1; EX-1004, ¶113.) The source is connected to the host computer via the routers, which forward the data packets from the source to the host computer. (EX-1004, ¶113.) Data packets that are received by the host computer are thus also received by a router. (EX-1004, ¶113.)

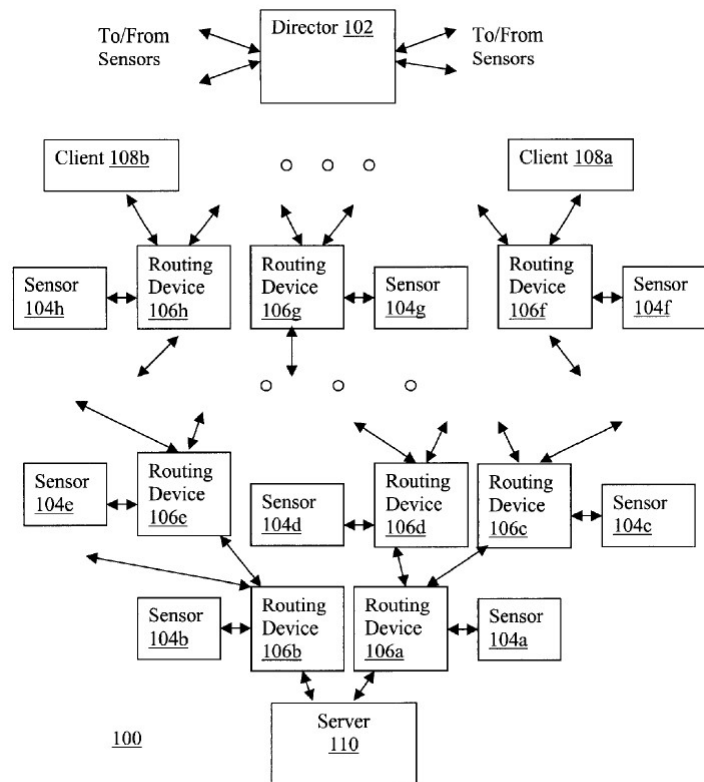


Figure 1

(EX-1006, Fig. 1.)

Doeppner describes a similar network configuration. In Fig. 2, packets travel from source S to a host computer T only via routers R1, R2, R3, and R4, such that packets received at host computer T are also received at the routers. (EX-1004, ¶114.)

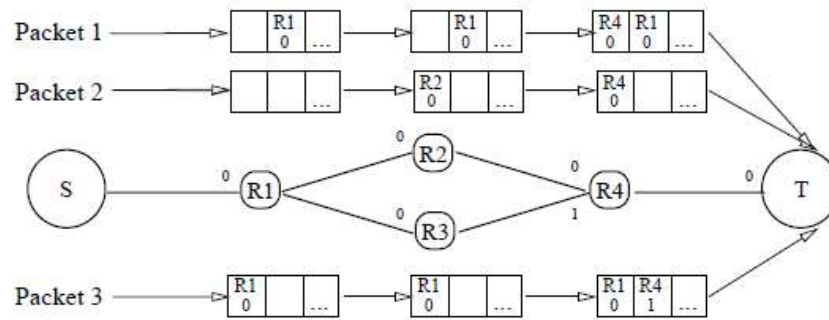


Figure 2: Packets 1, 2, 3 travel from *S* to *T*. They are processed by *R*₁, *R*₂, *R*₃ and *R*₄ which implement Router Stamping.

(EX-1007, Fig. 2.)

Additionally, in example network 100 of Wetherall, “Routing devices 106a-106h have different degrees of separation from server 110.” (EX-1006, 3:32-34; EX-1004, ¶115.) Routers 106a and 106b are one degree of separation from server 110, such that they transmit packets directly to server 110. (EX-1006, 3:35-39; EX-1004, ¶115.) Routers 106c and 106d are two degrees of separation from server 110, and transmit packets to server 110 only by transmitting them first to routing device 106a:

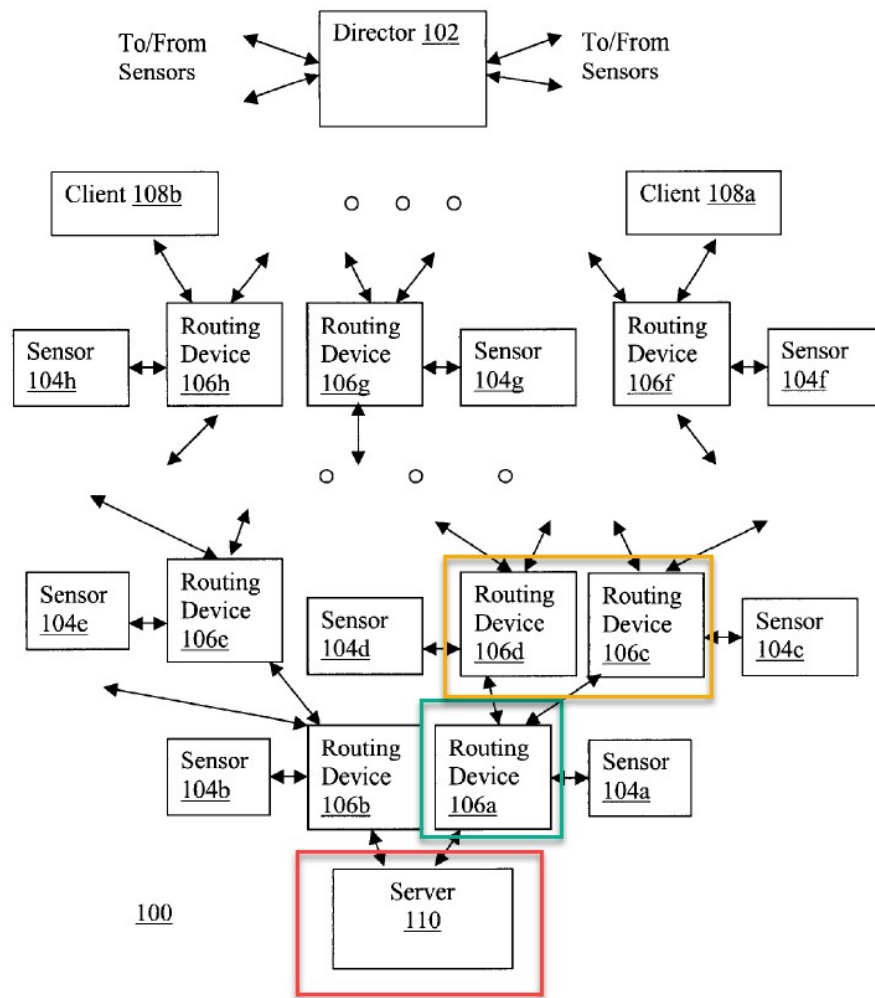


Figure 1

(EX-1006, 3:35-39, Fig. 1 (annotated); EX-1004, ¶115.)

Further, “regulation is progressively applied,” beginning with routers having the lowest degree of separation and extending to routers with a higher degree of separation. (EX-1006, 4:4-8.) That is, Wetherall teaches regulating (e.g., rate-limiting) data packets transmitted from a second router (e.g., router 106c or 106d) to a first router (e.g., router 106a or 106b), the same as it teaches regulating data packets

transmitted from the first router to the host computer (e.g., server 110). (EX-1004, ¶116.)

Claim 10 also recites *transmission rate*, whereas claim 7 recites *processing rate*. In the '497 patent, *transmission rate* differs from *processing rate* only in that *transmission rate* is used to describe the rate of packets transmitted from a router to a host computer; and *processing rate* is used to describe the rate of packets received at the host computer from the router. (EX-1006, 6:12-8:3, Figs. 1-9; EX-1004, ¶117.) To the extent claim 10 differs from claim 7 in this regard, any difference is taught by Wetherall in view of Doeppner at least because in Wetherall, “regulation involves apportioning the bandwidth of a ‘downstream’ interface” (e.g., a host computer) “to its ‘upstream’ interfaces” (e.g., a router that transmits packets to the host computer).⁵ (EX-1006, 7:23-25; *see also* EX-1006, 7:28-42; EX-1004, ¶117.)

Accordingly, as explained further below, claim 10 is rendered obvious by Wetherall in view of Doeppner for reasons analogous to those described for claim 7.

⁵In its infringement contentions in another lawsuit, the Patent Owner identifies the same instrumentality in the accused products as allegedly meeting both the *router* and the *host computer*, and both the *transmission rate* and the *processing rate*, for all of claims 7-12. (See EX-1010.)

- a. **[Preamble] *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:***

The preamble is taught by Wetherall in view of Doeppner as described above for the identical preamble of claim 7.

- b. **[A] *determining a path by which data packets arrive at said router 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;***

Wetherall in view of Doeppner teaches this element as described above for 7[A] and V.B.6. For example, Doeppner teaches determining a path by which data packets arrive at a host computer T via routers in a network, as in Fig. 2:

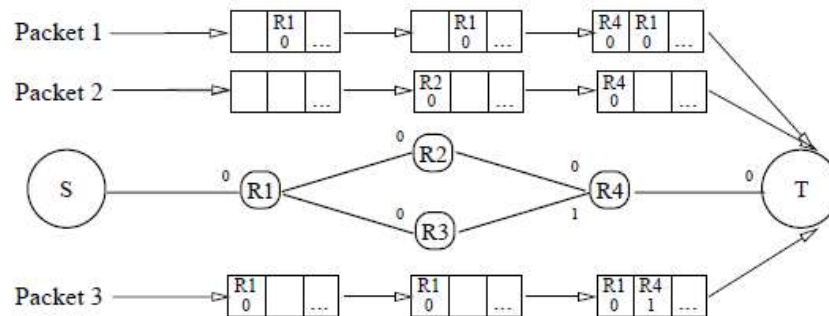


Figure 2: Packets 1, 2, 3 travel from S to T. They are processed by R₁, R₂, R₃ and R₄ which implement Router Stamping.

(EX-1007, 185, Fig. 2; *see also* EX-1007, Fig. 1; EX-1004, ¶120.)

The path taken by data packets 1, 2, or 3 in the attack (e.g., R1-R2-R4; R1-R3-R4) can be determined by packet marks applied by the routers. The paths R1-R2-R4 and R1-R3-R4 include *all routers in said network* along the packets' paths

from source S to host computer T. (EX-1007, 185, Fig. 2; EX-1004, ¶121.)

Determining these paths includes *determining a path by which data packets arrive at said router*, at least because determining a path from S to T includes determining a path to each of the routers on the path from S to T. (EX-1007, 185-188, Fig. 2; EX-1004, ¶121.)

- c. **[B] *classifying data packets received at said router via packet marks provided by routers leading to said host computer by path;***

Wetherall in view of Doeppner teaches this element as described above for 7[B] and V.B.6. (EX-1004, ¶122.)

- d. **[C] *associating a maximum acceptable transmission rate with each class of data packet received at said router; and***

Wetherall in view of Doeppner teaches this element as described above for 7[C] and 9[A] and V.B.6. (EX-1004, ¶123.) For example, Fig. 7b of Wetherall shows regulations (e.g., rate limits) “*for the various network traffic types of the network nodes*”:

710

Routing Device ID <u>712</u>	IP Addr <u>713</u>	Inter- face <u>714</u>	Network Node <u>715</u>	Regulation on Traffic Type 1 <u>716a</u>	...	Regulation on Traffic Type n <u>716n</u>	Other Data <u>718</u>

Figure 7b

(EX-1006, 9:42-54, Fig. 7b (annotated); EX-1004, ¶123.)

- e. ***[D] allocating a transmission rate equal to or less than said maximum acceptable transmission rate for unwanted data packets.***

Wetherall in view of Doeppner teaches this element as described above for 7[D] and V.B.6. (EX-1004, ¶124.)

7. Claim 11

Wetherall in combination with Doeppner renders obvious each limitation of claim 11. A POSITA would have been motivated to combine Wetherall with Doeppner to meet the limitations of claim 11 as described above in V.B.3.

Claim 11 includes limitations analogous to claim 8, except data packets in are transmitted from a *second router* to a *first router* in claim 11, instead of from a *router* to a *host computer* (or “*computer*”) as in claim 8. For the same reasons described above for claim 10, Wetherall’s teachings of regulating traffic from a first router (e.g., router 106a or 106b) to a host computer (e.g., server 110) apply equally to

regulating traffic from a second router (e.g., router 106c, or 106d) to the first router. (EX-1006, 4:4-8, Fig. 1; EX-1004, ¶126.) Some elements of claim 11 recite a *transmission rate* instead of a *processing rate* in claim 8. To the extent this difference is limiting, it is taught by Wetherall in view of Doeppner as described above for claim 10.

Accordingly, claim 11 is rendered obvious by Wetherall in view of Doeppner for reasons analogous to those described above for claim 8. (EX-1004, ¶127.)

- a. ***[Preamble] 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:***

The preamble is taught by Wetherall in view of Doeppner as described above for the identical preamble of claim 8.

- b. ***[A] classifying data packets received at a first router 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;***

Wetherall in view of Doeppner teaches this element as described above for 8[A] and V.B.7. (EX-1004, ¶129.)

- c. ***[B] associating a maximum acceptable transmission rate with each class of data packet received at said first router;***

Wetherall in view of Doeppner teaches this element as described above for 8[B] and 10[C] and V.B.7. (EX-1004, ¶130.)

- d. ***[C] 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;***

Wetherall in view of Doeppner teaches this element as described above for 8[C] and V.B.7. (EX-1004, ¶131.)

- e. ***[D] receiving by said second router of information regarding maximum acceptable transmission rate for data packets being transmitted to said first router; and***

Wetherall in view of Doeppner teaches this element as described above for 8[D] and V.B.7. (EX-1004, ¶132.)

- f. ***[E] controlling by said second router of the rate of transmission of data packets from said second router to said first router so that said rate of transmission is below the maximum acceptable transmission rate for each data packet class; and***

Wetherall in view of Doeppner teaches this element as described above for 8[E] and V.B.7. (EX-1004, ¶133.)

- g. [F] *freeing a portion of the network providing data packet transmission to said first router.***

Wetherall in view of Doeppner teaches this element as described above for 8[F] and V.B.7. (EX-1004, ¶134.)

8. Claim 12

Wetherall in combination with Doeppner renders obvious each limitation of claim 12. A POSITA would have been motivated to combine Wetherall with Doeppner to meet the limitations of claim 12 as described above in V.B.3.

Claim 12 includes limitations analogous to claim 9, except that data packets are transmitted from a *second router* to a *first router* in claim 12, instead of from a *router* to a *computer* as in claim 9. As described above for claim 10, Wetherall's teachings of regulating traffic from a first router (router 106a or 106b) to a computer (server 110) apply equally to regulating traffic from a second router (router 106c or 106d) to the first router. (EX-1006, 4:4-8, Fig. 1; EX-1004, ¶136.)

Accordingly, claim 12 is rendered obvious by Wetherall in view of Doeppner for reasons analogous to those described above for claim 9.

- a. [Preamble] *A method as described in claim 11, in which:***

Wetherall in view of Doeppner teaches a method described in claim 11 as described above for claim 11.

- b. ***[A] said second router receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and***

Wetherall in view of Doeppner teaches this element as described above for 9[A] and V.B.8. (EX-1004, ¶139.)

- c. ***[B] said second router controls the rate of transmission of each class of data packets to said first router.***

Wetherall in view of Doeppner teaches this element as described above for 9[B] and V.B.8. (EX-1004, ¶140.)

C. Ground 2: Claims 7-12 are Obvious in View of Wetherall and Savage

1. Summary of Savage

Savage is a printed publication that was publicly accessible in the United States at least by September 1, 2000, as discussed below.

Savage discloses “a technique for tracing anonymous packet flooding attacks in the Internet back towards their source.” (EX-1008, 295.) Tracing is difficult because packets can include “incorrect,” or “spoofed,” source addresses. (EX-1008, 295.) Fig. 1 shows an example computer network including “victim” computer V and potential attackers A₁ through A₃ which are connected to V by routers R₁ through R₇:

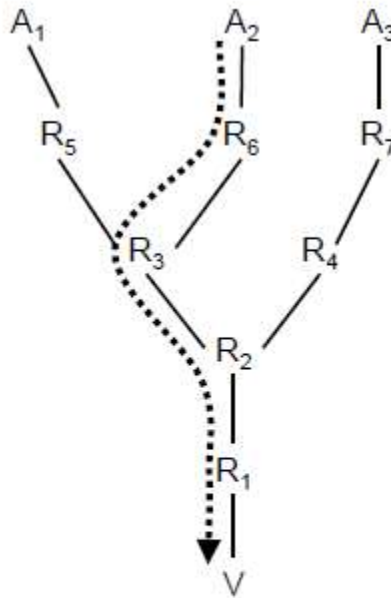


Figure 1: Network as seen from the victim of an attack, V . Routers are represented by R_i , and potential attackers by A_i . The dotted line represents a particular *attack path* between an attacker and the victim.

(EX-1008, 297-298, Fig. 1.)

Fig. 1 represents an “attack path” taken from the potential attacker A_2 to V in the network via routers R_6 , R_3 , R_2 , and R_1 . (EX-1008, 297-298; EX-1004, ¶143.) For example, an attack packet from A_2 can arrive at V via an attack path including routers R_6 , R_3 , R_2 , and R_1 , in that order. (EX-1004, ¶143.)

In Savage, attack paths can be identified even if packet information has been compromised by an attacker. (EX-1008, 304; EX-1004, ¶144.) For example, routers can probabilistically mark packets with IP address information per the following algorithm:

```
Marking procedure at router R:
  for each packet  $w$ 
    let  $x$  be a random number from  $[0..1)$ 
    if  $x < p$  then
      write  $R$  into  $w.start$  and 0 into  $w.distance$ 
    else
      if  $w.distance = 0$  then
        write  $R$  into  $w.end$ 
      increment  $w.distance$ 
```

(EX-1008, 299-300, Fig. 4.)

The victim host computer can then reconstruct the attack path by applying a reconstruction algorithm using the marked packets:

```
Path reconstruction procedure at victim  $v$ :
  let  $G$  be a tree with root  $v$ 
  let edges in  $G$  be tuples (start,end,distance)
  for each packet  $w$  from attacker
    if  $w.distance = 0$  then
      insert edge ( $w.start, v, 0$ ) into  $G$ 
    else
      insert edge ( $w.start, w.end, w.distance$ ) into  $G$ 
  remove any edge ( $x, y, d$ ) with  $d \neq$  distance from  $x$  to  $v$  in  $G$ 
  extract path ( $R_i..R_j$ ) by enumerating acyclic paths in  $G$ 
```

(EX-1008, 299-300, Fig. 4.)

2. Savage is § 102(a) prior art to the '497 patent

Petitioner submits the April 1, 2021 declaration of Scott Delman (EX-1012), the declaration of Dr. Kevin Jeffay (EX-1004), and archived copies of the SIGCOMM 2000 website (EX-1035) and Technical Program (EX-1036) to show that Savage was publicly accessible to a POSITA at least by September 1, 2000,

which precedes the priority date of the '497 patent. Dr. Jeffay was personally in attendance at the ACM SIGCOMM 2000 conference on September 1, 2000, received a published copy of Savage, and has personal knowledge of ACM, ACM conferences such as SIGCOMM, and ACM's publication practices. (EX-1004, ¶¶146-147.) SIGCOMM 2000 was a well-known forum for publications in the field. (EX-1004, ¶147.) As Mr. Delman explains, the published proceedings of that conference (including Savage) were made available on the ACM website (EX-1012, ¶7). Archived copies of the SIGCOMM 2000 website and Technical Program corroborate that Savage was presented at the conference on September 1, 2000. (EX-1035; EX-1036, EX-1004, ¶¶146-147.)

Accordingly, Savage was publicly accessible to the POSITA at least by September 1, 2000. (EX-1004, ¶¶146-148.) Savage is thus prior art under at least 35 U.S.C. § 102(a).

3. Claim 7

Wetherall in combination with Savage renders obvious each limitation of claim 7. A POSITA would have combined the two references.

First, Savage belongs to the same field of endeavor as Wetherall (network traffic management) and describes solutions to an analogous problem (defending a network against DoS packet flooding attacks). (EX-1008, 295; EX-1004, ¶150.)

Wetherall and Savage were authored around the same time, by common authors, suggesting that their teachings are compatible. (EX-1004, ¶154.)

Second, Savage identifies a problem unsolved by Wetherall: how to defend against DoS attacks using packet header information that might be “spoofed” by the attackers. (EX-1008, 295, 304; EX-1004, ¶151.) A POSITA would have been motivated to solve this problem by applying Savage’s marking of packets with path information to Wetherall’s teachings of rate-limiting the packets based on, e.g., source and destination addresses, to “control and contain attacks.” (EX-1008, 295; EX-1006, 6:40-48; EX-1004, ¶151.)

Third, a POSITA would have realized a technical advantage: improving Wetherall’s system by more precisely targeting attack traffic, rather than legitimate traffic. (EX-1004, ¶152.)

Fourth, Wetherall’s and Savage’s teachings are implemented on analogous computer components, such as networks with host computers, routers, and communication lines. (EX-1004, ¶153.) Savage’s teachings “can be efficiently implemented using conventional technology,” without requiring “interactive operational support” from ISPs. (EX-1008, 295; EX-1004, ¶153.) The combination of Savage and Wetherall would have yielded predictable results with a reasonable expectation of success. (EX-1004, ¶153.)

a. [Preamble]

The preamble is taught by Wetherall in view of Savage as described in V.B.3.a for Wetherall. In addition, Savage describes a computer network with a victim host computer that receives transmitted data packets from routers via communication lines. (EX-1008, 295-298, Fig. 1; EX-1004, ¶155.)

b. Element 7[A]

Wetherall in view of Savage teaches this element as described in V.B.3.b for Wetherall. In Savage, flooding attacks are traced by “marking” data packets with addresses of the routers R_i they traverse in transit to a victim host computer V in a computer network:

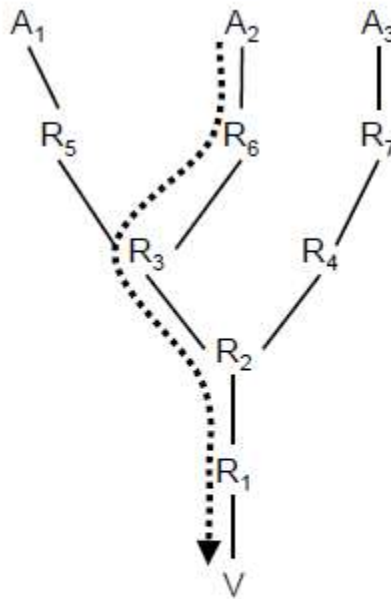


Figure 1: Network as seen from the victim of an attack, V . Routers are represented by R_i , and potential attackers by A_i . The dotted line represents a particular *attack path* between an attacker and the victim.

(EX-1008, 297-298, Fig. 1; EX-1004, ¶156.)

In example Figure 1, an “attack path” is an “ordered list of routers” between an origin A_i and V . (EX-1008, 297-298, Fig. 1; EX-1004, ¶157.) The attack path R_6, R_3, R_2, R_1 is the list of routers that a data packet can take from a source (e.g., A_2) to a host computer (e.g., V) in an attack. (EX-1008, 297-298, Fig. 1; EX-1004, ¶157.) Such paths include all routers in the network (e.g., R_6, R_3, R_2, R_1) via which the packets are routed to the host computer. (EX-1004, ¶157.)

Attack paths are determined using a “packet marking” approach, in which routers (e.g., routers R_6, R_3, R_2, R_1 in Fig. 1) encode path information into the packets. (EX-1008, 297-298; EX-1004, ¶158.) For example, a router probabilistically marks the packet with its own address to indicate a network edge along which the packet traveled:

```
Marking procedure at router R:
  for each packet  $w$ 
    let  $x$  be a random number from  $[0..1)$ 
    if  $x < p$  then
      write  $R$  into  $w.start$  and 0 into  $w.distance$ 
    else
      if  $w.distance = 0$  then
        write  $R$  into  $w.end$ 
      increment  $w.distance$ 
```

(EX-1008, 299-300, Fig. 4.)

The attack path can be determined by a victim host computer using the packet markings:

```
Path reconstruction procedure at victim v:  
  let  $G$  be a tree with root  $v$   
  let edges in  $G$  be tuples (start,end,distance)  
  for each packet  $w$  from attacker  
    if  $w.distance = 0$  then  
      insert edge ( $w.start,v,0$ ) into  $G$   
    else  
      insert edge ( $w.start,w.end,w.distance$ ) into  $G$   
  remove any edge ( $x,y,d$ ) with  $d \neq$  distance from  $x$  to  $v$  in  $G$   
  extract path ( $R_i..R_j$ ) by enumerating acyclic paths in  $G$ 
```

(EX-1008, 299-300, Fig. 4.)

c. Element 7[B]

Wetherall in view of Savage teaches this element as described in V.B.3.c for Wetherall.

d. Element 7[C]

Wetherall in view of Savage teaches this element as described in V.B.3.d for Wetherall.

e. Element 7[D]

Wetherall in view of Savage teaches this element as described in V.B.3.e for Wetherall.

4. Claim 8

Wetherall in combination with Savage renders obvious each limitation of claim 8. A POSITA would have been motivated to combine Wetherall with Savage to meet the limitations of claim 8 as described above in V.C.3.

a. [Preamble]

The preamble is taught by Wetherall in view of Savage as described above for the identical preamble of claim 7.

b. Element 8[A]

Wetherall in view of Savage teaches this element as described above in V.B.4.b for Wetherall. Further, in Savage, data packets are routed on an “attack path” from a potential attacker A_2 to host computer V:

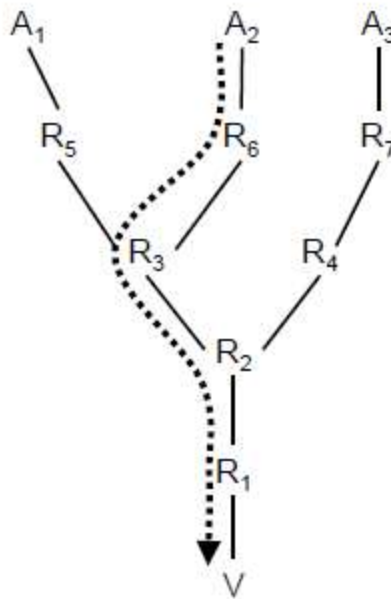


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i , and potential attackers by A_i . The dotted line represents a particular *attack path* between an attacker and the victim.

(EX-1008, 297-298, Fig. 1; EX-1004, ¶165.)

In Fig. 1, data packets from, A_2 can be routed on an attack path to V via routers R₆, R₃, R₂, and R₁. (EX-1008, 297-298, Fig. 1; EX-1004, ¶166.) Accordingly, the

data packets from A₂ comprise *data packets from all routers* (i.e., R₆, R₃, R₂, and R₁) *in said network via which said data packets are routed to said computer* (i.e., V). (EX-1004, ¶166.)

c. Element 8[B]

Wetherall in view of Savage teaches this element as described in V.B.4.c for Wetherall.

d. Element 8[C]

Wetherall in view of Savage teaches this element as described in V.B.4.d for Wetherall.

e. Element 8[D]

Wetherall in view of Savage teaches this element as described in V.B.4.e for Wetherall.

f. Element 8[E]

Wetherall in view of Savage teaches this element as described in V.B.4.f for Wetherall.

g. Element 8[F]

Wetherall in view of Savage teaches this element as described in V.B.4.g for Wetherall.

5. Claim 9

Wetherall in combination with Savage renders obvious each limitation of claim 9. A POSITA would have been motivated to combine Wetherall with Savage to meet the limitations of claim 9 as described above in V.C.3.

a. [Preamble]

Wetherall in view of Savage teaches a method described in claim 8 as above for claim 8.

b. Element 9[A]

Wetherall in view of Savage teaches this element as described in V.B.5.b for Wetherall.

c. Element 9[B]

Wetherall in view of Savage teaches this element as described in V.B.5.c for Wetherall.

6. Claim 10

Wetherall in combination with Savage renders obvious each limitation of claim 10. A POSITA would have been motivated to combine Wetherall with Savage to meet the limitations of claim 10 as described above in V.C.3.

As described in V.B.6, claim 10 includes limitations analogous to claim 7. Any differences in the two claims are taught by Wetherall in view of Savage for reasons analogous to those described in V.B.6.

a. [Preamble]

The preamble is taught by Wetherall in view of Savage as described above for the identical preamble of claim 7.

b. Element 10[A]

Wetherall in view of Savage teaches this element as described above for 7[A] and V.C.6. (EX-1004, ¶179.) Further, Savage teaches determining an attack path by which data packets arrive at a host computer V in a network:

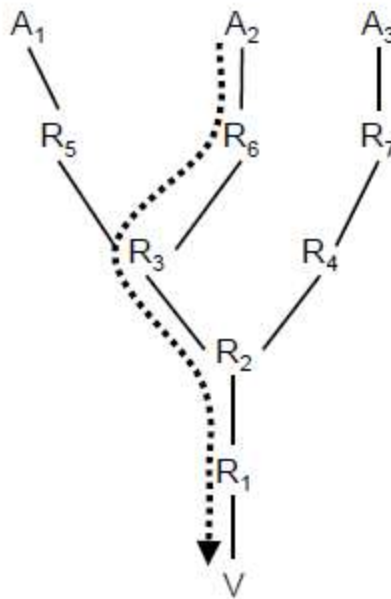


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i , and potential attackers by A_i . The dotted line represents a particular *attack path* between an attacker and the victim.

(EX-1008, 297-298, Fig. 1; EX-1004, ¶179.)

As explained above, the path taken by a data packet from A₂ in an attack (e.g., R₆-R₃-R₂-R₁) can be determined by packet marks applied by the routers in the

network. (EX-1008, 299-300, Fig. 4; EX-1004, ¶180.) The path R_6 - R_3 - R_2 - R_1 *comprises all routers in said network via which said packets are routed* to host computer V. (EX-1008, 299-300, Fig. 4; EX-1004, ¶180.) Determining these paths includes *determining a path by which data packets arrive at said router*, at least because determining a path from A_2 to V includes determining a path to each of the routers on the path from A_2 to V. (EX-1004, ¶180.)

c. Element 10[B]

Wetherall in view of Savage teaches this element as described above for 7[B] and V.C.6. (EX-1004, ¶181.)

d. Element 10[C]

Wetherall in view of Savage teaches this element as described above for 7[C], in V.C.6, and in V.B.6.d for Wetherall. (EX-1004, ¶182.)

e. Element 10[D]

Wetherall in view of Savage teaches this element as described above for 7[D] and V.C.6. (EX-1004, ¶183.) Moreover, Wetherall explains that, in an embodiment, “regulation involves apportioning the bandwidth of a ‘downstream’ interface to its ‘upstream’ interfaces”. (EX-1006, 7:23-25, 7:28-43; EX-1004, ¶183.)

7. Claim 11

Wetherall in combination with Savage renders obvious each limitation of claim 11. A POSITA would have been motivated to combine Wetherall with Savage to meet the limitations of claim 11 as described above in V.C.3.

As described in V.B.7, claim 11 includes limitations analogous to claim 8. Any differences in the two claims are taught by Wetherall in view of Savage for reasons analogous to those described in V.B.7.

a. [Preamble]

The preamble is taught by Wetherall in view of Savage as described above for the identical preamble of claim 8.

b. Element 11[A]

Wetherall in view of Savage teaches this element as described above for 8[A] and V.C.7. (EX-1004, ¶187.)

c. Element 11[B]

Wetherall in view of Savage teaches this element as described above for 8[B] and V.C.7. (EX-1004, ¶188.)

d. Element 11[C]

Wetherall in view of Savage teaches this element as described above for 8[C] and V.C.7. (EX-1004, ¶189.)

e. Element 11[D]

Wetherall in view of Savage teaches this element as described above for 8[D] and V.C.7. (EX-1004, ¶190.)

f. Element 11[E]

Wetherall in view of Savage teaches this element as described above for 8[E] and V.C.7. (EX-1004, ¶191.)

g. Element 11[F]

Wetherall in view of Savage teaches this element as described above for 8[F] and V.C.7. (EX-1004, ¶192.)

8. Claim 12

Wetherall in combination with Savage renders obvious each limitation of claim 12. A POSITA would have been motivated to combine Wetherall with Savage to meet the limitations of claim 12 as described above in V.C.3.

As described in V.B.8, claim 12 includes limitations analogous to claim 9. Any differences between the two are taught by Wetherall in view of Savage for reasons analogous to those described in V.B.8.

a. [Preamble]

Wetherall in view of Savage teaches a method described in claim 11 as described above for claim 11.

b. Element 12[A]

Wetherall in view of Savage teaches this element as described above for 9[A] and V.C.8. (EX-1004, ¶196.)

c. Element 12[B]

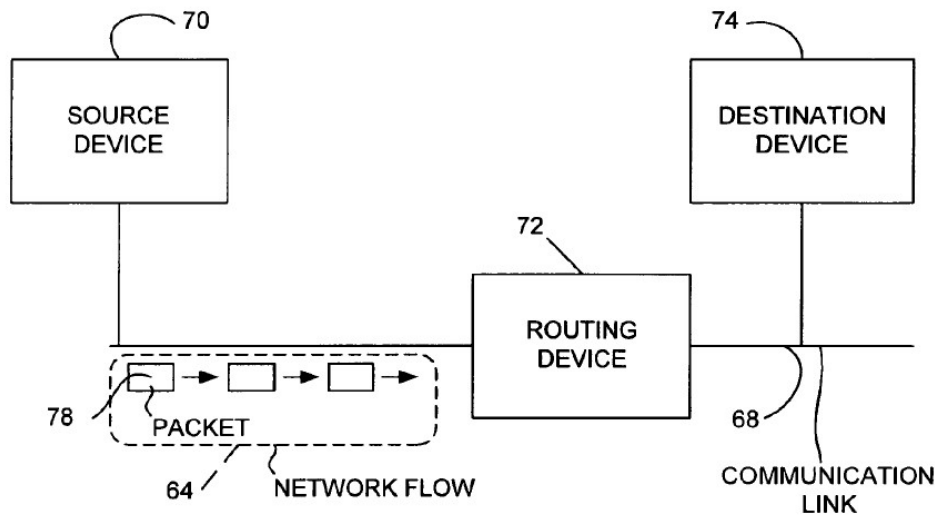
Wetherall in view of Savage teaches this element as described above for 9[B] and V.C.8. (EX-1004, ¶197.)

VI. CHERITON IN VIEW OF DOEPPNER OR SAVAGE RENDERS OBVIOUS CLAIMS 7-12

A. Summary of Cheriton

Cheriton is a U.S. patent filed on Aug. 31, 2000 that issued on Oct. 10, 2006. It is prior art to the '497 patent under at least 35 U.S.C. § 102(e).

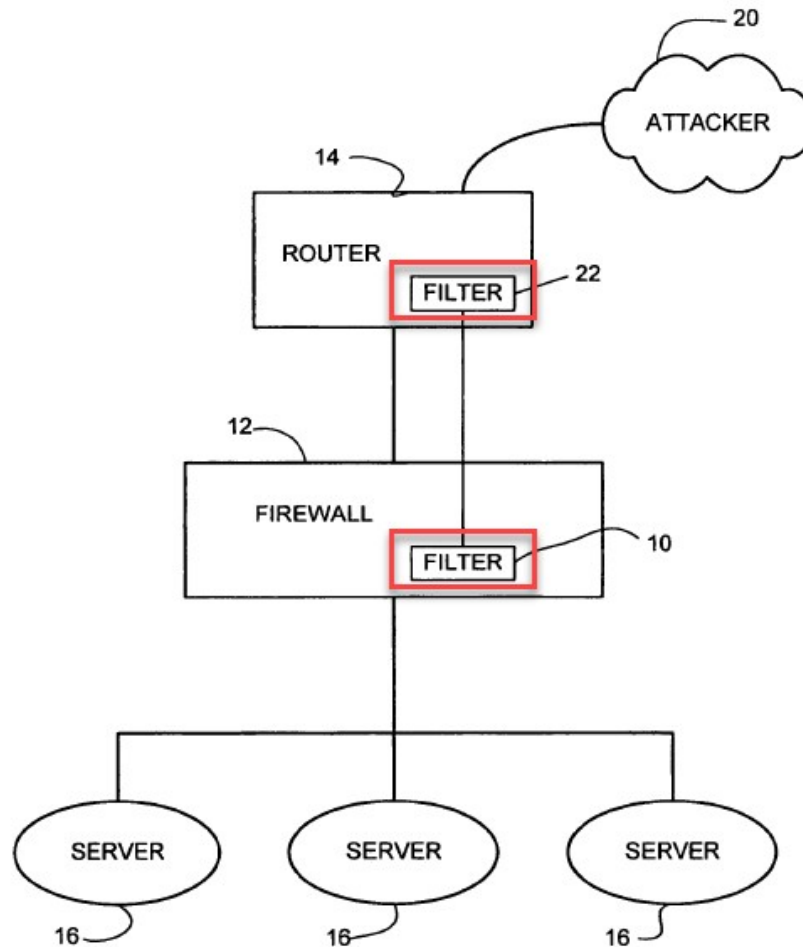
Cheriton relates to detecting, classifying, and filtering data in computer networks, such as for blocking attack packets in DoS attacks, or rate-limiting traffic with a “high rate of data.” (EX-1009, 1:7-58, 3:47-50; EX-1004, ¶199.) In such networks, a network flow 64 comprises data packets 78, which are transmitted from a source device 70 to a destination device 74 (such as a server) via a router 72:



(EX-1009, 5:40-46, Fig. 4.)

Network flows can be classified, such as by their packets' source and destination addresses, and flows can be separated and treated differently based on their classification. (EX-1009, 6:7-20, 6:28-31, 6:38-42, 6:49-51; EX-1004, ¶200.) Packets belonging to a flow can be filtered, such as by blocking or rate-limiting the flow according to a policy specifying a maximum rate. (EX-1009, 8:35-44; EX-1004, ¶200.)

For example, a network flow from an attacker in a DoS attack can be classified as harmful based on the source of its packets. (EX-1009, 7:12-24; EX-1004, ¶201.) That network flow can be filtered such that “only the destructive packets received from the actual attacker are dropped.” (EX-1009, 7:19-24; EX-1004, ¶201.) Filters can be implemented in a router, or in a firewall between the router and host computer:



(EX-1009, 3:38-40, 3:50-54, Fig. 1 (annotated); EX-1004, ¶202.)

B. Ground 3: Claims 7-12 are Obvious in View of Cheriton and Doeppner

1. Claim 7

Cheriton in combination with Doeppner meets each limitation of claim 7. The references would have been readily combined by a POSITA.

First, Cheriton and Doeppner belong to the same field of endeavor (computer network traffic management) and are directed to the same problem (defending against DoS attacks against a network). (EX-1004, ¶203.)

Second, a POSITA would have been motivated to combine Doeppner with Cheriton to solve a problem identified in both Doeppner and Cheriton. In a DoS attack, the source address in a packet header cannot be trusted, because header data can be manipulated (“spoofed”) by the attacker; and a DoS defense system that relies on header data being authentic can inadvertently penalize legitimate traffic instead of attack traffic. (EX-1007, 184; EX-1009, 9:52-55; EX-1004, ¶204.) This is analogous to a problem in the prior art identified in the ’497 patent. (EX-1001, 1:63-2:5; EX-1004, ¶204.)

Cheriton offers one possible solution (reverse path forwarding) to the problem but cautions that this approach is limited to networks where “the routing topology is restricted.” (EX-1009, 9:55-57; EX-1004, ¶205.) Doeppner explains that solutions with such restrictions on network topology may be ill-suited to environments, such as universities, “where the network configuration changes quickly,” and can exhibit high maintenance costs. (EX-1007, 184; EX-1004, ¶205.) Doeppner’s solution for identifying paths, even in the presence of compromised packet data, avoids these concerns and improves Cheriton’s proposed solution. (EX-1007, 184; EX-1004, ¶205.)

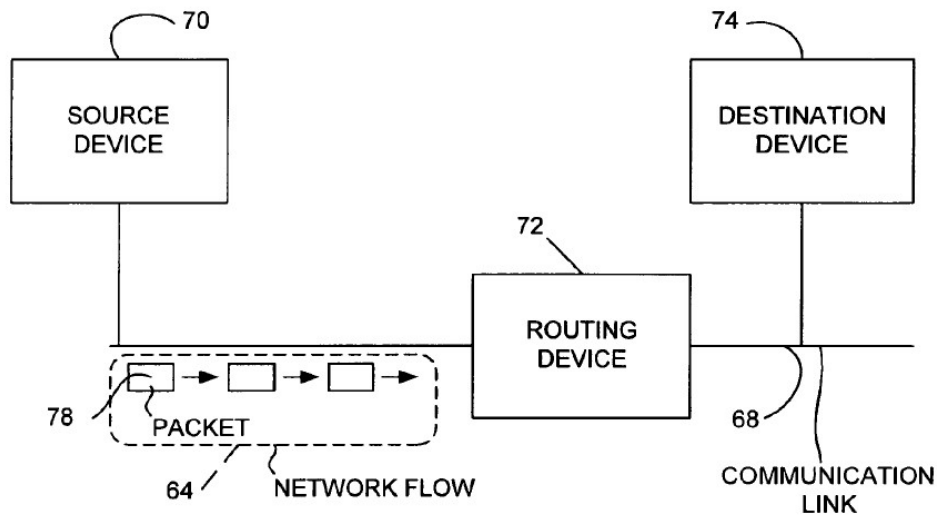
Third, Doeppner invites combination with Cheriton by expressly suggesting that, upon identifying the source of attack packets using its method, those packets

can be isolated and filtered. (EX-1007, 186-188; EX-1004, ¶206.) Cheriton teaches such techniques for isolating and filtering the packets. (EX-1004, ¶206.)

Fourth, Cheriton’s and Doeppner’s teachings are implemented on analogous computer components, such as networks that include host computers, routers, and communication lines. (EX-1004, ¶207.) Doeppner “can be used in conjunction with” other defense measures, such as in Cheriton. (EX-1007, 189.) Moreover, as noted in V.B.3, Doeppner’s teachings were well known, inexpensive, fault tolerant, and adaptable. (EX-1004, ¶¶207-208.) Doeppner’s combination with Cheriton would have yielded predictable results with a reasonable expectation of success. (EX-1004, ¶¶207-208.)

a. [Preamble]

The preamble is taught by Cheriton in view of Doeppner as described in V.B.3.a for Doeppner. In addition, Cheriton discloses a defense for packet flooding attacks for a network including a destination device (host computer) 74, router 72, communication link 68, and transmitted data packets 78:



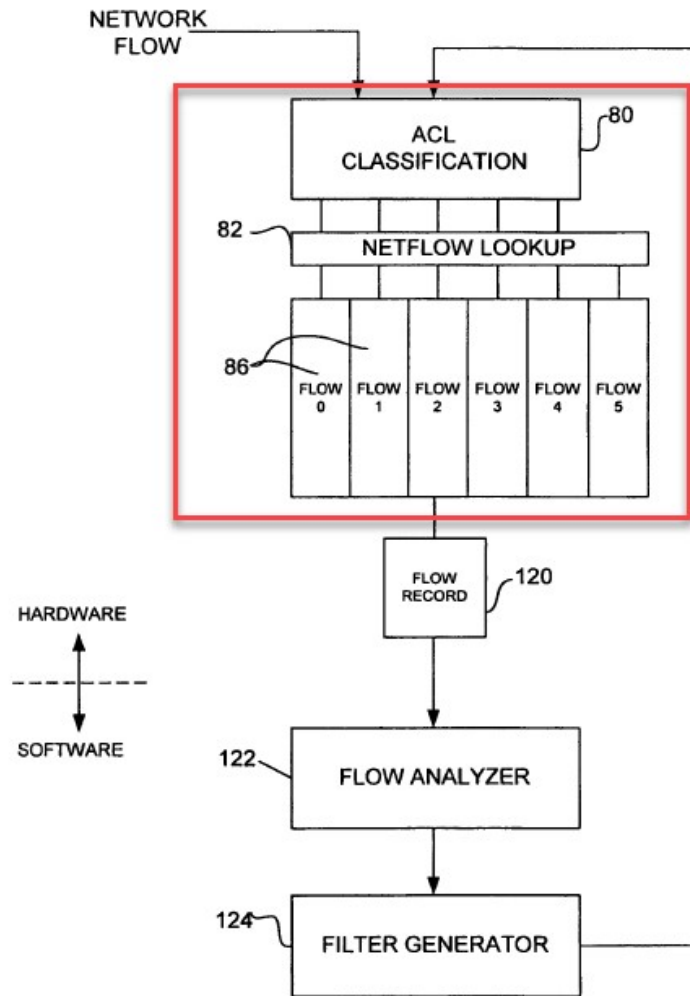
(EX-1009, 1:10-58, 5:40-46, Fig. 4; EX-1004, ¶209.)

b. Element 7[A]

Cheriton in view of Doeppner teaches this element as described in V.B.3.b for Doeppner.

c. Element 7[B]

Cheriton in view of Doeppner teaches this element as described in V.B.3.c for Doeppner. In addition, Cheriton discloses that packets are sent to an “ACL (Access Control List) classification device 80” configured to “classify the received packets 78” into “flows.” (EX-1009, 6:7-10, Fig. 3; EX-1004, ¶211.)

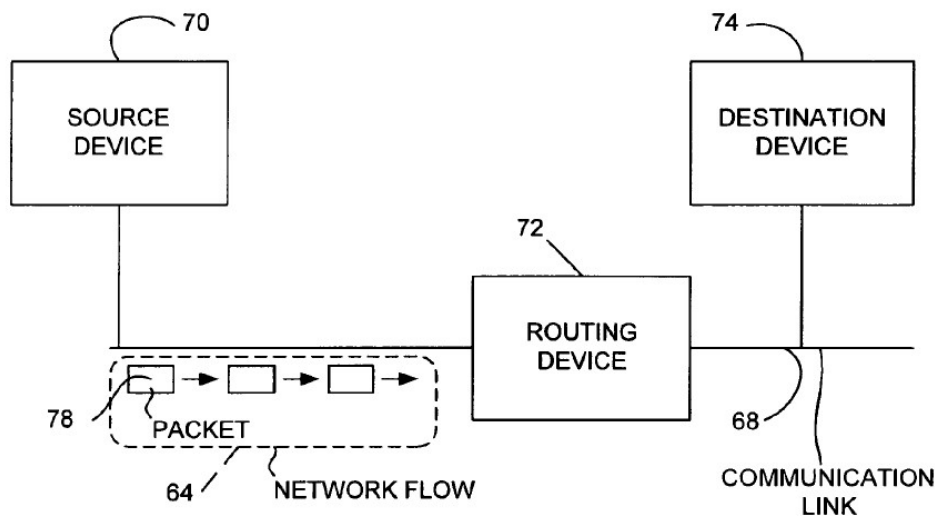


(EX-1009, Fig. 3 (annotated).)

In some embodiments, the packets can be classified as “harmful” flows (corresponding to attack packets in a packet flooding attack), and filtered from the network traffic, such that “only the destructive packets received from the actual attacker are dropped.” (EX-1009, 7:9-24; EX-1004, ¶212.) The “harmful” or “destructive” flows comprise *unwanted packets* that are dropped; the remaining packets are *wanted packets* that are not dropped. (EX-1004, ¶212.) In some

embodiments, the system can “identify sources that appear to represent excessive traffic” (*unwanted packets*), “separate them” (from *wanted traffic*) in the “overall aggregate,” and “throttle their traffic.” (EX-1009, 8:30-44; EX-1004, ¶212.)

A POSITA 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. (EX-1009, 5:40-44, 6:9-10; EX-1004, ¶213.)



(EX-1009, Fig. 4.)

The ACL classifier can “examine a header of the packet 78 and identify the IP address for the source device, the IP address for the destination device, and the

protocol type for the packet, for example, to classify the packet.” (EX-1009, 6:38-42, *see also* EX-1009, 6:10-20; EX-1004, ¶214.) Thus the classification is *by path* (i.e., from the source device to the destination device). (EX-1004, ¶214.)

d. Element 7[C]

Cheriton in view of Doeppner teaches this element. As described above, Cheriton discloses classifying data packets, and explains that “[t]he proper treatment of packets in the network flow is determined, for example, from the classification.” (EX-1009, 6:49-51; EX-1004, ¶215.) Cheriton discloses that “a policy may indicate a maximum aggregate rate of HTTP traffic of 100 [Mbps] and a maximum rate from any source of 25 Mbps.” (EX-1009, 8:37-39.) Cheriton discloses that data packets in a network flow can be classified by source. (EX-1009, 6:10-11 (“The flow may be classified, for example, by source node (IP address)”); EX-1004, ¶215.) Accordingly, the example policy in Cheriton that specifies “a maximum rate from any source of 25 Mbps” *associates a maximum acceptable processing rate* (i.e., 25 Mbps) *with each class of data packet received at said host computer* (i.e., each class of data packets classified by source). (EX-1004, ¶215.) The data packets are received at the host computer as described above for 7[B].

Additionally, as described above for 7[B], Cheriton discloses classifying data packets into unwanted packets (e.g., attack packets in a DoS attack) and wanted data packets. As described above, Cheriton further discloses filtering the packets such

that the unwanted packets are dropped, such that they are not processed, while the remaining packets (wanted packets) are not dropped. (EX-1009, 7:19-24; EX-1004, ¶216.) A POSITA would understand that configuring a filter to drop a class of packets is equivalent to associating that class with a *maximum acceptable processing rate* of zero. (EX-1004, ¶216.) Similarly, Cheriton discloses a “maximum aggregate rate” across all classes of traffic (e.g., a “maximum aggregate rate of HTTP traffic of 100 [Mbps]”). (EX-1009, 8:37-39.) A POSITA would understand that, where there exists a maximum aggregate rate, associating a maximum rate with one class of packets (e.g., 0 Mbps for unwanted packets) also associates a maximum rate with another class of packets (e.g., 100 Mbps for wanted packets), so that the maximum aggregate rate is not exceeded. (EX-1004, ¶216.)

e. Element 7[D]

Cheriton in view of Doeppner teaches this element as described in V.B.3.e for Doeppner. As described above for 7[B], Cheriton explains that “[t]he proper treatment of packets in the network flow is determined, for example, from the classification.” (EX-1009, 6:49-51; EX-1004, ¶217.) For example, Cheriton discloses dropping unwanted packets, thereby allocating a processing rate of zero to those packets. (EX-1004, ¶217.) A POSITA would understand a processing rate of zero to be *less than or equal to said maximum acceptable processing rate for*

unwanted data packets at least because the maximum acceptable processing rate cannot be less than zero. (EX-1004, ¶217.)

2. Claim 8

Cheriton in combination with Doeppner renders obvious each limitation of claim 8. A POSITA would have been motivated to combine Cheriton with Doeppner to meet the limitations of claim 8 as described above in VI.B.1.

a. [Preamble]

The preamble is taught by Cheriton in view of Doeppner as described above for the identical preamble of claim 7.

b. Element 8[A]

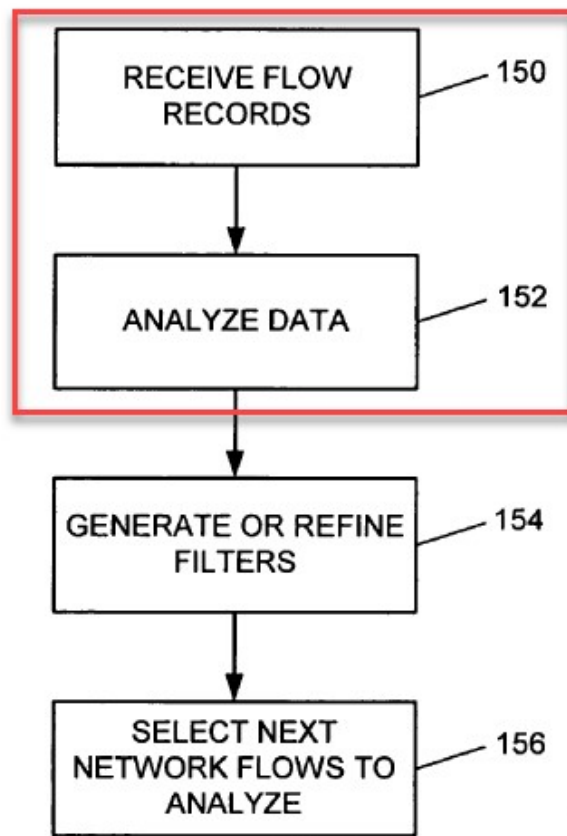
Cheriton in view of Doeppner teaches this element as described above for 7[B], and in V.B.4.b for Doeppner.

c. Element 8[B]

This element is taught by Cheriton in view of Doeppner as described above for 7[C].

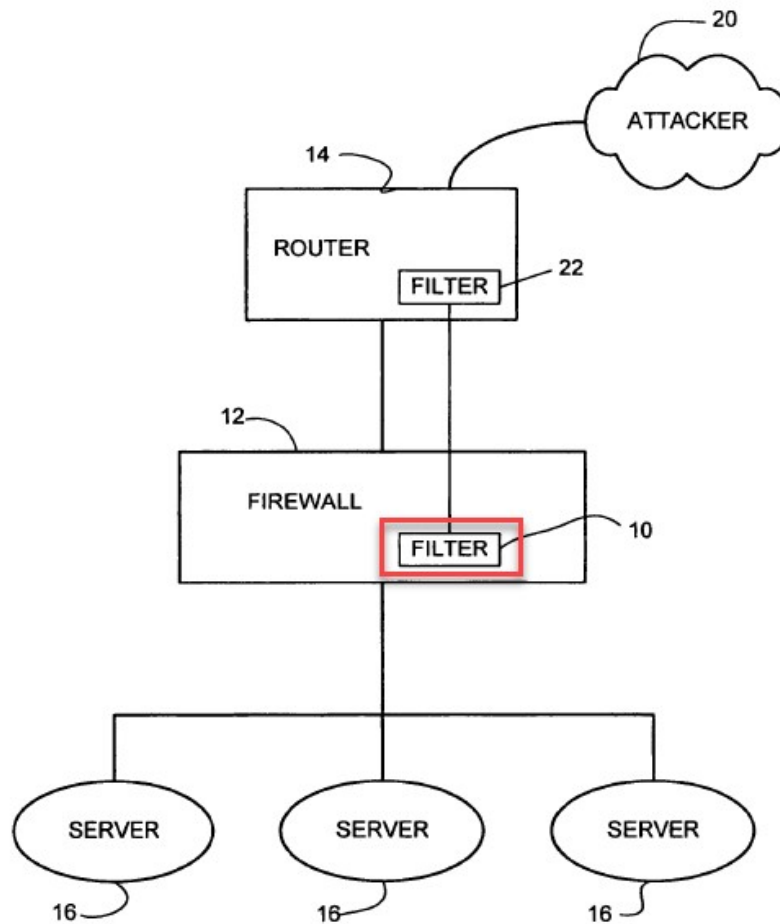
d. Element 8[C]

Cheriton in view of Doeppner teaches this element. For example, Cheriton discloses that records of flows classified by ACL classifier 80 can be analyzed by a flow analyzer 122. (EX-1009, 7:9-12, Fig. 6; EX-1004, ¶222.)



(EX-1009, Fig. 6 (annotated).)

Flow analyzer 122 “monitors the statistics associated with aggregate filters 10.” (EX-1009, 7:58-59; EX-1004, ¶223.) A POSITA would understand that the flow analyzer monitoring statistics associated with the filter includes the flow analyzer determining a rate of data packets *from a router to host computer*. For example, in Fig. 1, filter 10 sits between a router (14) and a host computer (server 16) and filters data packets transmitted from the router to the host computer:

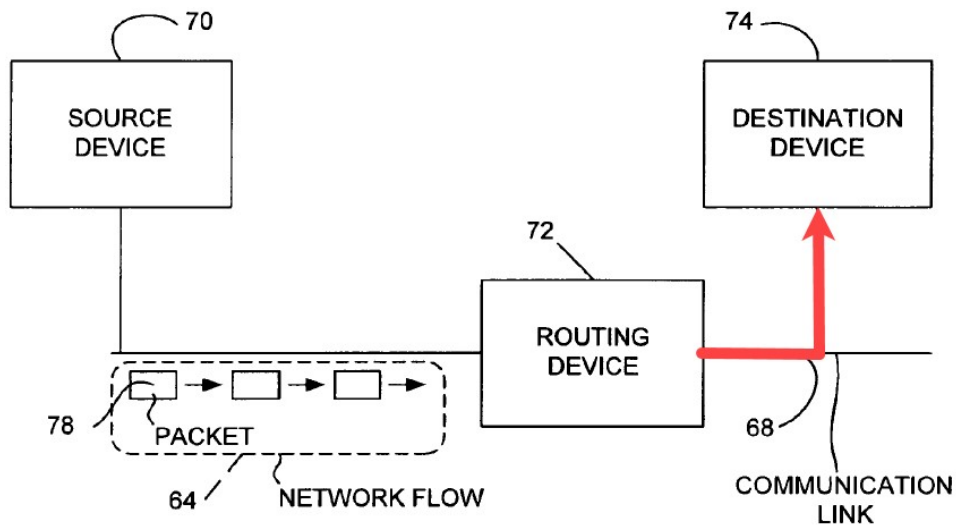


(EX-1009, Fig. 1 (annotated); EX-1004, ¶223.)

A POSITA would also understand that the statistics monitored include a *rate at which data packets are transmitted*. For example, Cheriton explains that the flow analyzer monitors statistics to “detect ... anomalies” within a flow; and that such anomalies can include the “rate of packets.” (EX-1009, 8:7-10, 8:23-27; EX-1004, ¶224.) Cheriton also discloses that the flow analyzer can “examin[e] the statistics” to recognize that a rate of traffic exceeds a maximum. (EX-1009, 8:11-14; EX-1004, ¶224.)

e. Element 8[D]

Cheriton in view of Doeppner teaches this element as described above for 7[C]. To the extent this element differs from 7[C] by reciting a *transmission rate* for packets *transmitted to* a computer, instead of a *processing rate* for packets *received by* the computer, the differences are taught by Cheriton in view of Doeppner. Cheriton discloses that a “unidirectional stream of packets 78” is “transmitted between pairs of transport service access points.” (EX-1009, 5:42-44; EX-1004, ¶225.) For example, packets 78 can be a unidirectional stream from a router 72 to a computer 74:



(EX-1009, Fig. 4 (annotated); EX-1004, ¶225.)

Accordingly, Cheriton in view of Doeppner teaches that a *maximum acceptable processing rate* for packets received by computer 74 can be the same as a *maximum acceptable transmission rate* for packets sent to the computer by router

72; and the maximum acceptable transmission rate in this element is thus taught for at least the same reasons as the maximum acceptable processing rate in 7[C]. (EX-1004, ¶226.)

f. Element 8[E]

Cheriton in view of Doeppner teaches this element as described above for 7[C] and 7[D]. For example, as described above, Cheriton discloses setting transmission rates to adhere to a policy that sets a maximum aggregate rate as well as a maximum per-source rate. (EX-1009, 8:30-44; EX-1004, ¶227.) To the extent this element differs from 7[D] in reciting a rate of *transmission* instead of a *processing* rate, the difference is taught by Cheriton in view of Doeppner as described above for 8[D].

g. Element 8[F]

Cheriton in view of Doeppner teaches this element as described above for 8[E] and V.B.4.g. The '497 patent explains that limiting the data packet transmissions, as taught by Cheriton in view of Doeppner, “thereby” results in *freeing a portion of the network providing data packet transmission to the computer*, as recited in the claim. (EX-1004, ¶228.)

3. Claim 9

Cheriton in combination with Doeppner renders obvious each limitation of claim 9, as described below. A POSITA would have been motivated to combine

Cheriton with Doeppner to meet the limitations of claim 9 as described above in VI.B.1.

a. [Preamble]

Cheriton in view of Doeppner teaches a method described in claim 8 as described above for claim 8.

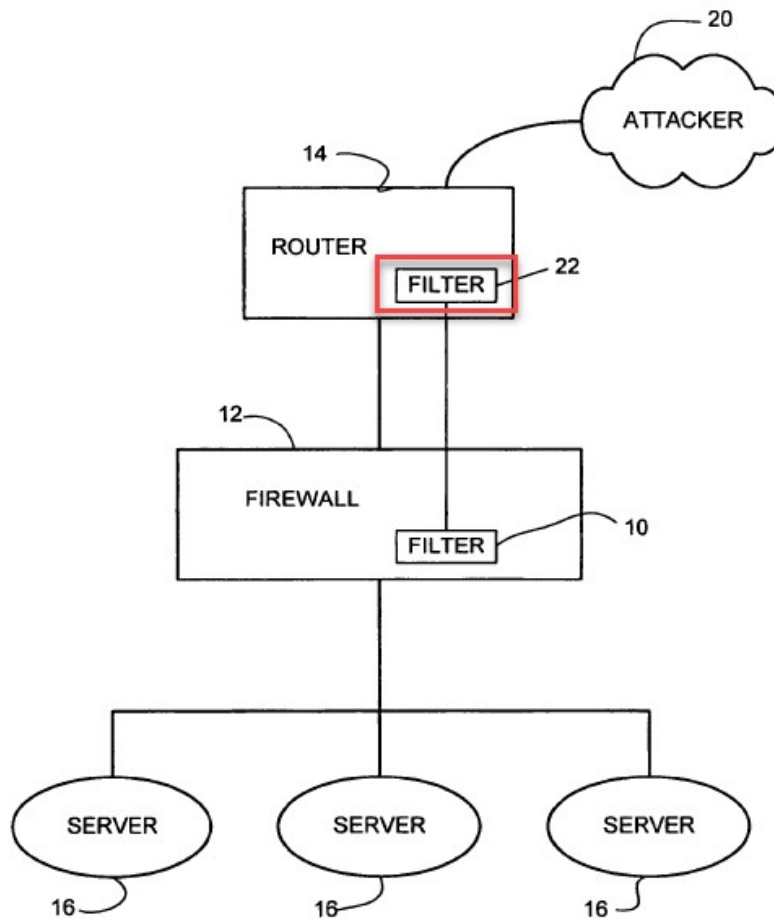
b. Element 9[A]

Cheriton in view of Doeppner teaches this element as described above for 8[D]. For example, as described above, Cheriton discloses setting transmission rates to adhere to a policy that sets a maximum aggregate rate as well as a maximum per-source rate. (EX-1009, 8:30-44; EX-1004, ¶231.) Thus, the maximum acceptable transmission rate is for *each class* of data packet. (EX-1004, ¶231.)

Further, Cheriton discloses “automatically propagat[ing] filter information” — such as “excessive traffic” from a particular source — upstream to filter data closer to the source, such as filter 22 located at router 14. (EX-1009, 8:51-58; EX-1004, ¶232.) Thus, the information is received by *said router*. (EX-1004, ¶232.)

c. Element 9[B]

Cheriton in view of Doeppner teaches this element as described above for 8[E]. (EX-1004, ¶233.) The rate of transmission can be controlled by *said router* at least because Cheriton discloses that network traffic filter 22 can be located within router 14:



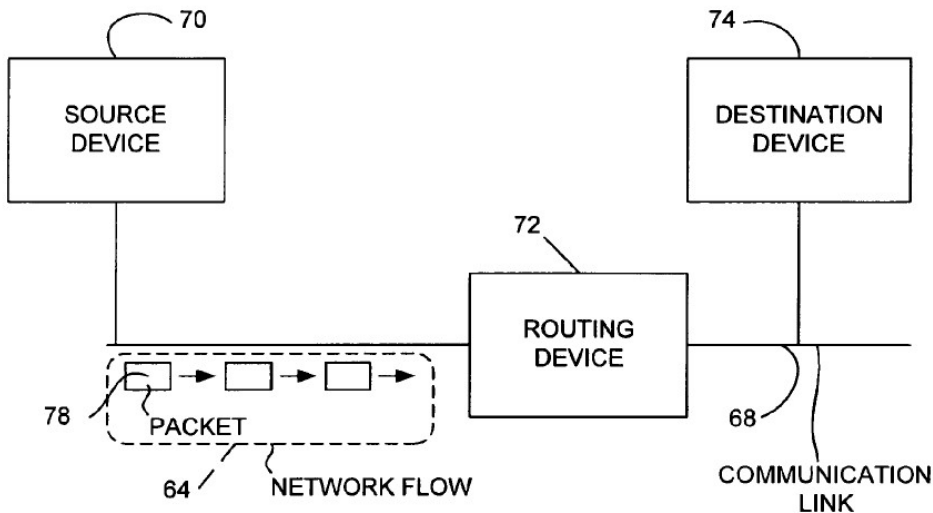
(EX-1009, 8:51-54, Fig. 1 (annotated); EX-1004, ¶233.)

4. Claim 10

Cheriton in combination with Doeppner renders obvious each limitation of claim 10. A POSITA would have been motivated to combine Cheriton with Doeppner to meet the limitations of claim 10 as described above in VI.B.1.

Claim 10 includes limitations analogous to claim 7. Any differences between the two are taught by Cheriton in view of Doeppner at least as described in V.B.6.

In addition, in Cheriton, data packets are transmitted from source 70, to router 72, to host computer 74, as shown in Fig. 4:

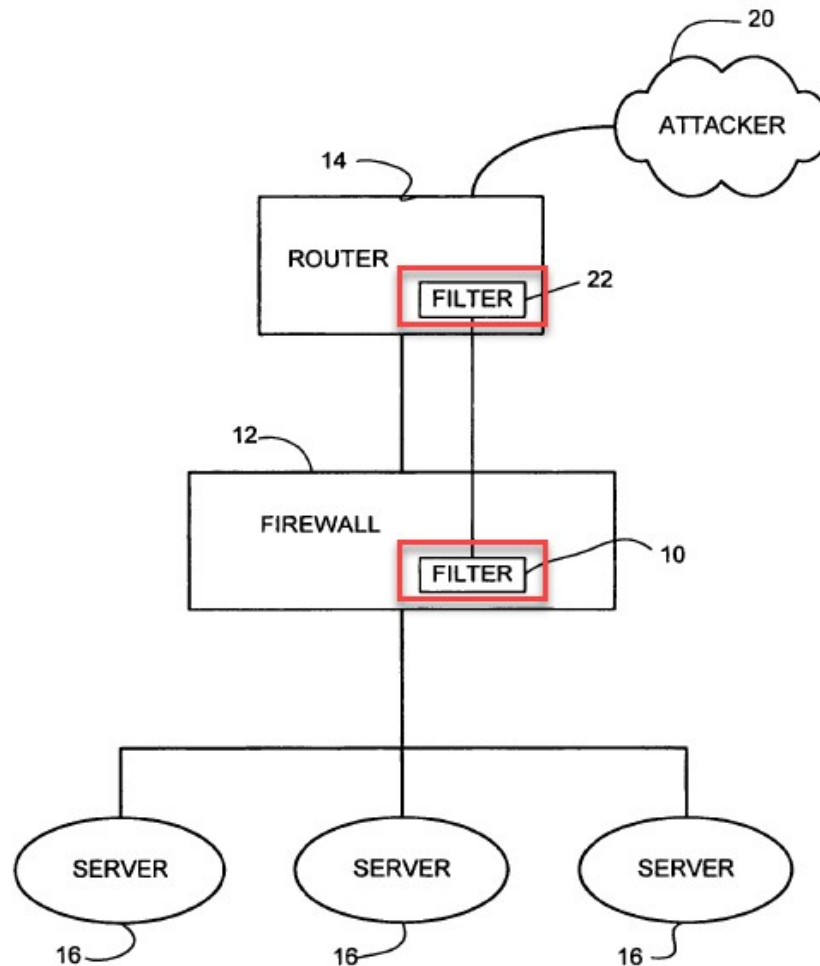


(EX-1009, Fig. 4.)

Thus, packets received at host computer 74 are also received at router 72.

(EX-1004, ¶¶235-236.)

Further, Cheriton discloses that network traffic filter 10 can be located in a firewall 12 that sits between router 14 and host computer 16. (EX-1009, 3:38-40; EX-1004, ¶237.) Cheriton also discloses that “[o]nce the initial filters 10 are defined within the firewall 12, the system may be used to automatically propagate filter information upstream to filter data closer to the source, such as *filter 22 located at router 14* shown in FIG. 1.” (EX-1009, 8:51-54; EX-1004, ¶237.) That is, the filter can be located within a firewall (for traffic received by the host computer), or within a router (for traffic received by the router):

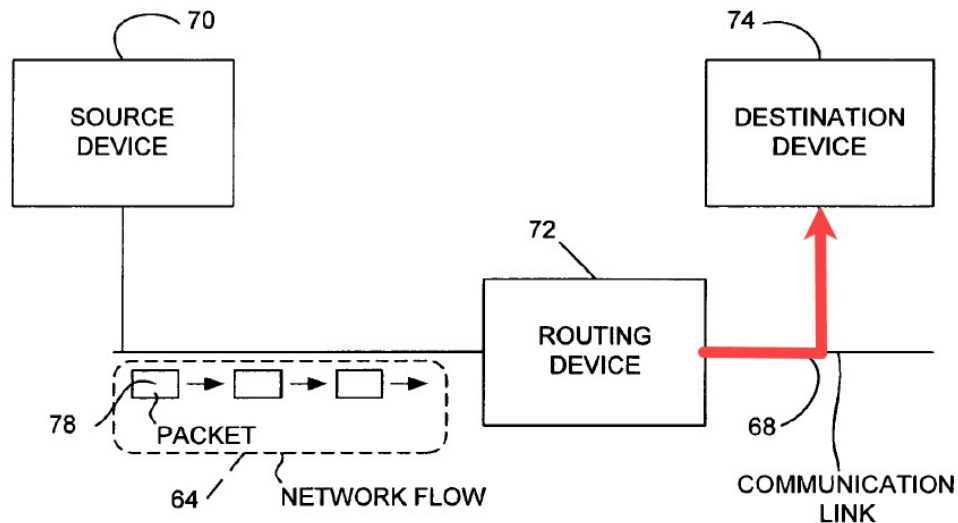


(EX-1009, Fig. 1 (annotated); EX-1004, ¶237.)

Accordingly, to the extent claim 10 differs from claim 7 in that data packets are received by a *router* instead of by a *host computer*, the differences are taught by Cheriton in view of Doeppner. (EX-1004, ¶238.)

To the extent claim 10 differs from claim 7 by reciting a *transmission rate* instead of a *processing rate*, the differences are taught by Cheriton in view of Doeppner at least as described for 8[D]. As described above, in embodiments of

Cheriton, a processing rate of packets received at a host computer is the same as a transmission rate of packets transmitted to the host computer. (EX-1004, ¶239.)



(EX-1009, Fig. 4 (annotated); EX-1004, ¶239.)

a. [Preamble]

The preamble is taught by Cheriton in view of Doeppner as described above for the identical preamble of claim 7.

b. Element 10[A]

Cheriton in view of Doeppner teaches this element as described above for 7[A] and VI.B.4. (EX-1004, ¶241.)

c. Element 10[B]

Cheriton in view of Doeppner teaches this element as described above for 7[B] and VI.B.4. (EX-1004, ¶242.)

d. Element 10[C]

Cheriton in view of Doeppner teaches this element as described above for 7[C] and VI.B.4. (EX-1004, ¶243.)

e. Element 10[D]

Cheriton in view of Doeppner teaches this element as described above for 7[D] and VI.B.4. (EX-1004, ¶244.)

5. Claim 11

Cheriton in combination with Doeppner renders obvious each limitation of claim 11. A POSITA would have been motivated to combine Cheriton with Doeppner to meet the limitations of claim 11 as described above in VI.B.1.

Claim 11 includes limitations analogous to claim 8. Any differences between the two are taught by Cheriton in view of Doeppner at least for the same reasons described in VI.B.4.

a. [Preamble]

The preamble is taught by Cheriton in view of Doeppner as described above for the identical preamble of claim 8.

b. Element 11[A]

Cheriton in view of Doeppner teaches this element as described above for 8[A] and VI.B.5. (EX-1004, ¶248.)

c. Element 11[B]

Cheriton in view of Doeppner teaches this element as described above for 8[B] and VI.B.5. (EX-1004, ¶249.)

d. Element 11[C]

Cheriton in view of Doeppner teaches this element as described above for 8[C] and VI.B.5. (EX-1004, ¶250.)

e. Element 11[D]

Cheriton in view of Doeppner teaches this element as described above for 8[D] and VI.B.5. (EX-1004, ¶251.)

f. Element 11[E]

Cheriton in view of Doeppner teaches this element as described above for 8[E] and VI.B.5. (EX-1004, ¶252.)

g. Element 11[F]

Cheriton in view of Doeppner teaches this element as described above for 8[F] and VI.B.5. (EX-1004, ¶253.)

6. Claim 12

Cheriton in combination with Doeppner renders obvious each limitation of claim 12. A POSITA would have been motivated to combine Cheriton with Doeppner to meet the limitations of claim 12 as described above in VI.B.1.

Claim 12 includes limitations analogous to claim 9. Any differences between the two are taught by Cheriton in view of Doeppner for reasons analogous to those described in VI.B.4.

a. [Preamble]

Cheriton in view of Doeppner teaches a method described in claim 11 as described above for claim 11.

b. Element 12[A]

Cheriton in view of Doeppner teaches this element as described above for 9[A] and VI.B.6. (EX-1004, ¶257.)

c. Element 12[B]

Cheriton in view of Doeppner teaches this element as described above for 9[B] and VI.B.6. (EX-1004, ¶258.)

C. Ground 4: Claims 7-12 are Obvious in View of Cheriton and Savage

1. Claim 7

Cheriton in combination with Savage renders obvious each limitation of claim 7. A POSITA would have combined the two references.

First, Savage belongs to the same field of endeavor as Cheriton (network traffic management) and describes solutions to an analogous problem (defending a network against DoS packet flooding attacks). (EX-1008, 295-296; EX-1004, ¶260.)

Second, Savage identifies a problem not fully solved by Cheriton: how to defend against DoS attacks using packet header information when that information can be “spoofed” by the attackers. (EX-1008, 295, 304; EX-1004, ¶261.) A POSITA would have been motivated to apply Savage’s marking of packets with path information to Cheriton’s teachings of identifying and rate-limiting the packets based on, e.g., source and destination addresses, to “control and contain attacks.” (EX-1008, 295; EX-1006, 6:40-48; EX-1004, ¶261.) While Cheriton suggests using reverse path forwarding to guard against spoofed packet data, reverse path forwarding relies on information reported by routers in a network, and may produce unreliable results when those routers are compromised. (EX-1009, 9:51-10:5; EX-1004, ¶261.) Cheriton offers no solution for this. Savage improves Cheriton’s reverse path forwarding by offering marking techniques that can identify compromised routers. (EX-1008, 298; EX-1004, ¶261.)

Third, a POSITA would have realized a technical advantage: improving the effectiveness of Cheriton’s system by more accurately targeting attack traffic, rather than legitimate traffic. (EX-1004, ¶262.)

Fourth, Cheriton’s and Savage’s teachings are implemented on analogous computer components, such as networks that include host computers, routers, and communication lines. (EX-1004, ¶263.) Savage’s teachings “can be efficiently implemented using conventional technology,” without requiring “interactive

operational support” from ISPs. (EX-1008, 295; EX-1004, ¶263.) Thus the combination of Savage and Cheriton would have yielded predictable results with a reasonable expectation of success. (EX-1004, ¶¶263-264.)

a. [Preamble]

The preamble is taught by Cheriton in view of Savage as described in VI.B.1.a for Cheriton and V.C.3.a for Savage.

b. Element 7[A]

Cheriton in view of Savage teaches this element as described in VI.B.1.b for Cheriton and V.C.3.b for Savage.

c. Element 7[B]

Cheriton in view of Savage teaches this element as described ins VI.B.1.c for Cheriton and V.C.3.c for Savage.

d. Element 7[C]

Cheriton in view of Savage teaches this element as described ins VI.B.1.d for Cheriton and V.C.3.d for Savage.

e. Element 7[D]

Cheriton in view of Savage teaches this element as described in VI.B.1.e for Cheriton and V.C.3.e for Savage.

2. Claim 8

Cheriton in combination with Savage renders obvious each limitation of claim 8. A POSITA would have been motivated to combine Cheriton with Savage to meet the limitations of claim 8 as described above in VI.C.1.

a. [Preamble]

The preamble is taught by Cheriton in view of Savage as described above for the identical preamble of claim 7.

b. Element 8[A]

Cheriton in view of Savage teaches this element as described in VI.B.2.b for Cheriton and V.C.4.b for Savage.

c. Element 8[B]

Cheriton in view of Savage teaches this element as described in VI.B.2.c for Cheriton and V.C.4.c for Savage.

d. Element 8[C]

Cheriton in view of Savage teaches this element as described in VI.B.2.d for Cheriton and V.C.4.d for Savage.

e. Element 8[D]

Cheriton in view of Savage teaches this element as described in VI.B.2.e for Cheriton and V.C.4.e for Savage.

f. Element 8[E]

Cheriton in view of Savage teaches this element as described in VI.B.2.f for Cheriton and V.C.4.f for Savage.

g. Element 8[F]

Cheriton in view of Savage teaches this element as described in VI.B.2.g for Cheriton and V.C.4.g for Savage.

3. Claim 9

Cheriton in combination with Savage renders obvious each limitation of claim 9, as described below. A POSITA would have been motivated to combine Cheriton with Savage to meet the limitations of claim 9 as described above in VI.C.1.

a. [Preamble]

Cheriton in view of Savage teaches a method described in claim 8 as described above for claim 8.

b. Element 9[A]

Cheriton in view of Savage teaches this element as described in VI.B.3.b for Cheriton and V.C.5.b for Savage.

c. Element 9[B]

Cheriton in view of Savage teaches this element as described in VI.B.3.c for Cheriton and V.C.5.c for Savage.

4. Claim 10

Cheriton in combination with Savage renders obvious each limitation of claim 10. A POSITA would have been motivated to combine Cheriton with Savage to meet the limitations of claim 10 as described above in VI.C.1.

As described in V.B.6, claim 10 includes limitations analogous to claim 7. Any differences between the two are taught by Cheriton in view of Savage for reasons analogous to those described in VI.B.4.

a. [Preamble]

The preamble is taught by Cheriton in view of Savage as described above for the identical preamble of claim 7.

b. Element 10[A]

Cheriton in view of Savage teaches this element as described above for 7[A] and VI.C.4. (EX-1004, ¶285.)

c. Element 10[B]

Cheriton in view of Savage teaches this element as described above for 7[B] and VI.C.4. (EX-1004, ¶286.)

d. Element 10[C]

Cheriton in view of Savage teaches this element as described above for 7[C] and VI.C.4. (EX-1004, ¶287.)

e. Element 10[D]

Cheriton in view of Savage teaches this element as described above for 7[D] and VI.C.4. (EX-1004, ¶288.)

5. Claim 11

Cheriton in combination with Savage renders obvious each limitation of claim 11. A POSITA would have been motivated to combine Cheriton with Savage to meet the limitations of claim 11 as described above in VI.C.1.

As described in V.B.7, claim 11 includes limitations analogous to claim 8. Any differences between the two are taught by Cheriton in view of Savage for reasons analogous to those described in VI.B.4.

a. [Preamble]

The preamble is taught by Cheriton in view of Savage as described above for the identical preamble of claim 8.

b. Element 11[A]

Cheriton in view of Savage teaches this element as described above for 8[A] and VI.C.5. (EX-1004, ¶292.)

c. Element 11[B]

Cheriton in view of Savage teaches this element as described above for 8[B] and VI.C.5. (EX-1004, ¶293.)

d. Element 11[C]

Cheriton in view of Savage teaches this element as described above for 8[C] and VI.C.5. (EX-1004, ¶294.)

e. Element 11[D]

Cheriton in view of Savage teaches this element as described above for 8[D] and VI.C.5. (EX-1004, ¶295.)

f. Element 11[E]

Cheriton in view of Savage teaches this element as described above for 8[E] and VI.C.5. (EX-1004, ¶296.)

g. Element 11[F]

Cheriton in view of Savage teaches this element as described above for 8[F] and VI.C.5. (EX-1004, ¶297.)

6. Claim 12

Cheriton in combination with Savage renders obvious each limitation of claim 12. A POSITA would have been motivated to combine Cheriton with Savage to meet the limitations of claim 12 as described above for claim 7.

As described in V.B.8, claim 12 includes limitations analogous to claim 9. Any differences between the two are taught by Cheriton in view of Savage for reasons analogous to those described in VI.B.4.

a. [Preamble]

Cheriton in view of Savage teaches a method described in claim 11 as described above for claim 11.

b. Element 12[A]

Cheriton in view of Savage teaches this element as described above for 9[A] and VI.C.6. (EX-1004, ¶301.)

c. Element 12[B]

Cheriton in view of Savage teaches this element as described above for 9[B] and VI.C.6. (EX-1004, ¶302.)

VII. DISCRETIONARY DENIAL WOULD BE INAPPROPRIATE AND IMPROPER

A. District Court Litigation

The Board should not deny institution under § 314 based on litigation in the United States District Court for the Western District of Texas (“Court”) between PacSec3 and Cloudflare. PacSec3’s lawsuit against Cloudflare, filed on February 4, 2022, has not progressed beyond the pleading stage given PacSec3’s failure to diligently prosecute the case and failure to timely serve all defendants in cases related to the lawsuit. The Court requires the parties to file a Case Readiness Status Report within 7 days after the last defendant in Related Cases (cases filed within a 30 day period sharing a common asserted patent) has responded to the initial pleadings and before the Case Management Conference can occur. (EX-1037, 1.)

The parties have not filed the necessary Report, because PacSec3 delayed serving all necessary defendants, and not all defendants have answered. (EX-1038.) It appears that PacSec3 failed to comply with the Court’s 6/14/2022 Order requiring PacSec3 to serve related defendant Dark Trace (sued on the same day as Cloudflare) by the end of June 2022, and Cloudflare is unaware of any service of process on Dark Trace. (EX-1039.) The lawsuit therefore is at its inception, with no case schedule, and certainly no infringement contentions, discovery, hearings, or trial date due to PacSec3’s long delay.

Fintiv factors 2, 3, and 6 weigh strongly in favor of institution in view of the above and given that the parties in the lawsuit do not have even a case schedule. *See Apple Inc. v. Fintiv Inc.*, IPR2020-00019, Paper 11 (PTAB March 20, 2020) (precedential, designated May 5, 2020). There is no trial date (factor 2), miniscule “investment in the parallel proceeding” (factor 3), and PacSec3’s extraordinary delay is a circumstance weighing in favor of institution (factor 6). *Id.*; *see also Beckman Coulter, Inc. v. Sirigen II Ltd.*, IPR2022-01203, Paper 12 (PTAB January 6, 2023) at 18 (stating that there is “no basis for Patent Owner’s argument for discretionary denial” where the district court has not set a trial date).

Factor 1 is neutral because the Board has previously “decline[d] to infer” how a District Court would decide a stay motion. *Fintiv*, Paper 15 at 12.

Factors 4 and 5 (overlap between lawsuit and IPR) also weigh in favor of institution because Petitioner stipulates not to pursue in the parallel district court proceeding the same grounds as in this Petition if the Board institutes this IPR. Therefore, the grounds addressed in the district court proceeding and the grounds addressed in this IPR will be mutually exclusive. The Board declined to deny institution for discretionary reasons in a situation involving a similar stipulation and a lawsuit that was more advanced than this case, where the Petition was filed four months after infringement contentions were served. *Apple Inc. v. Jawbone Innovations, LLC*, IPR2022-01084, Paper 9 (PTAB December 16, 2022) at 18-20.

Further, the Interim Guidance dated June 21, 2022 directs that “the PTAB will not deny institution based on *Fintiv* if there is compelling evidence of unpatentability.” (Interim Guidance at 5.) This Petition presents four grounds, each demonstrating the unpatentability of claims 7-12 for the reasons set forth above. Any of these grounds, let alone all four, plainly lead to the conclusion that the claims are unpatentable.

For the above reasons, the efficiency and integrity of the system are best served by instituting review.

B. *Ex Parte* Reexamination

The Board further should not deny institution under § 325(d) on the basis of either the prosecution of the original application, or its *ex parte* reexamination (Control No. 90/014,746) currently on appeal to the Board.

The Board applies a two-part framework for determining whether to deny institution under § 325(d) in view of prosecution of the original patent application and any subsequent reexamination: “(1) whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office; and (2) if either condition of first part of the framework is satisfied, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of challenged claims.” *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 8 (Feb. 13, 2020) (designated precedential on March 24, 2020).

Here, neither the same (or substantially the same) art nor arguments were previously presented to the Office. None of the references presented in this Petition (Wetherall, Doeppner, Savage, Cheriton) were considered during prosecution of the ’497 patent, and only one (Savage) was part of the reexamination request (which only included claims 7 and 10 of the six claims challenged in this Petition). Nor do the references presented here present arguments cumulative of those raised in original prosecution or in the reexamination.

While the references presented in the reexamination request (Savage, Maher, Schuba) are directed generally to network traffic management and security, the combinations identified in the reexamination request teach different technical solutions to those problems than those presented in this Petition. None of Savage, Maher, or Schuba discloses the system in Wetherall of regulating network traffic according to a “not-to-exceed” traffic profile; the automatic progressive filtering system of Cheriton; or the packet marking techniques of Doeppner, which render the claims obvious as set forth in this Petition.

In the reexamination request, neither the combination of Wetherall and Savage nor the combination of Cheriton and Savage was presented or considered. Neither Maher nor Schuba discloses the rate limiting system of Wetherall, nor the packet filtering system of Cheriton. Nor has Savage been considered, in any capacity, with respect to the challenged claims 8, 9, 11, or 12, which were not part of the reexamination request. The Office has yet to consider the teachings of Wetherall, Doeppner, Savage, and Cheriton, in the combinations set forth in this Petition, with respect to the challenged claims.

To the extent the same art or arguments were previously presented to the Office, the Office erred to the extent it failed to fully consider the significance of the art or arguments as set forth in this Petition. Accordingly, even if the first part of

the test is satisfied, the Board further should not deny institution based on the second part of the test.

VIII. NOTICES AND STATEMENTS

Pursuant to 37 C.F.R. § 42.8(b)(1), Cloudflare, Inc. is the real party-in-interest for Petitioner.

Pursuant to 37 C.F.R. § 42.8(b)(2), Petitioner identifies the following related matters. The '497 patent is asserted in the following litigation matters:

Case	Date Filed
<i>PacSec3, LLC v. Splunk Inc.</i> , Case No. 2:22-cv-00056 (E.D. Tex.) (consolidated with <i>Forescout</i> case below)	Feb. 18, 2022
<i>PacSec3, LLC v. Forescout Techs., Inc.</i> , Case No. 2:22-cv-00055 (E.D. Tex.)	Feb. 17, 2022
<i>PacSec3, LLC v. Mimecast N. Am., Inc.</i> Case No. 3:22-cv-00396 (N.D. Tex.)	Feb. 17, 2022
<i>PacSec3, LLC v. Imperva, Inc.</i> , Case No. 6:22-cv-00167 (W.D. Tex.)	Feb. 17, 2022
<i>PacSec3, LLC v. Rapid7, Inc.</i> , Case No. 6:22-cv-00168 (W.D. Tex.)	Feb. 17, 2022
<i>PacSec3, LLC v. Darktrace, PLC</i> , Case No. 6:22-cv-00126 (W.D. Tex.)	Feb. 4, 2022
<i>PacSec3, LLC v. CrowdStrike Holdings, Inc.</i> , Case No. 6:22-cv-00127 (W.D. Tex.)	Feb. 4, 2022
<i>PacSec3, LLC v. BlackBerry Corp.</i> , Case No. 6:22-cv-00128 (W.D. Tex.)	Feb. 4, 2022
<i>PacSec3, LLC v. Cloudflare, Inc.</i> , Case No. 6:22-cv-00129 (W.D. Tex.)	Feb. 4, 2022

Case	Date Filed
<i>PacSec3, LLC v. Fortinet, Inc.</i> , Case No. 2:21-cv-00450 (E.D. Tex.)	Dec. 13, 2021
<i>PacSec3, LLC v. NetScout Sys., Inc.</i> , Case No. 2:21-cv-12463 (E.D. Mich.)	Oct. 20, 2021
<i>PacSec3, LLC v. Juniper Networks, Inc.</i> , Case No. 5:21-cv-074812 (N.D. Cal.)	Oct. 6, 2021
<i>PacSec3, LLC v. Juniper Networks, Inc.</i> , Case No. 2:21-cv-00228 (E.D. Tex.)	June 23, 2021
<i>PacSec3, LLC v. WatchGuard Techs., Inc.</i> , Case No. 6:21-cv-00633 (W.D. Tex.)	June 18, 2021
<i>PacSec3, LLC v. McAfee, LLC</i> , Case No. 2:21-cv-00140 (E.D. Tex.)	Apr. 21, 2021
<i>PacSec3, LLC v. Palo Alto Networks, Inc.</i> , Case No. 2:21-cv-00141 (E.D. Tex.)	Apr. 21, 2021
<i>PacSec3, LLC v. Juniper Networks, Inc.</i> , Case No. 6:21-cv-00387 (W.D. Tex.)	Apr. 21, 2021
<i>PacSec3, LLC v. Cisco Sys., Inc.</i> , Case No. 6:21-cv-00388 (W.D. Tex.)	Apr. 21, 2021
<i>PacSec3, LLC v. F5 Networks Inc.</i> , Case No. 2:20-cv-01828 (W.D. Wash.)	Dec. 14, 2020
<i>PacSec3, LLC v. F5 Networks Inc.</i> , Case No. 2:20-cv-00697 (D. Utah)	Oct. 2, 2020
<i>PacSec3, LLC v. NetScout Sys., Inc.</i> , Case No. 6:20-cv-00914 (W.D. Tex.)	Oct. 2, 2020

The '497 patent is the subject of the pending *ex parte* reexamination, Control No. 90/014,746, currently on appeal to the Board. The '497 patent was the subject of IPR2022-01230 (*Splunk Inc. v. PacSec3, LLC*), which was terminated due to settlement prior to any institution decision.

Pursuant to 37 C.F.R. § 42.8(b)(3), Petitioner identifies the following counsel (and a power of attorney accompanies this Petition).

LEAD COUNSEL	BACKUP COUNSEL
Craig Tolliver ctolliver@ccrglaw.com Registration No.: 45,975 Charhon Callahan Robson & Garza, PLLC 3333 Lee Parkway Suite 460 Dallas, TX 75219 Tel: 469-587-7263 Fax: 214-764-8392	John Heuton jheuton@ccrglaw.com Registration No.: 62,467 Charhon Callahan Robson & Garza, PLLC 3333 Lee Parkway Suite 460 Dallas, TX 75219 Tel: 214-521-6400 Fax: 214-764-8392

Pursuant to 37 C.F.R. § 42.8(b)(4), service information for lead and back-up counsel is provided above. Petitioner consents to electronic service by email to the email addresses noted above.

Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the '497 patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review of the challenged claims on the grounds identified herein.

The USPTO is authorized to charge any required fees, including the fee as set forth in 37 C.F.R. § 42.15(a) and any excess claim fees, to 603576.

IX. CONCLUSION

Petitioner requests that the Board initiate *inter partes* review and cancel all the challenged claims of the '497 patent.

Dated: February 6, 2023

Respectfully submitted,

By: / Craig Tolliver /
Craig Tolliver
Registration No.: 45,975
CHARHON CALLAHAN ROBSON &
GARZA, PLLC
3333 Lee Parkway
Suite 460
ctolliver@ccrglaw.com
Dallas, TX 75219
Tel: 469-587-7263
Fax: 214-764-8392

Certification of Word Count (37 C.F.R. § 42.24)

I hereby certify that this Petition for *Inter Partes* Review has 13,983 words (as counted by the “Word Count” feature of the Microsoft Word™ word-processing system), exclusive of “a table of contents, a table of authorities, mandatory notices under § 42.8, a certificate of service or word count, or appendix of exhibits or claim listing.”

Dated: February 6, 2023

By: /Craig Tolliver/
Craig Tolliver

Certificate of Service (37 C.F.R. § 42.6(e)(4) and 42.205(a))

I hereby certify that the attached Petition for *Inter Partes* Review and supporting materials were served as of the below date by FedEx, which is a means at least as fast and reliable as U.S. Express Mail, on the Patent Owner at the correspondence address indicated for U.S. Patent No. 7,523,497, as well as at the address of counsel for Patent Owner in the district court action against Cloudflare related to the '497 Patent, further indicated below:

Donald Cohen
BELASCO JACOBS & TOWNSLEY, PC
6701 Center Drive West
14th Floor
Los Angeles CA 90045

William P. Ramey
RAMEY LLP
William P. Ramey, III
5020 Montrose Blvd., Suite 800
Houston, TX 77006

Inter Partes Review of U.S. Patent No. 7,523,497

Dated: February 6, 2023

By: / Craig Tolliver /
Craig Tolliver
Registration No.: 45,975
CHARHON CALLAHAN ROBSON &
GARZA, PLLC
3333 Lee Parkway
Suite 460
ctolliver@ccrglaw.com
Dallas, TX 75219
Tel: 469-587-7263
Fax: 214-764-8392