

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CLOUDFLARE, INC.

Petitioner,

v.

PACSEC3, LLC

Patent Owner.

IPR2023-00544 (Patent No. 7,523,497)

**PATENT OWNER'S PRELIMINARY RESPONSE
TO PETITION FOR INTER PARTES REVIEW**

TABLE OF CONTENTS

I. INTRODUCTION	1
II. OVERVIEW OF THE ‘497 PATENT	2
A. Brief Description	2
B. The ‘497 Patent Prosecution History.....	4
C. Claim Construction.....	4
IV. THE ASSERTED PRIOR ART	7
A. Wetherall (Ex. 1006)	7
B. Doeppner (Ex. 1007)	9
C. Savage (Ex. 1008).....	10
D. Cheriton (Ex. 1009).....	11
V. PETITIONER HAS NOT DEMONSTRATED A REASONABLE LIKELIHOOD OF SUCCESS FOR THE GROUNDS ADVANCED IN THE PETITION, AND THE PETITION SHOULD BE DENIED	12
A. Requirements for Showing Obviousness Under 35 U.S.C. § 103	12
B. Petitioner Fails to Establish in Ground 1 that Challenged Claims 7-12 are Obvious Over Wetherall and Doeppner	14
1. Claim 7	14
2. Claim 8	18
3. Claim 9	21
4. Claim 10	22
5. Claim 11	23
6. Claim 12	26
C. Petitioner Fails to Establish in Ground 2 that Challenged Claims 7-12 are Obvious Over Wetherall and Savage	26
D. Petitioner Fails to Establish in Ground 3 that Challenged Claims 7-12 are Obvious Over Cheriton and Doeppner.....	31
E. Petitioner Fails to Establish in Ground 4 that Challenged Claims 7-12 are Obvious Over Cheriton and Savage	37
VI. CONCLUSION.....	39

TABLE OF AUTHORITIES

Cases

<i>Ex parte Davis</i> , 80 USPQ 448	6
<i>Graham v. John Deere Co.</i> , 383 U.S. 1 (1966)	13, 17, 21
<i>Pers. Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	13
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	13
<i>LA Biomedical Res. Inst. Harbor-UCLA Med. Ctr. v. Eli Lilly</i> , 849 F.3d 1049 (Fed. Cir. 2017)	13
<i>Broadcom Corp. v. Emulex Corp.</i> , 732 F.3d 1325 (Fed. Cir. 2013)	14
<i>In re Van Os</i> , 844 F.3d 1359 (Fed. Cir. 2017)	14
<i>Innogenetics, N.V. v. Abbott Labs.</i> , 512 F.3d 1363 (Fed. Cir. 2008)	14
<i>CFMT, Inc. v. Yieldup Intern. Corp.</i> , 349 F.3d 1333, 1342 (Fed. Cir. 2003)	17, 21, 28

PTAB Cases

<i>Apple, Inc. v. Contentguard Holdings</i> , IPR2015-00355, Paper 9 (PTAB June 26, 2015)	13
---	----

Statutes

35 U.S.C. §103	12
----------------------	----

Rules

37 C.F.R. § 42.107	1
--------------------------	---

Exhibit List

Exhibit No.	Exhibit Description
2001	Microsoft Computer Dictionary
2002	Computer Networking: A top-down Approach

I. INTRODUCTION

On February 6, 2023, Cloudflare, INC. (“Petitioner”) submitted a Petition for *Inter Partes* Review (“Petition”) of U.S. Patent No. 7,523,497 (“the ‘497 Patent,” “Ex. 1001”), challenging Claims 7-12 (“Challenged Claims”). Pursuant to 37 C.F.R. § 42.107, Patent Owner Pacsec3, LLC, (“Patent Owner”) files this Preliminary Patent Owner Response to the Petition, setting forth reasons the Board should deny institution.

Petitioner challenges the patentability of Claims 7-12 of the ‘497 Patent based on four (4) different alleged prior art references as follows.

U.S. Pat. No. 6,801,503 (“Wetherall”);

“Using Router Stamping to Identify the Source of IP Packets,” (“Doeppner”);

“Practical Network Support for IP Traceback” (“Savage”); and

U.S. Pat. No. 7,120,931 (“Cheriton”).

Petitioner requests institution of the IPR proceeding on the following grounds.

Ground	Claims	Basis
1	7-12	§103– Wetherall, Doeppner
2	7-12	§103– Wetherall, Savage
3	7-12	§103–Cheriton, Doeppner
4	7-12	§103–Cheriton, Savage

Petitioner fails to establish a reasonable likelihood that the Challenged Claims are unpatentable. Patent Owner will specifically address each of Petitioners arguments in the following sections.

II. OVERVIEW OF THE '497 PATENT

A. Brief Description

1. Problems identified in the prior art

At the time of the invention of the '497 Patent, various methods have been developed for minimizing the effect of packet flooding attacks against computers connected to a network. The methods include using source and destination address matching to determine if packets should be transmitted to an end station or the end station disabled from participating in the network. The information used is the source/ destination address pairs in the packet. The methods assume this information is accurate. In an attack, this information will not be. The attacker will falsify the source address in order to confound the defense if it uses information the attacker controls, such as the source address. Ex.1001, 1:35-43. 1:67-2:5.

2. Summary of the Claimed Subject Matter

In order to address the deficiencies of prior network defense systems, the '497 Patent takes an approach to use the information of path rather than the information of source/ destination to defend packet flooding.

The '497 Patent teaches a packet flooding defense method 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. Ex.1001, 2:6-9. According to the '497 Patent, the defense is distributed among cooperating sites and routers. A set of transitively connected cooperating machines is called a "cooperating neighborhood". The quality of the defense is related to the size of the cooperating neighborhood, a larger neighborhood providing better defense. Within the neighborhood it is possible to trace the forwarding path of packets. The association of packets with the "users" is approximated by associating packets with "places" in the cooperating neighborhood from which those packets are forwarded. Ex.1001, 2:30-39.

The '497 Patent teaches that routers supply data about the forwarding path of the packets that arrive at a site. The site can use this data to allocate service. Ex.1001, 2:54-56. 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. Ex,1001, 6: 20-24; Fig. 1. In this invention, **a path (which is not controlled by the attacker) is used** to determine the actual direction of the packet flow towards the victim. Bandwidth is allocated based upon path (which is done via packet marks provided by routers leading up to the victim) Ex.1001, 3:62-66.

B. The ‘497 Patent Prosecution History

The application issued as the ‘497 Patent was filed on May 7, 2004. Ex. 1001, 1:7-15. Which is a continuation of application No.09/715,813, filed on Nov. 16, 2000. Ex. 1001, 1:7-24.

References cited by the applicant and considered by the Examiner include U.S. Patent No. 5,367,523 (Chang). After amendment, On November 23, 2008, “A Notice of Allowance” was mailed allowing claims 1-18, 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.

C. Claim Construction

According to 37 C.F.R. §42.100(b), in an inter partes review, claim terms are construed using the same standard used in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

The ordinary and customary meaning of a term may be evidenced by a variety of sources, including the words of the claims themselves, the specification, drawings, and prior art. However, the best source for determining the meaning of a

claim term is the specification – the greatest clarity is obtained when the specification serves as a glossary for the claim terms. The words of the claim must be given their plain meaning unless the plain meaning is inconsistent with the specification. *In re Zletz*, 893 F.2d 319, 321, 13 USPQ2d 1320, 1322 (Fed. Cir. 1989); *Chef America, Inc. v. Lamb-Weston, Inc.*, 358 F.3d 1371, 1372, 69 USPQ2d 1857 (Fed. Cir. 2004).

In accordance with these principles, Patent Owner submits that the terms of the '497 Patent are clear on their face, except the following claim term which should be construed as follows:

a. “Path” (Claims 7 and 10)

An ordinary meaning of the term “path,” as known in the art, is defined in Microsoft Computer Dictionary as “In communications, a link between two nodes in a network.” Ex. 2001, at 394. James F. Kurose describes the term “path” in the book “Computer Networking: A top-down Approach” as “The sequence of communication links and packet switches traversed by a packet from the sending end system to the receiving end system is known as a route or path through the network” Ex. 2002, at 4. and “a packet starts in a host (the source), passes through a series of routers, and ends its journey in another host (the destination). As a packet travels from one node (host or router) to the subsequent node (host or router) along

this path, the packet suffers from several types of delays at each node along the path.”

Ex. 2002 at 35-36.

According to ordinary meaning, the term “path” is a link between two nodes (source and destination) in a network, the link can be a series of routers or packet switches. Which means a path must include a link such as a series of routers or packet switches.

The language of claim 7 defines path as “said path comprising all routers in said network via which said packets are routed to said computer.” which means a “path” being a path in claim 7 because it includes routers, without router, there can be no path either. Since “[C]omprising” is a term of art used in claim language which means that the named elements are essential, but other elements may be added and still form a construct within the scope of the claim. *Ex parte Davis*, 80 USPQ 448, 450. The specification also supports that “Routers will supply data about the forwarding path of the packets that arrive at a site.” Ex. 1001, 2:54-55. “In this invention a path (which is not controlled by the attacker) is used to determine the actual direction of the packet flow towards the victim.” Ex. 1001, 3:62-64.

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

Patent Owner reserves all rights to raise claim construction arguments in district court and in this proceeding should the Board grant institution.

III. LEVEL OF ORDINARY SKILL IN THE ART

For purposes of this Response, PO adopt Petitioner's proffered level of ordinary skill in the art because it comports with the technology and claims of the '497 Patent as well as the asserted prior art.

IV. THE ASSERTED PRIOR ART

A. Wetherall (Ex. 1006)

Wetherall describes a method and system for "regulating network traffic destined for a network node, such as a server, to facilitate ensuring the quality of service provided by the network to the network node and the parties interacting with it, such as a client." Ex.1006, 1:44-48.

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. Network 110 is also provided with director 102 to manage network traffic routing within network 100 to ensure a desired not-to-exceed network traffic profile of server 110 is adhered to. In one embodiment, the desired not-to-exceed network traffic profile is specified using one or more metrics, and

preferably by network traffic types. For example, at most 10% each of the incoming bandwidth to be used for TCP synchronize (SYN) packets and for domain name system (DNS) packets, with remaining incoming bandwidth to be used by other TCP traffic. Ex.1006, 3:47-57.

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

In operation, director 102 is first provided with a desired “not-to-exceed” network traffic profile of server 110, and a topology and routing map of network 100. Director 102 receives network traffic reports on the network traffic routed through routing devices 106 a-106 h. The reported data include various statistics and “characteristic” information describing the network traffic routed through the ingress/egress interfaces of routing devices 106 a-106 h. For example, the reported data includes destination information or network traffic types. In addition to the TCP SYN and DSN packets, network traffic types may further include Web, Real Networks, Secure Web, Other TCP, Other user datagram protocol (UDP), internet control message protocol (ICMP), TCP packets with acknowledge (ACK) set, TCP packets without SYN set, and so forth. In general, any information carried as part of

the packets may be used as typing criteria to divide the network traffic into different traffic types. i.e. whatever data are necessary to support the employment of the desired “not-to-exceed” metrics. Ex.1006, 6:4-48.

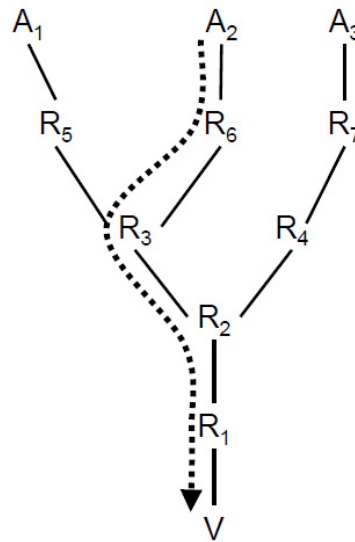
In response to the receipt of the reported data, director 102 automatically determines whether network traffic routing in network 100 needs to be (further) regulated or de-regulated (using the received data, and the limits and operating margins specified in the earlier described desired “not-to-exceed” network traffic profile). Regulation/de-regulation is advantageously performed in a progressive manner, thus if regulation (or further regulation) is needed, director 102 determines the regulation to be imposed on the routing devices of the next **degree of separation** (along the reverse direction the routing paths traversed by the packets to reach the network node). if e.g. regulation is already in effect on both the ingress and egress interfaces of routing devices 106 a-106 b, further regulation is determined for routing devices 106 c-106 e **with two degrees of separation from server 110**. Ex.1006, 6:50-7:6.

B. Doeppner (Ex. 1007)

Doeppner discloses a “router stamping” method that identifies the source of Denial of Service attacks. Ex.1007, Abstract. In Doeppner, a router “stamps” a data packet with an IP address corresponding to the previous router, Ex.1007, 184-185, The data packet’s path can then be determined based on packet marks.

C. Savage (Ex. 1008)

Fig. 1 of Savage is shown below.



Ex. 1008 Figure 1

10

method (node append algorithm) is to append each node's address to the end of the packet as it travels through the network from attacker to victim, every packet received by the victim arrives with a complete ordered list of the routers it traversed—a built-in attack path (Ex.1008, 299).

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

Savage teaches inserting a mark in each packet as it traverses each router in transit. The algorithm attempts to determine the approximate origin of attack traffic (Ex.1008, 304).

D. Cheriton (Ex. 1009)

Cheriton discloses a method and system for generating filters based on analyzed flow data. The method comprises separating the data into different network

flows, analyzing at least one of the network flows, and detecting potentially harmful network flows. Ex. 1009, 2:20-24.

The flow may be classified, for example, by source node (IP address), destination node (IP address), detail destination node (destination address, source TCP/UDP port, destination TCP/UDP port, protocol), host matrix (source address/destination address pair), detail host matrix (source/destination address, port, protocol), source TCP/UDP (transportation layer source port), destination TCP/UDP port (transport layer destination port), protocol (protocol name), detail interface (input-output physical interface pair), or some combination thereof. Ex. 1009, 6:10-20.

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. That network flow can be filtered such that “only the destructive packets received from the actual attacker are dropped.” Ex.1009, 7:19-24. Filters can be implemented in a router, or in a firewall between the router and host computer. Ex.1009, 3:38-40.

V. PETITIONER HAS NOT DEMONSTRATED A REASONABLE LIKELIHOOD OF SUCCESS FOR THE GROUNDS ADVANCED IN THE PETITION, AND THE PETITION SHOULD BE DENIED

A. Requirements for Showing Obviousness Under 35 U.S.C. § 103

The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art, (2) any

differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) where in evidence, so called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). The Board has held that a failure to identify the differences between the claimed subject matter and the prior art is fatal to an obviousness challenge. See, *Apple, Inc. v. Contentguard Holdings, Inc.*, IPR2015-00355, Decision Denying Institution of *Inter Partes* Review, Paper 9 at 9-10 (P.T.A.B. June 26, 2015) (denying institution for failure to identify the differences between the claimed subject matter and the prior art).

In arriving at an obviousness determination, the Board must sufficiently explain and support the conclusions that the prior art references disclose all the elements recited in the Challenged Claims and a relevant skilled artisan not only could have made, but would have been motivated to combine all the prior-art references in the way the patent claims. *Pers. Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017). That is, even if all the claim elements are found across a number of references, an obviousness determination must consider whether a person of ordinary skill in the art would have been motivated to combine those references. *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1368 (Fed. Cir. 2016); *Los Angeles Biomedical Res. Inst. at Harbor-UCLA Med. Ctr. v. Eli Lilly Co.*, 849 F.3d 1049, 1067 (Fed. Cir. 2017) (vacating and remanding an obviousness determination, in part, because the Board did not make factual findings

as to whether there was an apparent reason to combine all three prior art references to achieve the claimed invention and whether a POSITA would have had a reasonable expectation of success from such a combination). This combination determination, as supported by an articulated motivation to combine, requires a plausible rationale as to why those prior art references would have worked together. *Broadcom Corp. v. Emulex Corp.*, 732 F.3d 1325, 1335 (Fed. Cir. 2013). Absent some articulated rationale, a “common sense” finding is no different than the conclusory statement “would have been obvious.” *In re Van Os*, 844 F.3d 1359, 1361 (Fed. Cir. 2017). Of additional importance, “knowledge of a problem and motivation to solve it are entirely different from motivation to combine particular references.” *Innogenetics, N.V. v. Abbott Labs.*, 512 F.3d 1363, 1373 (Fed. Cir. 2008).

B. Petitioner Fails to Establish in Ground 1 that Challenged Claims 7-12 are Obvious Over Wetherall and Doeppner

1. Claim 7

Independent claim 7 has been divided into elements for consideration by the Petitioner as follows:

[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:

[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;

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

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

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

a. Wetherall in view of Doeppner does not teach the limitation 7[B]

To argue that Wetherall discloses limitation “classifying data packets received at said host computer into wanted data packets and unwanted data packets **by path**.” Petitioner proffers that Wetherall discloses “any information carried as part of the packets may be used as typing criteria to divide the network traffic into different traffic types.” (Citing 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. (Citing EX1006, 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. (Citing Ex.1004, ¶84.) Pet., 20.

Petitioner further proffers that Doeppner discloses “identify[ing] and isolat[ing] problem-causing packets” in a DoS attack. (Citing 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. (Citing Ex.1007, 187-188; Ex.1004, ¶85.) For example, packets originating from source Rx and having host computer T as their destination can be blocked by routers in a network. (Citing Ex.1007, 187-188; Ex.1004, ¶85.) These are unwanted packets associated with the DoS attack. (Citing Ex.1004, ¶85.) Meanwhile, packets not having that path (wanted packets) are left uninterrupted. (Citing Ex.1007, 187-188; Ex.1004, ¶85.) Pet., 21.

It is clear that Petitioner equates “source and destination addresses” in Wetherall and “source” in Doeppner with “path” in the ’497 Patent. As set forth in above claim construction in section II.C, a “path” must include a link such as a series of routers, a “path” must not comprise only source and destination.

The ’497 Patent teaches a packet flooding defense method 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. Ex.1001, 2:6-9. The method is radically

different from methods in use at the time. While other methods at the time used source and destination address matching to determine if packets should be transmitted to an end station or the end station disabled from participating in the network. Ex.1001, 1:35-43. the information used is the source/ destination address pairs in the packet. The methods assume this information is accurate. In an attack, this information will not be. The attacker will falsify the source address in order to confound the defense if it uses information the attacker controls, such as the source address. Ex.1001, 1:67-2:5. The '497 Patent takes an approach to use the information of path rather than the information of source/ destination to defend packet flooding.

Thus, Wetherall in view of Doeppner does not teach “classifying data packets received at said host computer into wanted data packets and unwanted data packets by path” as required by Claim 7.

b. Wetherall in view of Doeppner does not Not Render Claim 7 Obvious

Petitioner fails to undertake a proper Graham analysis, because Wetherall in view of Doeppner lacks evidence of crucial limitations of claim 7, such as the elements [7B]. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Therefore, Wetherall in view of Doeppner does not render claim 7 obvious because it has not established its prima facie case, since “obviousness requires a suggestion of all limitations in a claim.” *CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003).

2. Claim 8

Independent claim 8 has been divided into elements for consideration by the Petitioner as follows:

[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:

[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;

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

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

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

[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

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

a. Wetherall in view of Doeppner does not teach the limitation 8[A]

Semantic analyzing of the limitations 8[A]-8[E], a POSITA would conclude that “classifying data packets” is based on the destination of the packets (the host computer), that is, the criterion of the classification is the destination of the packets. The method of “classifying data packets” includes controlling the rate of transmission of data packets from routers to said computer (destination of the packets) so that data packet transmissions received at said computer are kept below the maximum acceptable processing rate for each data packet class.

Therefore, the limitation 8[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” shows that the criterion of “classifying data packets” is the destination of the packets.

To argue that Wetherall in view of Doeppner does not teach the limitation 8[A], Petitioner only proffers “This element is taught by Wetherall in view of Doeppner as described above for element 7[B].”

Regarding element 7[B], Petitioner proffers that Wetherall discloses “any information carried as part of the packets may be used as typing criteria to divide the network traffic into different traffic types.” (Citing 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. (Citing Ex1006, 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. (Citing Ex.1004, ¶84.) Pet., 20.

According to Petitioner, the criterion of “classifying data packets” in Wetherall is the “specific source and destination address combinations” of the packets, which is distinct from the criterion of claim 8 of the ‘497 Patent, since the criterion of “classifying data packets” is only the destination address of the packets.

Regarding element 7[B], Petitioner further proffers that Doeppner discloses “identify[ing] and isolat[ing] problem-causing packets” in a DoS attack. (Citing 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. (Citing Ex.1007, 187-188; Ex.1004, ¶85.) For example, packets originating from source Rx and having host computer T as their destination can be blocked by routers in a network. (Citing Ex.1007, 187-188; Ex.1004, ¶85.) These

are unwanted packets associated with the DoS attack. (Citing Ex.1004, ¶85.) Pet., 21.

It is clear that the criterion of “classifying data packets” in Doeppner is the source of the packets, not the destination address of the packets as required by claim 8 of the ‘497 Patent.

b. Wetherall in view of Doeppner does not Not Render Claim 8 Obvious

Petitioner fails to undertake an adequate Graham analysis, because Wetherall in view of Doeppner lacks evidence of crucial limitations of claim 8, such as the elements 8[A]. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Therefore, Wetherall in view of Doeppner does not render claim 8 obvious because it has not established its prima facie case, since “obviousness requires a suggestion of all limitations in a claim.” *CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003).

3. Claim 9

Claim 9 depends from claim 8, containing all limitations of claim 8, thus claim 9 is not obvious over Wetherall in view of Doeppner for at least the same reasons.

4. Claim 10

Independent claim 10 has been divided into elements for consideration by the Petitioner as follows:

[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:

[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;

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

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

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

As to claim 10, Petitioner proffers “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. (Citing EX-1004, ¶112.) Pet.33.

The elements of claim 10 include “said path comprising all routers in said network via which said packets are routed to said computer” in 10[A] and “classifying data packets received at said router via packet marks provided by routers leading to said host computer by path” of 10[B], which are identical to corresponding elements of claim 7[B]. As set forth above, Wetherall in view of Doeppner does not teach element 7[B], similarly, Wetherall in view of Doeppner does not teach element 10[B], therefore, Wetherall in view of Doeppner does not render claim 10 obvious.

5. Claim 11

Independent claim 11 has been divided into elements for consideration by the Petitioner as follows:

[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:

[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;

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

[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;

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

[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

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

As to claim 11, Petitioner proffers 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. (Citing Ex.1006, 4:4-8, Fig. 1; Ex.1004, ¶126.) Pet. 44-41.

Although Claim 11 includes limitations analogous to claim 8, claim 11 comprises limitation distinct from claim 8. For example, claim 11 comprises limitation 11[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” which claim 8 does not include.

Regarding limitation 11[C], Petitioner only proffers “Wetherall in view of Doeppner teaches this element as described above for 8[C] and V.B.7. (Citing Ex. 1004, ¶131.) Pet. 42.

Limitation 8[C] recites “determining the rate at which data packets of each class are transmitted from a router to said computer.” Petitioner proffers that “The reported data [in Wetherall] 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.” (Citing Ex.1006, 6:42-48.) Pet.28. Petitioner then concludes that 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 (Citing Ex. 1004, ¶99). Pet.28.

To the extent that Wetherall in view of Doeppner teaches Limitation 8[C], since Limitation 8[C] is different from Limitation 11[C], specifically, Wetherall in view of Doeppner does not teach “rate at which data packets of each class transmitted from a second router to said first router **is determined by the first router.**”

Wetherall in view of Doeppner does not teach element 11[C], therefore, Wetherall in view of Doeppner does not render claim 11 obvious.

6. Claim 12

Claim 12 depends from claim 11, containing all limitations of claim 11, thus claim 12 is not obvious over Wetherall in view of Doeppner for at least the same reasons.

C. Petitioner Fails to Establish in Ground 2 that Challenged Claims 7-12 are Obvious Over Wetherall and Savage

1.Claim 7

a. Wetherall in view of Savage does not teach the limitation 7[B]

As to the limitation 7[B], Petitioner only proffers “Wetherall in view of Savage teaches this element as described in V.B.3.c for Wetherall.” Pet.51.

As set forth in above section V.B.1, Wetherall does not teach “classifying data packets received at said host computer into wanted data packets and unwanted data packets **by path**” as required by limitation 7[B].

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

In order to determine the attack path and the associated attack origin for each attacker, Savage provides a marking algorithm including two methods. The first method (node append algorithm) is to append each node’s address to the end of the packet as it travels through the network from attacker to victim, every packet received by the victim arrives with a complete ordered list of the routers it traversed—a built-in attack path. The second method includes a node sampling algorithm and edge sampling algorithm. Ex. 1008 at 299.

Savage describes a traceback technique using packet marks to encode path. The focus of Savage is to trace attacks back towards their origin—ideally stopping an attack at the source. Ex. 1008 at 295. Savage is concerned with using the path information in the detected attack packets to traceback to the true source address of the attack. It is thus clear that just like Doeppner, Savage classifies data packets by source, not by path.

b. Wetherall in view of Savage does not Not Render Claim 7 Obvious

Petitioner fails to undertake a Graham analysis, because Wetherall in view of Savage lacks evidence of crucial limitations of claim 7, such as the elements [7B]. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Therefore, Wetherall in view of Savage does not render claim 7 obvious because it has not established its prima facie case, since “obviousness requires a suggestion of all limitations in a claim.” *CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003).

2.Claim 8

Wetherall in view of Savage does not teach the limitation 8[A]

Regarding the limitation 8[A], Petitioner proffers “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 A₂ to host computer V, 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” (Citing Ex. 1004, ¶166.). Pet. 52.

As set forth in above section V.B.2, the criterion of “classifying data packets” in limitation 8[A] is the destination of the packets. Wetherall does not teach limitation 8[A].

As set forth in above section V.C.1, the criterion of “classifying data packets” of Savage is the source of the packets, not the destination of the packets, thus Savage does not teach limitation 8[A] either.

Wetherall in view of Savage does not teach element 8[A], therefore, Wetherall in view of Savage does not render claim 8 obvious.

3.Claim 9

Claim 9 depends from claim 8, containing all limitations of claim 8, thus claim 9 is not obvious over Wetherall in view of Savage for at least the same reasons.

4.Claim 10

As to claim 10, Petitioner proffers “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. Pet.54.

The elements of claim 10 include “said path comprising all routers in said network via which said packets are routed to said computer” in 10[A] and “classifying data packets received at said router via packet marks provided by routers leading to said host computer by path” of 10[B], which are identical to corresponding elements of claim 7[B]. As set forth above, Wetherall in view of Savage does not teach element 7[B], similarly, Wetherall in view of Savage does not teach element 10[B], therefore, Wetherall in view of Savage does not render claim 10 obvious.

5.Claim 11

Petitioner proffers “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.” Pet., 57.

Regarding limitation 11[C], Petitioner only proffers “Wetherall in view of Savage teaches this element as described above for 8[C] and V.C.7. (Citing Ex.1004, ¶189.) Pet.,57.

As set forth in above section V.B.5, Wetherall does not teach element 11[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.” Since the focus of Savage is to trace attacks back towards their origin--ideally stopping an attack at the source, Savage does not teach element 11[C] either. Therefore, Wetherall in view of Savage does not render claim 11 obvious.

6. Claim 12

Claim 12 depends from claim 11, containing all limitations of claim 11, thus claim 12 is not obvious over Wetherall in view of Savage for at least the same reasons.

D. Petitioner Fails to Establish in Ground 3 that Challenged Claims 7-12 are Obvious Over Cheriton and Doeppner

1.Claim 7

a. Cheriton in view of Doeppner does not teach the limitation 7[B]

As to limitation 7[B], Petitioner proffers “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.” (Citing Ex.1009, 6:7-10, Fig. 3; EX-1004, ¶211.) 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.” (Citing Ex.1009, 8:30-44; EX-1004, ¶212.)” Pet. 65-66.

Petitioner further proffers 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.” (Citing Ex.1009, 6:38-42, 6:10-20; Ex. 1004, ¶214.) Thus the classification is by path (i.e., from the source device to the destination device). (Citing Ex.1004, ¶214.)

The cited portion of the Petition shows that Petitioner equates “source and destination addresses” in Cheriton with “path” in the ’497 Patent. As set forth in

above claim construction in section II.C, a “path” must include a link such as a series of routers, a “path” must not comprise only source and destination. Thus, Cheriton does not teach “classifying data packets received at said host computer into wanted data packets and unwanted data packets **by path**” as required by the limitation 7[B].

As set forth above in section V.B.1, Doeppner does not teach the limitation 7[B] either. Since Cheriton in view of Doeppner does not teach element 7[B], Cheriton in view of Doeppner does not render claim 7 obvious.

2. Claim 8

Regarding the limitation 8[C] “determining the rate at which data packets of each class are transmitted from a router to said computer.” Petitioner proffers (Cheriton’s) Flow analyzer 122 “monitors the statistics associated with aggregate filters 10.” (Citing 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 (server16) and filters data packets transmitted from the router to the host computer (Citing Ex.1009, Fig. 1; Ex.1004, ¶223.) Pet.70

Petitioner further proffers “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.” (Citing 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. (Citing Ex,1009, 8:11-14; Ex,1004, ¶224.)” Pet.71.

Cheriton relates to filtering data in high-speed computer networks. High-speed networks make detecting and responding to certain types of failures and attacks difficult. The high speed makes it difficult to carefully examine every packet or even maintain state and monitor the state of every data stream without extensive hardware support. Ex.1009,1:59-63.

In order to filter data in high-speed computer networks, Cheriton provides a method generally comprises separating the data into different network flows, analyzing at least one of the network flows, and detecting potentially harmful network flows (corresponding to data packet in the ‘497 Patent). Ex.1001, 2:20-25. In Cheriton, detecting potentially harmful network flows comprises detecting source of the potentially harmful network flows and limit transmitting rate of network flows from the source, for example, Cheriton describes:

Once the flow 64 passes through the netflow directory, flow records 120 are created that provide information about a particular network flow (FIG. 3). The flow records 120 are sent to a flow analyzer 122 where the flows are analyzed to

identify characteristics of packets 78 involved in an attack or a failure. For example, if a large number of SYN packets or an unusual distribution of packets is identified as **coming from a source (e.g., attacker 20)**, it is likely that the source is involved in an attack. Therefore, instead of filtering out all data arriving from the identified organization, **only the destructive packets received from the actual attacker are dropped.** Ex.1009,6:66-7:24.

Although Cheriton's Flow analyzer 122 can detect "a rate of traffic exceeds a maximum," the filter is used to "identity detailed characteristics of packets involved in an attack or a failure" Ex.1009, 5: 28-29. In order to dissolve the effect of denial of service attack, the method of Cheriton is to identify sources that appear to represent excessive traffic and limit the traffic of the identified sources. The method is described as follows:

For example, a policy may indicate a maximum aggregate rate of HTTP traffic of 100 Mbps and a maximum rate from any source of 25 Mbps. Rather than explicitly policing every flow, the system can be used to identify sources that appear to represent excessive traffic, allowing aggregate filters to be created that separate them out of the overall aggregate and throttle their traffic appropriately. Ex.1009,8:37-44.

The cited portion of Cheriton shows that Cheriton identifies source of potentially harmful data package and limits the transmission rate of the identified sources. There is no need in Cheriton to determine the rate at which data packets of

each class are transmitted from a router to said computer, thus Cheriton does not teach the limitation 8[C]. limitations 8[D] and 8[E] recite further limitation of transmission rate from the router based on limitation 8[C]. Cheriton does not teach the limitation 8[C] and certainly does not teach the limitations 8[D] and 8[E].

Doeppner teaches using packet marks 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; Doeppner does not teach limiting transmission rate of routers, thus Doeppner does not teach the limitations 8[C], 8[D] and 8[E].

Cheriton in view of Doeppner does not teach limitations 8[C], 8[D] and 8[E], therefore, Cheriton in view of Doeppner does not render claim 8 obvious.

3. Claim 9

Claim 9 depends from claim 8, containing all limitations of claim 8, thus claim 9 is not obvious over Cheriton in view of Doeppner for at least the same reasons.

4. Claim 10

Similar to V.D.1, Cheriton in view of Doeppner does not teach element 10[B], Cheriton in view of Doeppner does not render claim 8 obvious.

5. Claim 11

Cheriton in view of Doeppner does not teach the limitations 11[B] -11[E]

the limitations 11[B] -11[E] recite as follows:

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

[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;

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

[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;

As set forth in above V.D.2 Section, Cheriton and Doeppner does not teach limiting transmission rate of routers, while limitations 11[B] -11[E] are relate to limitation of transmission rate of routers, thus Cheriton and Doeppner do not teach the limitations 11[B] -11[E], Cheriton in view of Doeppner does not render claim 11 obvious.

6. Claim 12

Claim 12 depends from claim 11, containing all limitations of claim 11, thus claim 12 is not obvious over Cheriton in view of Doeppner for at least the same reasons.

E. Petitioner Fails to Establish in Ground 4 that Challenged Claims 7-12 are Obvious Over Cheriton and Savage

1. Claim 7

Cheriton in view of Savage does not teach the limitation 7[B]

As set forth in V.D.1, Cheriton does not teach the limitation 7[B], Savage does not teach the limitation 7[B] in V.C.1, thus Cheriton and Savage does not teach the limitation 7[B], Cheriton in view of Savage does not render claim 7 obvious.

2. Claim 8

As set forth in V.D.2, Cheriton does not teach the limitations 8[C], 8[D] and 8[E].

Savage describes a technique for tracing anonymous packet flooding attacks on the Internet back towards their source. Ex. 1008 at Abstract. Savage does not teach limiting transmission rate of routers, thus Savage does not teach the limitations 8[C], 8[D] and 8[E].

Cheriton in view of Savage does not teach limitations 8[C], 8[D] and 8[E], therefore, Cheriton in view of Savage does not render claim 8 obvious.

3. Claim 9

Claim 9 depends from claim 8, containing all limitations of claim 8, thus claim 9 is not obvious over Cheriton in view of Savage for at least the same reasons.

4. Claim 10

Similar to V.E.1, Cheriton in view of Savage does not teach element 10[B], Cheriton in view of Savage does not render claim 8 obvious.

5. Claim 11

As set forth in V.D.5, Cheriton does not teach the limitations 11[B] -11[E]. Savage describes a technique for tracing anonymous packet flooding attacks on the Internet back towards their source. Ex. 1008 at Abstract. Savage does not teach limiting transmission rate of routers, while limitations 11[B] -11[E] are relate to limitation of transmission rate of routers, thus Cheriton and Savage do not teach the limitations 11[B] -11[E], Cheriton in view of Savage does not render claim 11 obvious.

6. Claim 12

Claim 12 depends from claim 11, containing all limitations of claim 11, thus claim 12 is not obvious over Cheriton in view of Savage for at least the same reasons.

VI. CONCLUSION

For the foregoing reasons, Patent Owner respectfully requests that the Board deny institution of the Petition in its entirety.

Dated: June 19, 2023

Respectfully submitted,

RAMEY LLP

/Jacob B. Henry/
Registration No.: 61,093
5020 Montrose Blvd, Suite 800
Houston TX 77006
Telephone: (832) 454-1456
Fax: (832) 900-4941
jhenry@rameyfirm.com
uspto@rameyfirm.com

Attorneys for Patent Owner

CERTIFICATE OF WORD COUNT

Counsel for Patent Owner hereby certifies that the foregoing document -- not including material excluded under 37 C.F.R. 42.24(a)(1) -- contains 8,576 words as calculated using the word count function of Microsoft Word.

Dated: June 19, 2023

/Jacob B. Henry/
Jacob B. Henry

CERTIFICATE OF SERVICE

I hereby certify that on February 27, 2023, a true and correct copy of the foregoing document was served via email to the Petitioner by serving the correspondence email addresses of record as follows:

Lead Counsel Craig Tolliver Charhon Callahan Robson & Garza, PLLC 3333 Lee Parkway, Suite 460 Dallas, TX 75219 Email: ctolliver@ccrglaw.com	Back-Up Counsel John Heuton Charhon Callahan Robson & Garza, PLLC 3333 Lee Parkway, Suite 460 Dallas, TX 75219 Email: jheuton@ccrglaw.com
--	--

Dated: June 19, 2023

/Jacob B. Henry/
Jacob B. Henry