UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/014,746	05/03/2021	7523497	50348.65	9957

31718 7590 06/15/2022

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

EXAMINER	
LAROSE, COLIN M	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
06/15/2022	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE
SUITE 700
DALLAS, TX 75219

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/014,746* .

PATENT UNDER REEXAMINATION *7523497* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

PTOL-465 (Rev.07-04)

Ex Parte Reexamination Advisory Action ***Before the Filing of an Appeal Brief***	**Control No.** 90/014,746	**Patent Under Reexamination** 7523497	
	Examiner Colin LaRose	**Art Unit** 3992	**AIA (FITF) Status** No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

THE PROPOSED RESPONSE FILED 16 May 2022 FAILS TO OVERCOME ALL OF THE REJECTIONS IN THE FINAL REJECTION MAILED 16 March 2022.

1. ☑ Unless a timely appeal is filed, or other appropriate action by the patent owner is taken to overcome all of the outstanding rejection(s), this prosecution of the present *ex parte* reexamination proceeding WILL BE TERMINATED and a Notice of Intent to Issue *Ex Parte* Reexamination Certificate will be mailed in due course. Any finally rejected claims, or claims objected to, will be CANCELLED.
   THE PERIOD FOR RESPONSE IS EXTENDED TO RUN 5 MONTHS FROM THE MAILING DATE OF THE FINAL REJECTION.
   Extensions of time are governed by 37 CFR 1.550(c).

NOTICE OF APPEAL

2. ☐ An Appeal Brief is due two months from the date of the Notice of Appeal filed on _____ to avoid dismissal of the appeal. See 37 CFR 41.37(a). Extensions of time are governed by 37 CFR 1.550(c). See 37 CFR 41.37(e) .

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final action, but prior to the date of filing a brief, will not be entered because:
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the proceeding in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: _____ (See 37 CFR 1.116 and 41.33(a)).
4. ☐ Patent owner's proposed response filed _____ has overcome the following rejection(s): _____
5. ☐ The proposed new or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
6. ☐ For purposes of appeal, the proposed amendment(s) a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claim(s) would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) patentable and/or confirmed: _____
   Claim(s) objected to: _____
   Claim(s) rejected: _____
   Claim(s) not subject to reexamination: _____

AFFIDAVIT OR OTHER EVIDENCE

7. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____ .
8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because patent owner failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence fails to overcome all rejections under appeal and/or appellant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☑ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See attached explanation .
12. ☐ Note the attached Information Disclosure Statement(s), PTO/SB/08, Paper No(s) _____ .
13. ☐ Other: _____ .

/COLIN M LAROSE/ Primary Examiner, Art Unit 3992	/Nick Corsaro/ Primary Examiner, Art Unit 3992.	

cc: Requester (if third party requester)

EX PARTE REEXAMINATION – ADVISORY OFFICE ACTION

Continuation of Box 11:

Claim Construction

Patent Owner asserts that Functional Phrases #1-16 do not invoke § 112, sixth paragraph, because "sufficient structure exists in 'means' of Functional Phrases #1-16." See Patent Owner remarks dated 5/16/2022, at p 6.

Patent Owner also asserts that to the extent § 112, sixth paragraph, is applied to Functional Phrases #1-16, the specification of the '497 Patent allegedly discloses sufficient structure for executing the corresponding functions, in the form of algorithms. See id, at pp. 7-11.

These arguments were fully addressed in the Final Rejection on pp. 5-10, and they are not persuasive for the same reasons previously given – specifically, the specification of the '497 Patent does not disclose sufficient algorithms for executing the claimed functions.

Claim Rejections – Ground 1

Patent Owner's arguments regarding the rejections of claims 1, 4, 13, and 16 based on Maher have been considered. See id., at pp. 11-15. Specifically, Patent Owner argues that Maher does not anticipate the claims because the specification of the '497 Patent discloses specific algorithms for executing the claimed functions in claims 1, 4, 13, and 16. However, as previously indicated in the Final Rejection at pp. 5-10, the specification of the '497 Patent does not disclose sufficient algorithms for executing the claimed functions.

Furthermore, Patent Owner's arguments in relation to the classifying data packets "by path" limitation have been considered, but are not sufficient to overcome the previous rejections since the corresponding structures of the means-plus-function limitations are considered to be general-purpose computers or routers.

Claim Rejections – Ground 2

Patent Owner argues Maher does not disclose classifying data packets "by path," as claimed in claim 7. The Examiner's position on this issue was discussed on pp. 11-13 of the Final Rejection, and that position is maintained herein. Additionally, Patent Owner expressly recognizes that a "source" of transmitted data can be considered "a part of a path" (see 5/16/2022 Remarks, at p. 14). Accordingly, Maher's classification of data packets being based on the source of the packets is tantamount to being based on partial path information. This teaching corresponds to the claimed limitation of "classifying data packets … by path" because the claim does not require *complete* path information to be used in classifying the data packets.

Claim 7 does require "determining a path by which data packets arrive at a host … said path comprising all routers in said network via which said packets are routed to said computer." The claim then further recites, " classifying data packets received … by path." It should be noted that "by path" for the classifying clause does not necessarily refer to the "determined" path. If instead the claim recited "by the path" or "by said path," then the path recited in the classifying clause would unequivocally refer to the same path recited in the determining clause. Since the claim does not provide this direct correspondence between the "path" recited in the determining clause and the classifying clause, the classifying step is not required to be executed based on the

same path in the determining clause – in other words, it is not required that *complete* path information be utilized for the classifying step.

For these reasons, the previous rejections are maintained.

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.550(a)). Extensions of time in *ex parte* reexamination proceedings are provided for in 37 CFR 1.550(c). See MPEP § 2265.

All correspondence relating to this *ex parte* reexamination proceeding should be directed:

By Mail to: Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

By EFS: Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at

https://efs.uspto.gov/efile/myportal/efs-registered

Any inquiry concerning this communication should be directed to Colin LaRose at (571) 272-7423. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew J. Fischer can be reached at 571-272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/COLIN M LAROSE/
Primary Examiner, Art Unit 3992

Conferees:

/NICK CORSARO/
Primary Examiner, Art Unit 3992

/ANDREW J. FISCHER/
Supervisory Patent Reexamination Specialist, Art Unit 3992

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,746	7523497
	Certificate Date	Certificate Number

Requester Correspondence Address: ☐ Patent Owner ☑ Third Party
HAYNES AND BOONE, LLP IP SECTION 2323 VICTORY AVENUE SUITE 700 DALLAS, TX 75219

LITIGATION REVIEW ☑	CML (examiner initials)	04 May 2021 (date)
Case Name		Director Initials
PacSec3, LLC v. NETSCOUT Systems, Inc, 6:20-cv-00914, W.D. TX.		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	**NUMBER**
n/a	

/COLIN M LAROSE/ Primary Examiner, Art Unit 3992	

CERTIFICATE OF SERVICE

The undersigned certifies that copies of the following,

1) Patent Owner Statement Pursuant to 37 C.F.R.§ 1.530;

in their entirety were served on:

Raghav Bajaj
Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, TX 75219
raghav.bajaj@haynesboone.com

the attorney of record, in accordance with 37 C.F.R. § 1.510(b)(5), on the 16th day of May 2022.

Dated: May 16, 2022

William P. Ramey, III
Registration No.: 44,295

Electronic Acknowledgement Receipt

EFS ID:	45727101
Application Number:	90014746
International Application Number:	
Confirmation Number:	9957
Title of Invention:	PACKET FLOODING DEFENSE SYSTEM
First Named Inventor/Applicant Name:	7523497
Customer Number:	31718
Filer:	William Peterson Ramey/Theresa Evenbly
Filer Authorized By:	William Peterson Ramey
Attorney Docket Number:	50348.65
Receipt Date:	16-MAY-2022
Filing Date:	03-MAY-2021
Time Stamp:	19:50:16
Application Type:	Reexam (Patent Owner)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2022-05-16_ResponseFOA_20227-0009REEX00_FINAL.pdf	317262 9a6243c49fd926a6202334218ca321d78a703360	yes	24

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Reexam Response to Final Rejection	1	23
	Reexam Certificate of Service	24	24
Warnings:			
Information:			
	Total Files Size (in bytes):	317262	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Donald N. Cohen	Group Art Unit: 3992
Appl. No.: 10/841,064	Examiner: Larose, Colin M
Filed: May 7, 2004	Confirmation No: 9957
U.S. Patent No. 7,523,497 Issue Date: April 21, 2009	Atty. Dkt. No.: 20227.0009.REEX00
Reexamination Control No. 90/014,746	
Title: PACKET FLOODING DEFENSE SYSTEM	

Mail Stop "Ex Parte Reexam"
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted today via the Office electronic filing system (EFS-Web) in accordance with 37 CFR §1.8.

Date: May 16, 2022 Signature: /Theresa M. Evenbly/
Printed Name: Theresa M. Evenbly

RESPONSE TO FINAL OFFICE ACTION OF MARCH 16, 2022

Enclosed herewith is PacSec3 LLC's Response pursuant to 37 C.F.R § 1.111 and 1.550 to the Final Office Action filed of March 16, 2022.

I. STATUS OF THE CLAIMS

Claims 1-18 stand issued in U.S. Patent No. 7,523,497 of which claims 1, 4, 7, 10, 13 and 16 are subject to reexamination. Claims 2, 3, 5, 6, 8, 9, 11, 12, 14, 15, 17 and 18 are not subject to reexamination. Of those claims subject to reexamination, claims 1, 4, 7, 13 and 16 are rejected, claim 10 is confirmed patentable. The Patent Owner has not presently amended the claims.

II. OVERVIEW OF THE OFFICE ACTION

In the Final Office Action of March 16, 2022 ("FOA"), the Examiner rejects claims 1, 4, 7, 13 and 16 on the following grounds:

Ground 1: Claims 1, 4, 13 and 16 are rejected under 35 U.S.C.§ 102(e) as being anticipated by Maher (U.S. 7,058,974).

Ground 2: Claim 7 is rejected under 35 U.S.C.§ 103(a) as obvious over Maher (U.S. 7,058,974) in view of Savage ("Practical Network Support for IP Traceback").

Patent Owner disagrees with Examiner's assessment. Patent Owner respectfully traverses these grounds of rejection and requests entry of the present Response and Reconsideration of the rejection in view of the arguments presented herein.

III. SUMMARY OF THE '497 PATENT

U.S. Patent No. 7,523,497 ("the '497 Patent") is directed to a system to defend against and resist packet flooding Distributed Denial of Service (DDoS) attacks for a network. '497 Patent, 2: 6-14.

Previous commercial system exchanges rate request and rate response messages between data senders and receivers to allow the sender to adjust the data rate to avoid congestion and to control the data flow. But 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. '497 Patent, 1: 49-2:5

The system of the '497 Patent has a plurality of host computers, routers, communication lines and transmitted data packets. The system includes means for classifying data packets received at a host computer as are means for associating a maximum acceptable processing rate with each class of data packet received at the computer. Means are also provided for the computer to find information for packets it receives regarding the path by which the packets came to the computer. Thus, the computer can use the information to allocate the processing rate available for packets of each class in a desired way.

IV. Claim Construction

During reexamination ordered under 35 U.S.C. 304, claims are given the broadest reasonable interpretation consistent with the specification and limitations

in the specification are not read into the claims *(In re Yamamoto,* 740 F.2d 1569, 222 USPQ934 (Fed. Cir. 1984)). (Ex. 2001 at ¶17).

The Examiner states that the following limitations should be interpreted under pre-AIA 35 U.S.C.§ 112, sixth paragraph.

Functional Phrase #1 (claim 1): means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;

Functional Phrase #2 (claim 1): means for associating a maximum acceptable processing rate with each class of data packet received at said computer;

Functional Phrase #3 (claim 1): means for said computer to find information for packets it receives regarding the path by which said packets came to said 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;

Functional Phrase #4 (claim 1): means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate.

Functional Phrase #5 (claim 4): means for classifying data packets received at a router into wanted data packets and unwanted data packets;

Functional Phrase #6 (claim 4): means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

Functional Phrase #7 (claim 4): means for said router to find information for packets it receives regarding the path by which said packets came to 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;

Functional Phrase #8 (claim 4): means in said router for said router to use said information to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable transmission rate.

Functional Phrase #9 (claim 13): means for 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;

Functional Phrase #10 (claim 13): means for classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;

Functional Phrase #11 (claim 13): means for assigning a maximum acceptable processing rate to each class of data packet;

Functional Phrase #12 (claim 13): means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets.

Functional Phrase #13 (claim 16): means for a router to determine a path by which said packets came to said router via packet marks provided by routers leading to

said router; said path comprising all routers in said network via which said packets are routed to said computer;

Functional Phrase #14 (claim 16): means for classifying data packets received at said router into wanted data packets and unwanted data packets by path;

Functional Phrase #15 (claim 16): means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

Functional Phrase #16 (claim 16): means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate.

The Examiner further states Functional Phrase #1, Functional Phrase #2, Functional Phrase #3, Functional Phrase #4, Functional Phrase #9, Functional Phrase #10, Functional Phrase #11, and Functional Phrase #12 correspond to a computer, while Functional Phrase #5, Functional Phrase #6, Functional Phrase #7, Functional Phrase #8, Functional Phrase #13, Functional Phrase #14, Functional Phrase #15, and Functional Phrase #16 correspond to a router, since no special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent.

Sufficient structure exists when the claim language specifies the exact structure that performs the function in question without need to resort to other portions of the specification or extrinsic evidence for an adequate understanding of

the structure. *Altiris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1376, 65 USPQ2d 1865, 1874 (Fed. Cir. 2003).

Patent owner respectively submits that Functional Phrases #1-16 do not invoke pre-AIA 35 U.S.C.§ 112, sixth paragraph, since sufficient structure exists in "means" of Functional Phrases #1-16.

"means" in Functional Phrases #1-4, 9-12 correspond to host computers 18 in Figs.1-9. A host compute has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. The user interface, specialized software, network address, protocol stack of the host compute provides sufficient structure to perform the functions in Functional Phrases #1-4, 9-12. Therefore, "means" in Functional Phrases #1-4, 9-12 do not merely recite general computers having basic functions, but recite host computers having the ability to perform the functions in Functional Phrases #1-4, 9-12.

Similarly, "means" in Functional Phrases #5-8, 13-16 correspond to routers 22 in Figs.1-9. A router is a piece of electronic equipment that connects computer networks to each other, and sends information between networks, A router may have interfaces for different types of physical layer connections, such as copper cables, fiber optic, or wireless transmission. It can also support different network layer transmission standards. Each network interface is used to enable data packets to be forwarded from one transmission system to another. The hardware and

interfaces of the router provide sufficient structure to perform the functions in Functional Phrases #5-8, 13-16. Therefore, "means" in Functional Phrases #5-8, 13-16 do not merely recite general routers having basic functions, but recite routers having the ability to perform the functions in Functional Phrases #5-8, 13-16.

To the extent that pre-AIA 35 U.S.C.§ 112, sixth paragraph is applied to Functional Phrases #1-16, the specification of the '497 Patent discloses sufficient structure for executing the corresponding functions in Functional Phrases #1-16.

Construction of a means-plus-function limitation includes two steps. "First, the court must determine the claimed function. Second, the court must identify the corresponding structure in the written description of the patent that performs the function." *Applied Med. Res. Corp. v. U.S. Surgical Corp.,* 448 F.3d 1324, 1332 (Fed. Cir. 2006).

In a means-plus-function claim 'in which the disclosed structure is a computer, or microprocessor, programmed to carry out an algorithm, the disclosed structure is not the general purpose computer, but rather the special purpose computer programmed to perform the disclosed algorithm. *WMS Gaming, Inc. v. Int'l Game Tech.,* 184 F.3d 1339, 1349 (Fed. Cir. 1999).

The specification can express the algorithm "in any understandable terms including as a mathematical formula, in prose, or as a flow chart, or in any other

manner that provides sufficient structure." *Finisar Corp. v. DirecTV Grp., Inc.*,523 F.3d 1323, 1340 (Fed. Cir. 2008).

Regarding Functional Phrases #1, 5, 10,14, "means for classifying data packets received at a/said host computer/router into wanted data packets and unwanted data packets/by path". The '497 Patent specification clearly links the function to the description as follows:

Even if the traffic is not reduced, the distinction between "wanted" and "unwanted packets plays an important role in "reasonable' allocation. **For a site there are normally some packets (in fact, the great majority) that are expected in a very strong sense.** It is reasonable to process these at the highest possible rate. **All other packets are not exactly unwanted**, but the site is willing to process them at only a limited rate. A reasonable approach is to schedule these as described above (using the places from which they were forwarded) at a limited rate, and regard as "unwanted those that end up being significantly delayed (or discarded). '497 Patent, 3: 13-23.

Therefore, the '497 Patent specification discloses an algorithm to carry out the function "classifying data packets received at a/said host computer/router into wanted data packets and unwanted data packets/by path" in Functional Phrases #1, 5, 10,14.

Regarding Functional Phrases #2, 6, 11,15, "means for assigning / associating a maximum acceptable processing / transmission rate to each class of data packet", the '497 Patent specification clearly links the function to the description as follows:

The final step in the defense is that cooperating routers will **limit the rate** at which they forward packets to places that so request. This may not be essential in the allocation of service, but it is useful for limiting the bandwidth used by "unwanted packets. The rate-limiting request is to be made when a site detects a high rate of unwanted packets coming from one place. This helps the site because it no longer has to process as many unwanted packets. It helps the network by freeing some of the bandwidth for other use. '497 Patent, 3: 4-12.

Therefore, the '497 Patent specification discloses an algorithm to carry out the function "assigning / associating a maximum acceptable processing / transmission rate to each class of data packet" in Functional Phrases #2, 6, 11,15.

Regarding Functional Phrase #3, 7, 9, 13, "means for said computer/router to find information for packets it receives regarding the path by which said packets came to said computer/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", the '497 Patent specification clearly links the function to the description as follows:

Routers will supply data about the forwarding path of the packets that arrive at a site. The site can use this data to allocate service as described above among the packets that arrive. This would solve the problem of unfair service if the packets that arrived were a fair sample of those that were sent to the site. '497 Patent, 2: 54-59.

Therefore, the '497 Patent specification discloses an algorithm – **a process to be followed** – to carry out the function "finding information for packets it receives regarding the path by which said packets came to said computer/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" in Functional Phrases #3, 7, 9,13.

Regarding Functional Phrases #4, 8, 12, 16, "means in said computer/router for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate", the '497 Patent specification clearly links the function to the description as follows:

The final step in the defense is that cooperating routers will limit the rate at which they forward packets to places that so request. This may not be essential in the allocation of service, but it is useful for limiting the bandwidth used by "unwanted packets. The rate-limiting request is to be made when a site detects a high rate of unwanted packets coming from one place. This helps the site because it no

longer has to process as many unwanted packets. It helps the network by freeing some of the bandwidth for other use. '497 Patent, 3: 4-12.

Therefore, the '497 Patent specification discloses an algorithm to carry out the function "using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate" in Functional Phrases #4, 8, 12, 16.

Therefore, even if the Functional Phrases #1-16 should be interpreted under pre-AIA 35 U.S.C.§ 112, sixth paragraph, there were specific algorithms for executing the claimed function disclosed in the specification of the '497 Patent. "means" in Functional Phrases #1-16 should be considered to be computers/routers that have been specially programmed to execute the claimed functions, rather than general-purpose computers/routers.

V. CLAIM REJECTIONS

A. Ground 1: Maher Fails to anticipate Claims 1, 4, 13 and 16.

Under Ground 1, the Office action rejects Claims 1, 4, 13 and 16 under 35 U.S.C.§ 102(e) as being anticipated by Maher. Patent Owner respectfully submits that Maher fails to teach or suggest each and every limitation of Claims 1, 4, 13 and 16 and requests that the rejections of Claims 1, 4, 13 and 16 under Ground 1 be withdrawn.

Based on the interpretation under pre-AIA 35 U.S.C.§ 112, sixth paragraph, the Examiner states that the various means-plus-function terms in claims1,4, 13 and 16 should only to be construed as general-purpose computers/routers. Accordingly, claims 1 and 13 are interpreted as a packet flooding defense system that comprises one or more computers respectively; claims 4 and 16 are interpreted as a packet flooding defense system that comprises one or more computers respectively. Maher discloses a packet flooding system for a network comprising a plurality host computers and routers, thus, claims 1, 4, 13 and 16 are anticipated by Maher.

As set forth above, since the '497 Patent's specification discloses specific algorithms – **processes to be followed to solve a problem or carry out a task** – for executing the claimed function in claims 1,4, 13 and 16, "means" in claims 1,4, 13 and 16 should be considered to be computers/routers that have been specially programmed to execute the claimed functions, rather than general-purpose computers/routers. Accordingly, whether Maher discloses computers/routers that performs the algorithm disclosed in the specification of the '497 Patent', or the equivalent should be considered to determine whether claims 1,4, 13 and 16 would have been anticipated by Maher.

Regarding claims 1, and 4, Maher is directed to "a method and apparatus for preventing denial of service type attacks on data networks", the apparatus includes a traffic flow scanning engine 140 and a quality of service processor. Maher does

not disclose " to find information for packets it receives regarding the path by which said packets came to said computer/router via packet marks provided by routers leading to said host computer", not to mention "said path comprising all routers in said network via which said packets are routed to said computer" as required by claim 1.

The Examiner states that Maher teaches classifying data packets "by path" since the source of the packets is taken into consideration when classifying them. Page 7, *Ex Parte* Reexamination of U.S. 7,523,497-Non-final Office Action, Nov. 12, 2021. "Since the source of the packets is a **partial path information**". Page 6, *Id.*

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". 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"(page 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"(pages 35-36).

According to ordinary meaning, the term "path" is a **link** between two nodes 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 words of the claim 1 itself also recite "said path comprising all routers in said network via which said packets are routed to said computer".

Maher discloses that "the quality of service queues 132 also allow network apparatus 100 to manage network attacks such as denial of service (DoS) attacks. Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the contents contain valid network traffic between known sources and destinations. Traffic flows that have not been verified because they are from unknown Sources or because they are new unclassified flows can be assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic. Since most DoS attacks send either new session information, data from spoofed sources, or meaningless data, network apparatus 100 would assign those traffic flows to low quality traffic queues". Maher, 7:54-67.

The written description of Maher shows that Maher teaches classifying data packets "by source". Although "source" can be recognized as a part of a path, "source" does not include a link, "source" cannot be recognized as a path. Therefore, Maher does not teach " to find information for packets it receives regarding the path by which said packets came to said computer/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" as required by claims 1 and 4.

Similarly, Maher does not teach "to determine a path by which said packets came to [a host computer] /[said router] via packet marks provided by routers leading to said router; said path comprising all routers in said network via which said packets are routed to said computer" as required by claims 13 and 16.

Therefore, as a content scanning method for packet flood attacks, Maher does not disclose, anticipate claims 1, 4, 13 and 16 of the '497 Patent.

B. Ground 2: The combination of Maher and Savage fails to render obvious Claim 7.

The Final Office action rejects Claim 7 under 35 U.S.C.§ 103(a) as obvious over Maher in view of Savage. Patent Owner respectfully submits that neither Maher nor Savage, whether considered alone or in combination, teach or suggest each and every limitation of Claim 7, and requests that the rejections of Claim 7 be withdrawn.

Regarding the step "classifying data packets received at said host computer into wanted data packets and unwanted data packets by path", the Final Office Action states that "Classifying the packets based only on the source and destination information may comprise classifying based on incomplete path information. The claim, however, does not require complete path information. Rather, it merely requires classifying the packets "by path." By Patent Owner's and Narayanaswamy's

admissions, the source and destination addresses of a data packet comprise at least partial path information". Final Office Action, page 13.

The Final Office Action also states that "By explicitly reciting that the claimed path includes complete path information, i.e., all routers via which the packets are routed, the Patent Owner has implicitly recognized that the claimed term "path," per se, does not necessarily comprise complete path information. Rather, the claimed term "path" may comprise merely some of the path information, such as only the source and destination nodes, and a narrowing amendment was submitted to limit the claims to the complete path traversed by the packets". And Since claim 7 does not require such complete path information to be considered when classifying packets as wanted or unwanted, the broadest reasonable interpretation of "classifying data packets ... by path" includes a classification that is performed using partial path information, such as classifying packets using only source and destination information, as taught by Maher. Final Office Action, page 13.

The term "path" is defined 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" and "a packet starts in a host (the source), **passes through a series of routers**, and ends its journey in another host (the destination) (Ex. 2003, at 4.)

Claim 7 recites:

a method of providing packet flooding defense for a network comprises a plurality of host computers, routers, communication lines and transmitted data packets, said method comprising the steps of:

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;

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

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

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

The language of claim 7 defines path as "comprising all routers in said network via which said packets are routed to said computer." The specification also supports that "Routers will supply data about the forwarding **path** of the packets that arrive at a site". The '497 Patent, 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." The '497 Patent, 3:62-64.

The language of claim 7 and the specification of the '497 Patent illustrate that the path of claim 7 must include a link such as a series of routers, which means that "a path" must provide information about how the data packets come from source to destination.

Maher discloses sources and destinations, although "source" and "destination" can be recognized as a part of a path, "source" and "destination" do not include a link, "source" and "destination" cannot be recognized as a path. Because only "source" and "destination" does not provide any information about how the data packets come from source to destination.

The Final Office Action states "According to Patent Owner, "a path must include a link such as a series of routers or packets switches". It is unclear that this proffered interpretation of "path" comports with the broadest reasonable interpretation thereof since it appears to neglect the scenario in which a direct path between a source node and a destination node is taken. In such an instance, there might be no intervening routers or packet switches linking the two nodes, and if Patent Owner's interpretation of path requires routers and/or packet switches to define a path, there would evidently be no "path" therebetween (since the path does not "include ... a series of routers or packet switches")" Final Office Action, page 12.

Patent owner respectfully submits that packet flooding defense system is used to handling unwanted data transmission between local networks, not in a local network, routers or packets switches exist between local networks, the language of claim 7 shows that a path comprises all routers in said network via which said packets are routed to said computer, which means a path comprises at least one router. Even if the scenario in which a direct path between a source node and a destination node is taken, only “source” and “destination” information does not include information of “a path”, since only “source” and “destination” information does not tell how the data packets come from source to destination, that is, only “source” and “destination” information can not determine the data packets comes from the source node to destination node directly or through routers.

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. The '497 Patent, 2:6-9. The method is radically different from methods in use at the time and perhaps was ahead of its 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. The '497 Patent, 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. The '497 Patent, 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, Maher 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. Savage does not cure the deficiencies of Maher with respect to Claim

VII. UPDATE IN PARALLEL LITIGATION INVOLVING '564 PATENT

An updated table of litigation involving the '564 patent is provided below:

Case Heading	Number	Court	Filed	Status
PacSec3, LLC v. NETSCOUT Systems, Inc.	2:21-cv-12463	E.D. Mich.	Oct. 10, 2021	Pending
PacSec 3, LLC v Darktrace, PLC	6:22-cv-00126	W.D. Tex.	Feb. 4, 2022	Pending
PacSec 3, LLC v Crowdstrike Holdings, Inc.	6:22-cv-00127	W.D. Tex.	Feb. 4, 2022	Pending
PacSec 3, LLC v Blackberry Corporation	6:22-cv-00128	W.D. Tex.	Feb. 4, 2022	Pending
PacSec 3, LLC v Cloudflare, Inc.	6:22-cv-00129	W.D. Tex.	Feb. 4, 2022	Pending
PacSec3, LLC v Splunk, Inc.	2:22-cv-00056	E.D.Tex.	Feb. 18, 2022	Pending
PacSec 3, LLC v Imperva, Inc.	6:22-cv-00167	W.D. Tex	Feb. 17, 2022	Pending

Case Heading	Number	Court	Filed	Status
PacSec 3, LLC v Rapid7, Inc.	6:22-cv-00168	W.D. Tex	Feb. 17, 2022	Pending
PacSec 3, LLC v Forescout Technologies, Inc.	2:22-cv-00055	E.D. Tex	Feb. 17, 2022	Pending
PacSec3, LLC v. McAfee, LLC	2:21-cv-00140	E.D. Tex.	April 21, 2021	Dismissed
PacSec3, LLC v. Fortinet, Inc.	2:21-cv-00450	E.D. Tex.	Dec. 13, 2021	Dismissed with Prejudice
PacSec3, LLC v. F5 Networks, Inc.	2:20-cv-00697	D. Utah	Oct 2, 2020	Terminated
PacSec3, LLC v. F5 Networks, Inc.	2:20-cv-01828	W.D. Wash.	Dec. 14, 2020	Terminated
PacSec3. LLC v. NETSCOUTS, Inc.	6:20-CV-00914	W.D. Tex.	Oct. 2, 2020	Terminated
PacSec3, LLC v. Palo Alto Networks, Inc.,	2:2 l-cv-00141	E.D. Tex.	Oct. 2, 2020	Terminated
PacSec3, LLC v. Cisco Systems, Inc.	6:21-cv-00388	W.D. Tex.	Apr. 21, 2021	Terminated
PacSec3, LLC v. Juniper Networks, Inc.	6:21-cv-00387	W.D. Tex.	Apr. 21, 2021	Terminated
PacSec3, LLC v. Watchguard Technologies, Inc.	6:21-cv-00633	W.D. Tex	June 18, 2021	Terminated
PacSec3, LLC v. Juniper Networks, Inc.	2:21-cv-00228	E.D. Tex	June 23, 2021	Terminated
PacSec3, LLC v. Juniper Networks, Inc.	*5:21-cv-07812*	*N.D. Cal.*	Oct. 21, 2021	Terminated

VIII. CONCLUSION

Therefore, the Examiner should find Claims 1, 4, 7, 13 and 16 are patentable over the prior art.

Ramey & Schwaller, LLP
5020 Montrose Blvd., Ste. 800
Houston, Texas 77006
(713) 426-3923 (telephone)

Respectfully submitted,
/William P. Ramey III/
William P. Ramey, III
Reg. No.: 44,295
Attorney for Applicant

Notice of References Cited	Application/Control No. 90/014,746	Applicant(s)/Patent Under Reexamination 7523497	
	Examiner Colin LaRose	Art Unit 3992	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
	A					
	B					
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
*	U	Peterson, Larry L., et al. Computer Networks: A Systems Approach, Third Edition. Morgan Kaufmann Publishers, 2003, pp. 239-242 .
*	V	Microsoft Computer Dictionary, Fifth Edition. Microsoft Press, 2002, p. 394.
*	W	Kurose, James F., et al. Computer Networking: A Top-Down Approach, Sixth Edition. Addison-Wesley, 2013, pp. 2-5 and 34-36.
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,746	7523497
	Certificate Date	Certificate Number

Requester Correspondence Address: ☐ Patent Owner ☑ Third Party
HAYNES AND BOONE, LLP IP SECTION 2323 VICTORY AVENUE SUITE 700 DALLAS, TX 75219

LITIGATION REVIEW ☑	CML (examiner initials)	04 May 2021 (date)
Case Name		Director Initials
PacSec3, LLC v. NETSCOUT Systems, Inc, 6:20-cv-00914, W.D. TX.		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	**NUMBER**
n/a	

/COLIN M LAROSE/ Primary Examiner, Art Unit 3992	

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/014,746	05/03/2021	7523497	50348.65	9957

31718 7590 03/16/2022

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

EXAMINER	
LAROSE, COLIN M	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
03/16/2022	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE
SUITE 700
DALLAS, TX 75219

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/014,746* .

PATENT UNDER REEXAMINATION *7523497* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

PTOL-465 (Rev.07-04)

FINAL REJECTION (REEXAMINATION OF U.S. PATENT 7,523,497)

TABLE OF CONTENTS

I. ACKNOWLEDGEMENTS 2
II. STATUS OF CLAIMS 3
III. PRIORITY AND AIA STATUS 4
IV. PRIOR ART CITED HEREIN 4
V. RESPONSE TO PATENT OWNER'S ARGUMENTS 5
VI. INFORMATION CONSIDERED 14
VII. CLAIM INTERPRETATION – PHRASES INVOKING 35 U.S.C. § 112, SIXTH PARAGRAPH 14
VIII. CLAIM REJECTIONS – 35 USC § 102 (ANTICIPATION) 26
IX. CLAIM REJECTIONS – 35 USC § 103 (OBVIOUSNESS) 28
X. CONFIRMED PATENTABLE CLAIM 31
XI. CONCLUSION 35

I. ACKNOWLEDGEMENTS

This final Office action addresses *ex parte* reexamination control no. 90/014,746 ("Instant Proceeding"). The Instant Proceeding is an *ex parte* reexamination of U.S. Patent No. 7,523,497 ("Patent Under Reexamination" or "'497 Patent") titled "PACKET FLOODING DEFENSE SYSTEM." The Patent Under Reexamination was filed on May 7, 2004 ("Non-Provisional Filing Date"), and assigned by the Office non-provisional U.S. patent application control number 10/841,064 ("Non-Provisional Application"), and issued on April 21, 2009, with claims 1-18 ("Originally Patented Claims").

On May 3, 2021, a third-party request to reexamine claims 1, 4, 7, 10, 13, and 16 was submitted ("Request").

On June 17, 2021, an order granting the request to reexamine the '497 Patent was issued in response to the Request ("Order").

On August 17, 2021, Patent Owner submitted an optional statement in response to the Order ("Patent's Owner Statement").

On October 15, 2021, Requester submitted a response to the Patent Owner's Statement ("Requester's Reply").

On November 12, 2021, a non-final Office action was issued ("Nov 2021 Non-Final Rejection").

On January 12, 2022, Patent Owner submitted a response to the Nov 2021 Non-Final Rejection ("Jan 2022 Response").

This final Office action addresses Patent Owner's Jan 2022 Response.

II. STATUS OF CLAIMS

Claims 1-18 are currently pending ("Pending Claims").

Claims 1, 4, 7, 10, 13, and 16 are currently examined ("Examined Claims").

Claims 2, 3, 5, 6, 8, 9, 11, 12, 14, 15, 17, and 18 are withdrawn from consideration.

Regarding the Examined Claims and as a result of this Office action:

Claims 1, 4, 13, and 16 are rejected under 35 U.S.C. § 102.

Claim 7 is rejected under 35 U.S.C. § 103.

Claim 10 is confirmed patentable.

III. PRIORITY AND AIA STATUS

Domestic Priority. Based upon a review of the '497 Patent, the Examiner finds that there is a claim for benefit of domestic priority under 35 U.S.C. §§ 120 or 119(e) to parent application control no. 09/715,813 ("Parent Application"). To the extent the disclosure of the Parent Application supports the Pending Claims under 35 U.S.C. § 112, the supported claims receive benefit of an effective date of November 16, 2000, which is the filing date of the Parent Application.

AIA Status. Because the '497 Patent does not contain a claim having an effective date on or after March 16, 2013, the America Invents Act First Inventor to File ("AIA-FITF") provisions do not apply. Instead, the pre-AIA "First to Invent" provisions will govern this proceeding. See 35 U.S.C. § 100 (note). In the event the determination of the status of the application as subject to pre-AIA 35 U.S.C. §§ 102 and 103 is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

IV. PRIOR ART CITED HEREIN

The following prior art patents and printed publications are cited herein:

U.S. Patent 6,725,378 ("Schuba");

U.S. Patent 7,058,974 ("Maher"); and

"Practical Network Support for IP Traceback" ("Savage").

V. RESPONSE TO PATENT OWNER'S ARGUMENTS

Claim Construction

(see Jan 2022 Response at pp. 2-11)

Patent Owner asserts that Functional Phrases #1-16 do not invoke § 112, sixth paragraph, because the phrases each recite sufficient structure. This argument is unpersuasive inasmuch as the claimed term "means" is well-recognized as a placeholder for structure, rather than actual structure. The recitation of "means" plus functional language raises a rebuttable presumption that the means-plus-function phrase invokes § 112, sixth paragraph. The presumption can be overcome when the limitation further includes the structure necessary to perform the recited function. See MPEP § 2181(I).

In this instance, each of the Functional Phrases #1-16 recite "means" without further reciting any additional modifiers or limitations that would indicate the recited means corresponds to sufficient structure for performing the claimed functions, without resorting to other portions of the specification or extrinsic evidence for an adequate understanding of the structure. Accordingly, the presumption that Functional Phrases #1-16 invoke § 112, sixth paragraph, is not overcome.

Patent Owner additionally asserts that, even if § 112, sixth paragraph, is invoked for each of the Functional Phrases, the specification discloses sufficient structure in the form of algorithms for performing the entirety of the claimed functions, such that the disclosed algorithms transform a general-purpose computing device into a specially-programmed computing device. This argument is also unpersuasive for the following reasons.

Functional Phrases #1, 5, 10, and 14 recite, "means for classifying data packets received at a/said computer/router into wanted data packets and unwanted data packets/by path."

Patent Owner identifies the corresponding algorithm for these Functional Phrases as being disclosed at column 3:13-23 of the Patent Under Reexamination:

> Even if the traffic is not reduced, the distinction between "wanted" and "unwanted" packets plays an important role in "reasonable" allocation. For a site there are normally some packets (in fact, the great majority) that are expected in a very strong sense. It is reasonable to process these at the highest possible rate. All other packets are not exactly unwanted, but the site is willing to process them at only a limited rate. A reasonable approach is to schedule these as described above (using the places from which they were forwarded) at a limited rate, and regard as "unwanted" those that end up being significantly delayed (or discarded).

This passage does not disclose an algorithm for classifying packets into wanted and unwanted packets. That is, it does not describe in any definite and understandable terms (such as a mathematical formula, prose, a flow chart, pseudo code, etc.) how to categorize packets into "wanted" and "unwanted" classifications. At best, the passage recognizes that wanted and unwanted packets should be distinguished and processed at different rates. In addition, the remainder of the specification has been reviewed, and an algorithm that corresponds to the claimed function does not appear to be disclosed elsewhere.

Accordingly, the Patent Under Reexamination does not appear to disclose a sufficient algorithm for performing the entire claimed function, and for the purposes of interpreting these Functional Phrases under § 112, sixth paragraph, for the instant *ex parte* reexamination it is presumed that a general-purpose computing device such as a computer or router represents the corresponding structure.

Functional Phrases #2, 6, 11, and 15 recite, "means for assigning/associating a maximum acceptable processing/transmission rate to each class of data packet."

Patent Owner identifies the corresponding algorithm for these Functional Phrases as being disclosed at column 3:4-12 of the Patent Under Reexamination:

> The final step in the defense is that cooperating routers will limit the rate at which they forward packets to places that so request. This may not be essential in the allocation of service, but it is useful for limiting the bandwidth used by "unwanted" packets. The rate-limiting request is to be made when a site detects a high rate of unwanted packets coming from one place. This helps the site because it no longer has to process as many unwanted packets. It helps the network by freeing some of the bandwidth for other use.

This passage does not disclose an algorithm for assigning or associating a maximum acceptable processing or transmission rate to each class of data packet. That is, it does not describe in any definite and understandable terms (such as a mathematical formula, prose, a flow chart, pseudo code, etc.) how to assign or associate a maximum acceptable processing or transmission rate to each class of data packet. The passage makes no mention of maximum acceptable rates or how to associate such rates with different classes of data packets. At best, the passage recognizes unwanted packets are preferably rate-limited. In addition, the remainder of the specification has been reviewed, and an algorithm that corresponds to the claimed function does not appear to be disclosed elsewhere.

Accordingly, the Patent Under Reexamination does not appear to disclose a sufficient algorithm for performing the entire claimed function, and for the purposes of interpreting these Functional Phrases under § 112, sixth paragraph, for the instant *ex parte* reexamination it is presumed that a general-purpose computing device such as a computer or router represents the corresponding structure.

Functional Phrases #3, 7, 9, and 13 recite, "means for said computer/router to find information for packets it receives regarding the path by which said packets came to said computer/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."

Patent Owner identifies the corresponding algorithm for these Functional Phrases as being disclosed at column 2:54-59 of the Patent Under Reexamination.

> Routers will supply data about the forwarding path of the packets that arrive at a site. The site can use this data to allocate service as described above among the packets that arrive. This would solve the problem of unfair service if the packets that arrived were a fair sample of those that were sent to the site.

This passage does not disclose an algorithm for finding information for packets received regarding the path by which said packets came to said computer/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. That is, it does not describe in any definite and understandable terms (such as a mathematical formula, prose, a flow chart, pseudo code, etc.) how to find the path that packets traverse using packet marks provided by routers. The passage makes no mention of packets marks, how to find information about complete paths of data packets, or what information is to be found. At best, the passage teaches that routers can supply data about forwarding paths of packets, and the data can be used to allocate service. In addition, the remainder of the specification has been reviewed, and an algorithm that corresponds to the claimed function does not appear to be disclosed elsewhere.

Accordingly, the Patent Under Reexamination does not appear to disclose a sufficient algorithm for performing the entire claimed function, and for the purposes of interpreting these Functional Phrases under § 112, sixth paragraph, for the instant *ex parte* reexamination it is

presumed that a general-purpose computing device such as a computer or router represents the corresponding structure.

Functional Phrases #4, 8, 12, and 16 recite, "means in said computer/router for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate."

Patent Owner identifies the corresponding algorithm for these Functional Phrases as being disclosed at column 3:4-12 of the Patent Under Reexamination.

> The final step in the defense is that cooperating routers will limit the rate at which they forward packets to places that so request. This may not be essential in the allocation of service, but it is useful for limiting the bandwidth used by "unwanted" packets. The rate-limiting request is to be made when a site detects a high rate of unwanted packets coming from one place. This helps the site because it no longer has to process as many unwanted packets. It helps the network by freeing some of the bandwidth for other use.

This passage does not disclose an algorithm for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate. That is, it does not describe in any definite and understandable terms (such as a mathematical formula, prose, a flow chart, pseudo code, etc.) how to use the found information to allocate processing rates for unwanted data packets. The passage makes no mention of the found information pertaining to the paths of data packets or how to use such information for limiting the processing rate of unwanted packets. At best, the passage recognizes unwanted packets are preferably rate-limited. In addition, the remainder of the specification has been reviewed, and an algorithm that corresponds to the claimed function does not appear to be disclosed elsewhere.

Accordingly, the Patent Under Reexamination does not appear to disclose a sufficient algorithm for performing the entire claimed function, and for the purposes of interpreting these Functional Phrases under § 112, sixth paragraph, for the instant *ex parte* reexamination it is presumed that a general-purpose computing device such as a computer or router represents the corresponding structure.

Furthermore, it is noted that each of the above passages identified by the Patent Owner appear in the "Background of the Invention" section of the Patent Under Reexamination. It is unclear how the passages correspond to the claimed invention because it appears they merely provide background information and technological context for the description of the invention that follows. No further elaboration on the putative algorithms contained in these passages appears in any other portion of the Patent Under Reexamination, including the summary of the invention, detailed description of the invention, drawings, and description of the drawings.

For the above reasons, the previous interpretations of Functional Phrases 1-16 are maintained herein.

Claim Rejections – Ground #1
(see Jan 2022 Response at pp. 11-15)

For Ground #1, claims 1, 4, 13, and 16 were rejected under 35 U.S.C. § 102 as being anticipated by Maher. This rejection was based on the above § 112, sixth paragraph, interpretation of the claims in which the corresponding structure for each of the claimed

Functional Phrases #1-16 was identified as either a computer or a router. See also Section +++, *infra*.

On p. 12 of the Jan 2022 Response, Patent Owner asserts that the specification of the Patent Under Reexamination "discloses specific algorithms for executing the claimed function[s] in claims 1, 4, 13, and 16," and therefore, each means-plus-function limitation should be considered a specially-programmed computer or router, rather than a general-purpose computer or router.

This argument is unpersuasive since, as explained above, the specification does not appear to disclose sufficient algorithms for any of the Functional Phrases #1-16. Since the corresponding structure of a specially-programmed computer or router (in the form of an algorithm) cannot be determined from the specification, for purposes of reexamination it is presumed that a general-purpose computer or router corresponds to each of the recited "means."

Patent Owner does not dispute that Maher discloses a packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system comprising one or more computers and/or one or more routers. Accordingly, the previous rejections of claims 1, 4, 13, and 16 are maintained.

Claim Rejections – Ground #2
(see Jan 2022 Response at pp. 15-21)

For Ground #2, claim 7 was rejected under 35 U.S.C. § 103 as being obvious over the combination of Maher and Savage. Patent Owner argues the rejection is improper because Maher does not teach "classifying data packets received at said host computer into wanted data packets and unwanted data packets ***by path***" (***emphasis added***). Specifically, Patent Owner argues that Maher, at best, teaches that packets can be classified into wanted or unwanted based on whether

the packets are transmitted between known sources and destinations, and although the source and destination information may be known, the Maher system has no ability to determine paths the packets travel.

According to Patent Owner, "a path must include a link such as a series of routers or packets switches" (see Jan 2022 Response at p. 18). It is unclear that this proffered interpretation of "path" comports with the broadest reasonable interpretation thereof since it appears to neglect the scenario in which a *direct* path between a source node and a destination node is taken. In such an instance, there might be no intervening routers or packet switches linking the two nodes, and if Patent Owner's interpretation of path requires routers and/or packet switches to define a path, there would evidently be no "path" therebetween (since the path does not "include . . . a series of routers or packet switches"). Alternatively, Patent Owner's proffered interpretation *would* encompass a direct path between a source node and a destination node because there would necessarily be a link between the two nodes so that data can flow between them. Such a direct link would not include "a series of routers or packet switches," but Patent Owner's definition does not seemingly require the link to include routers and/or packet switches since the "such as" language is suggestive and merely provides examples of the types of links that can correspond to a path.

Nonetheless, Patent Owner (as well as the Narayanaswamy declaration – Exhibit 3001 at ¶ 61) readily admits that a source node and a destination node "can be recognized as part of a path" (*see id.*). Accordingly, the classifying of received data packets into wanted data packets and unwanted data packets using source and destination information corresponds to classifying the packets "by path," as claimed, even if the path information is not the complete path information.

Classifying the packets based only on the source and destination information may comprise classifying based on incomplete path information. The claim, however, does not require ***complete*** path information. Rather, it merely requires classifying the packets "by path." By Patent Owner's and Narayanaswamy's admissions, the source and destination addresses of a data packet comprise at least partial path information.

Furthermore, during the initial prosecution of the Patent Under Reexamination, the claims were narrowed to specify that the claimed path comprises "all routers in said network via which said packets are routed to said computer." See 10/16/2008 claim amendments in the Non-Provisional Application 10/841,064. By explicitly reciting that the claimed path includes complete path information, i.e., all routers via which the packets are routed, the Patent Owner has implicitly recognized that the claimed term "path," *per se*, does not necessarily comprise complete path information. Rather, the claimed term "path" may comprise merely some of the path information, such as only the source and destination nodes, and a narrowing amendment was submitted to limit the claims to the complete path traversed by the packets.

Since claim 7 does not require such complete path information to be considered when classifying packets as wanted or unwanted, the broadest reasonable interpretation of "classifying data packets . . . by path" includes a classification that is performed using partial path information, such as classifying packets using only source and destination information, as taught by Maher.

For these reasons, the previous § 103 rejection of claim 7 is maintained.

VI. INFORMATION CONSIDERED

On January 12, 2022, Patent Owner submitted a declaration by Swamy Narayanaswamy (Exhibit 3001). This declaration has been made of record and considered.

Patent Owner has also submitted excerpts from three non-patent prior art references:

(1) Microsoft Computer Dictionary (Exhibit 3002);

(2) Computer Networking: A Top-Down Approach (Exhibit 3003); and

(3) Computer Networks: A System Approach (Exhibit 3004).

These three documents have been considered and are listed on the attached PTO-892.

VII. CLAIM INTERPRETATION – PHRASES INVOKING 35 U.S.C. § 112, SIXTH PARAGRAPH

The following is a quotation of pre-AIA 35 U.S.C. 112, sixth paragraph:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

As explained in MPEP § 2181, subsection I, claim limitations that meet the following three-prong test will be interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph:

(A) the claim limitation uses the term "means" or a term used as a substitute for "means" that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning) for performing the claimed function;

(B) the term "means" or the generic placeholder is modified by functional language, typically, but not always linked by the transition word "for" (e.g., "means for") or another linking word or phrase, such as "configured to" or "so that"; and

(C) the term "means" or the generic placeholder is not modified by sufficient structure for performing the claimed function.

Use of the word "means" in a claim with functional language creates a rebuttable presumption that the claim limitation is to be treated in accordance with pre-AIA 35 U.S.C. § 112, sixth paragraph. The presumption that the claim limitation is interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph, is rebutted when the claim limitation recites sufficient structure to entirely perform the recited function.

Claim limitations in this application that use the word "means" are being interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph, except as otherwise indicated in an Office action. Conversely, claim limitations in this application that do not use the word "means" are not being interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph, except as otherwise indicated in an Office action.

Such claim limitations that invoke § 112, sixth paragraph are:

Functional Phrase #1 (claim 1) – means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;

Functional Phrase #2 (claim 1) – means for associating a maximum acceptable processing rate with each class of data packet received at said computer;

Functional Phrase #3 (claim 1) – means for said computer to find information for packets it receives regarding the path by which said packets came to said 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; and

Functional Phrase #4 (claim 1) – means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate.

Functional Phrase #5 (claim 4) – means for classifying data packets received at a router into wanted data packets and unwanted data packets;

Functional Phrase #6 (claim 4) – means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

Functional Phrase #7 (claim 4) – means for said router to find information for packets it receives regarding the path by which said packets came to 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; and

Functional Phrase #8 (claim 4) – means in said router for said router to use said information to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable transmission rate.

Functional Phrase #9 (claim 13) – means for 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;

Functional Phrase #10 (claim 13) – means for classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;

Functional Phrase #11 (claim 13) – means for assigning a maximum acceptable processing rate to each class of data packet; and

Functional Phrase #12 (claim 13) – means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets.

Functional Phrase #13 (claim 16) – means for a router to determine a path by which said packets came to said router via packet marks provided by routers leading to said router; said path comprising all routers in said network via which said packets are routed to said computer;

Functional Phrase #14 (claim 16) – means for classifying data packets received at said router into wanted data packets and unwanted data packets by path;

Functional Phrase #15 (claim 16) – means for associating a maximum acceptable transmission rate with each class of data packet received at said router; and

Functional Phrase #16 (claim 16) – means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate.

Because these claim limitations are being interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph, they are being interpreted to cover the corresponding structure described in the specification as performing the claimed function, and equivalents thereof.

If Applicant does not intend to have any of these limitations interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph, Applicant may:

(1) amend the claim limitation(s) to avoid it/them being interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph (e.g., by reciting sufficient structure to perform the claimed function); or

(2) present a sufficient showing that the claim limitations recite sufficient structure to perform the claimed functions so as to avoid them being interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph.

Based upon a review of the '497 Patent, the Examiner concludes that the corresponding structures for the above-identified Functional Phrases are disclosed in the '497 Patent as follows:

Functional Phrase #1 (claim 1) – means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system includes means for classifying data packets 30 received at a host computer 18.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #2 (claim 1) – means for associating a maximum acceptable processing rate with each class of data packet received at said computer;

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system of FIG. 1 includes means for associating a maximum acceptable processing rate 34 with each class 38 of data packet 30 received at the computer 18.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #3 (claim 1) – means for said computer to find information for packets it receives regarding the path by which said packets came to said 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; and

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system of FIG. 1 includes means 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.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #4 (claim 1) – means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate.

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system of FIG. 1 includes a computer 18 that 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.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #5 (claim 4) – means for classifying data packets received at a router into wanted data packets and unwanted data packets;

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes means for classifying data packets 30 received at a router 22.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #6 (claim 4) – means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes means for associating a maximum acceptable processing rate 74 with each class 38 of data packet 30 received at the router 22.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #7 (claim 4) – means for said router to find information for packets it receives regarding the path by which said packets came to 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; and

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes means for the router 22 to find information for packets 30 it receives regarding the path 50 by which the packets 30 came to the router 22.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #8 (claim 4) – means in said router for said router to use said information to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable transmission rate.

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes a router 22 that can use the information to allocate the processing rate for each class 38 in a desired way.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #9 (claim 13) – means for 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;

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system of FIG. 1 includes means 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.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #10 (claim 13) – means for classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system includes means for classifying data packets 30 received at a host computer 18.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #11 (claim 13) – means for assigning a maximum acceptable processing rate to each class of data packet; and

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system of FIG. 1 includes means for associating a maximum acceptable processing rate 34 with each class 38 of data packet 30 received at the computer 18.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #12 (claim 13) – means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets.

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system of FIG. 1 includes a computer 18 that 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.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #13 (claim 16) – means for a router to determine a path by which said packets came to said router via packet marks provided by routers leading to said router; said path comprising all routers in said network via which said packets are routed to said computer;

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes means for the router 22 to find information for packets 30 it receives regarding the path 50 by which the packets 30 came to the router 22.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #14 (claim 16) – means for classifying data packets received at said router into wanted data packets and unwanted data packets by path;

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes means for classifying data packets 30 received at a router 22.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #15 (claim 16) – means for associating a maximum acceptable transmission rate with each class of data packet received at said router; and

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes means for associating a maximum acceptable processing rate 74 with each class 38 of data packet 30 received at the router 22.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #16 (claim 16) – means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate.

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes a router 22 that can use the information to allocate the processing rate for each class 38 in a desired way.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

If Applicant wishes to provide further explanation or dispute the Examiner's interpretation of the corresponding structure, Applicant must identify the corresponding structure with reference to the specification by page and line number, and to the drawing, if any, by reference characters in response to this Office action.

VIII. CLAIM REJECTIONS – 35 USC § 102 (ANTICIPATION)

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 4, 13, and 16 are rejected under 35 U.S.C. § 102(e) as being anticipated by Maher (U.S. 7,058,974).

Regarding **claim 1**, Maher discloses a packet flooding defense system (FIGS. 1a and 1b) for a network comprising a plurality of host computers (30), routers (22), communication lines (60) and transmitted data packets (*e.g.*, IP data), said system comprising:

one or more computers (30).

Note that the means-plus-function limitations of claim 1 have been interpreted in accordance with 35 U.S.C. § 112, sixth paragraph. As indicated above in Section VII, the corresponding structure for each of the means-plus-function limitations of claim 1 is a computer. Accordingly, claim 1 is interpreted as a packet flooding defense system that comprises one or more computers.

Regarding **claim 4**, Maher discloses a packet flooding defense system (FIGS. 1a and 1b) for a network comprising a plurality of host computers (30), routers (22), communication lines (60) and transmitted data packets (*e.g.*, IP data), said system comprising:

one or more routers (22).

Note that the means-plus-function limitations of claim 4 have been interpreted in accordance with 35 U.S.C. § 112, sixth paragraph. As indicated above in Section VII, the corresponding structure for each of the means-plus-function limitations of claim 4 is a router. Accordingly, claim 4 is interpreted as a packet flooding defense system that comprises one or more routers.

Regarding **claim 13**, Maher discloses a packet flooding defense system (FIGS. 1a and 1b) for a network comprising a plurality of host computers (30), routers (22), communication lines (60) and transmitted data packets (*e.g.*, IP data), said system comprising:

one or more computers (30).

Note that the means-plus-function limitations of claim 13 have been interpreted in accordance with 35 U.S.C. § 112, sixth paragraph. As indicated above in Section VII, the corresponding structure for each of the means-plus-function limitations of claim 13 is a computer. Accordingly, claim 13 is interpreted as a packet flooding defense system that comprises one or more computers.

Regarding **claim 16**, Maher discloses a packet flooding defense system (FIGS. 1a and 1b) for a network comprising a plurality of host computers (30), routers (22), communication lines (60) and transmitted data packets (*e.g.*, IP data), said system comprising:

one or more routers (22).

Note that the means-plus-function limitations of claim 16 have been interpreted in accordance with 35 U.S.C. § 112, sixth paragraph. As indicated above in Section VII, the corresponding structure for each of the means-plus-function limitations of claim 16 is a router. Accordingly, claim 16 is interpreted as a packet flooding defense system that comprises one or more routers.

IX. CLAIM REJECTIONS – 35 USC § 103 (OBVIOUSNESS)

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 7 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Maher (U.S. 7,058,974) in view of Savage ("Practical Network Support for IP Traceback").

Regarding **claim 7**, Maher discloses a method (FIG. 5) of providing packet flooding defense for a network (*see*, *e.g.*, FIGS. 1a and 1b) comprising a plurality of host computers (*i.e.*, webfarm 16 includes one or more network apparatuses, illustrated in FIGS. 2 and 4, performing host computing functions), routers (22), communication lines and transmitted data packets, said method comprising the steps of:

classifying data packets received at said host computer into wanted data packets and unwanted data packets by path (step 514; see also columns 7:54–8:3 – data packets received by a network apparatus (FIG. 2 or FIG. 4) are classified into valid ("wanted") and unverified ("unwanted") categories based on whether the packets are transmitted between known sources and destinations, *i.e.*, via a known path; the packets are considered "wanted" or "unwanted" to the extent that is it desirable or favorable for packets to flow between known sources and destinations, and it is undesirable or unfavorable for packets to flow from unverified sources);

associating a maximum acceptable processing rate with each class of data packet received at said host computer (*see* columns 7:54–8:3 and column 11:66–12:19 – the "wanted" class of packets is given a high priority processing rate, i.e., "quality of service," whereas the "unwanted" class of packets is given a low priority processing rate); and

allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets (*see id.* – unwanted packets are given a lower processing rate than wanted packets).

Maher does not appear to expressly disclose the method includes:

"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," as claimed.

Savage discloses methods for combatting denial-of-service attacks that involve anonymous packet flooding (*see* Abstract). Savage teaches that is it conventional to employ "ingress filtering" in order to defend against anonymous attacks (*see* Section 2.1). Ingress filtering involves configuring routers to block packets that arrive with illegitimate source addresses (*see id.*). This is a similar prevention technique that is employed by Maher, which as explained above, teaches giving higher priority to traffic originating from verified sources, and giving lower priority to traffic from unverified sources.

Savage, however, identifies problems with ingress filtering. Notably, as traffic is aggregated from multiple ISPs into transmit networks, there is no longer enough information to unambiguously determine if an arriving packet originates from a valid, known source. Also, since its effectiveness depends on widespread, if not universal, deployment, the overhead of ingress filtering can become prohibitive on high-speed links, and even if universally deployed, attackers could still circumvent the filtering by forging addresses within a valid customer network. *See id.*

With these problems in mind, Savage proposes tracing flooding attacks by marking packets, either probabilistically or deterministically, with the addresses of the routers they traverse (*see* Section 3). For instance, a packet can be marked by appending the address of each node it traverses so that every received packet has a complete ordered list of the routers it traversed; this provides a complete path of the packet through a network and allows the receiver

of the packet to trace the entire path back to its origin (*see* Section 4.1). Alternatively, probabilistic marking of only one node address can allow reconstruction of a complete traffic path from a given source when enough packets have been received (*see* Section 4.2).

It would have been obvious to those skilled in the art to modify Maher by Savage to achieve the claimed invention by determining a complete path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer, as claimed, since Savage teaches that providing a complete traceback of a received packet via marking at each traversed node is a more effective way to combat denial-of-service flooding attacks than the ingress filtering technique that is employed by Maher. Accordingly, Savage provides an express teaching and motivation to improve upon Maher's system by determining complete path information rather than simply filtering packets based on their source addresses.

X. CONFIRMED PATENTABLE CLAIM

Regarding **claim 10**, Maher discloses a method (FIG. 5) of providing packet flooding defense for a network (*see*, *e.g.*, FIGS. 1a and 1b) comprising a plurality of host computers (i.e., webfarm 16 includes webservers 30), routers (i.e., webfarm 16 includes one or more network apparatuses, illustrated in FIG. 4, performing host routing and computing functions), communication lines and transmitted data packets, said method comprising the steps of:

classifying data packets received at said router (step 514; see also columns 7:54–8:3 – data packets received by a network apparatus (FIG. 4) are classified into valid ("wanted") and unverified ("unwanted") categories based on whether the packets are transmitted between known

sources and destinations, *i.e.*, via a known path; the packets are considered "wanted" or "unwanted" to the extent that is it desirable for packets to flow between known sources and destinations, and it is undesirable for packets to flow from unverified sources);

associating a maximum acceptable transmission rate with each class of data packet received at said router (*see* columns 7:54–8:3 and column 11:66–12:19 – the "wanted" class of packets is given a high priority processing rate, i.e., "quality of service," whereas the "unwanted" class of packets is given a low priority processing rate); and

allocating a transmission rate equal to or less than said maximum acceptable transmission rate for unwanted data packets (*see id.* – unwanted packets are given a lower processing rate than wanted packets).

Maher does not appear to expressly disclose the method includes:

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.

Also, Maher discloses classifying data packets received at said router but does not appear to disclose the classifying is done via packet marks provided by routers leading to said host computer by path, as claimed.

Savage discloses methods for combatting denial-of-service attacks that involve anonymous packet flooding (*see* Abstract). Savage teaches that is it conventional to employ "ingress filtering" in order to defend against anonymous attacks (*see* Section 2.1). Ingress filtering involves configuring routers to block packets that arrive with illegitimate source addresses (*see id.*). This is a similar prevention technique that is employed by Maher, which as

explained above, teaches giving higher priority to traffic originating from verified sources, and giving lower priority to traffic from unverified sources.

Savage, however, identifies problems with ingress filtering. Notably, as traffic is aggregated from multiple ISPs into transit networks, there is no longer enough information to unambiguously determine if an arriving packet originates from a valid, known source. Also, its effectiveness depends on widespread, if not universal, deployment. The overhead of ingress filtering can become prohibitive on high-speed links, and even if universally deployed, attackers could still circumvent the filtering by forging addresses within a valid customer network. *See id.*

With these problems in mind, Savage proposes tracing flooding attacks by marking packets probabilistically or deterministically, with the addresses of the routers they traverse (see Section 3). For instance, a packet can be marked by appending the address of each node it traverses so that every received packet has a complete ordered list of the routers it traversed; this provides a complete path of the packet through a network and allows the receiver of the packet to trace the entire path back to its origin (*see* Section 4.1). Alternatively, probabilistic marking of only one node address can allow reconstruction of a complete traffic path from a given source when enough packets have been received (*see* Section 4.2).

It would have been obvious to those skilled in the art to modify Maher by Savage to determine a complete path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer, as claimed, since Savage teaches that providing a complete traceback of a received packet via marking at each traversed node is a more effective way to combat denial-of-service flooding attacks than the ingress filtering technique that is employed by Maher. Accordingly, Savage provides an express teaching and motivation to

improve upon Maher's system by determining complete path information rather than simply filtering packets based on their source addresses.

However, neither Maher nor Savage appears to disclose or suggest the classifying of data packets is done "via packet marks provided by routers leading to said host computer by path," as claimed.

Maher is silent on the incorporation of router-provided packet marks, and therefore does not teach classifying the packets on such a basis.

Savage discloses utilizing router-provided packet marks in order to acquire complete traceback information for packets received by a victim. However, Savage does not appear to disclose using the router-provided packet marks for classifying the packets, as claimed. Rather, Savage only appears to be concerned with determining the path of received packets (the "traceback" problem) and does not seem to disclose any methods or algorithms for using the router marking data to classify received packets in any manner, *e.g.* to distinguish between the packets from an attacker and the packets from a non-attacker.

For this reason, claim 10 is confirmed as patentable over the combination of Maher and Savage. Furthermore, Schuba does not appear to cure this deficiency in the teachings of Maher and Savage because Schuba's disclosure does not involve routers marking traversed packets, as claimed.

XI. CONCLUSION

THIS ACTION IS MADE FINAL.

A shortened statutory period for response to this action is set to expire **TWO MONTHS** from the mailing date of this action.

Extensions of time under 37 CFR 1.136(a) do not apply in reexamination proceedings. The provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Further, in 35 U.S.C. 305 and in 37 CFR 1.550(a), it is required that reexamination proceedings "will be conducted with special dispatch within the Office."

Extensions of time in reexamination proceedings are provided for in 37 CFR 1.550(c). A request for extension of time must specify the requested period of extension and it must be accompanied by the petition fee set forth in 37 CFR 1.17(g). Any request for an extension in a third party requested ex parte reexamination must be filed on or before the day on which action by the patent owner is due, and the mere filing of a request will not effect any extension of time. A request for an extension of time in a third party requested ex parte reexamination will be granted only for sufficient cause, and for a reasonable time specified. Any request for extension in a patent owner requested ex parte reexamination (including reexamination ordered under 35 U.S.C. 257) for up to two months from the time period set in the Office action must be filed no later than two months from the expiration of the time period set in the Office action. A request for an extension in a patent owner requested ex parte reexamination for more than two months from the time period set in the Office action must be filed on or before the day on which action by the patent owner is due, and the mere filing of a request for an extension for more than two months will not effect the extension. The time for taking action in a

patent owner requested ex parte reexamination will not be extended for more than two months from the time period set in the Office action in the absence of sufficient cause or for more than a reasonable time.

The filing of a timely first response to this final rejection will be construed as including a request to extend the shortened statutory period for an additional two months. In no event, however, will the statutory period for response expire later than SIX MONTHS from the mailing date of the final action. See MPEP § 2265.

The patent owner is reminded of the continuing responsibility under 37 CFR § 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving Patent No. 7,523,497 throughout the course of this reexamination proceeding. The third-party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Colin LaRose whose telephone number is 571-272-7423.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew J. Fischer can be reached at 571-272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-9900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

General inquiries may be directed to the Central Reexamination Unit customer service line at (571) 272-7705.

/COLIN M LAROSE/
Primary Examiner, Art Unit 3992

Conferees:

/YUZHEN GE/
Primary Examiner, Art Unit 3992

/ANDREW J. FISCHER/
Supervisory Patent Reexamination Specialist, Art Unit 3992

Office Action in Ex Parte Reexamination	**Control No.** 90/014,746	**Patent Under Reexamination** 7523497	
	Examiner Colin LaRose	**Art Unit** 3992	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

a. ☑ Responsive to the communication(s) filed on 12 January 2022.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

b. ☑ This action is made FINAL.

c. ☐ A statement under 37 CFR 1.530 has not been received from the patent owner.

A shortened statutory period for response to this action is set to expire 2 month(s) from the mailing date of this letter. Failure to respond within the period for response will result in termination of the proceeding and issuance of an *ex parte* reexamination certificate in accordance with this action. 37 CFR 1.550(d). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).** If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☑ Notice of References Cited by Examiner, PTO-892.
2. ☐ Information Disclosure Statement, PTO/SB/08.
3. ☐ Interview Summary, PTO-474.
4. ☐ _____.

Part II SUMMARY OF ACTION

1a. ☑ Claims 1,4,7,10,13 and 16 are subject to reexamination.

1b. ☑ Claims 2-3,5-6,8-9,11-12,14-15 and 17-18 are not subject to reexamination.

2. ☐ Claims _____ have been canceled in the present reexamination proceeding.

3. ☑ Claims 10 are patentable and/or confirmed.

4. ☑ Claims 1,4,7,13 and 16 are rejected.

5. ☐ Claims _____ are objected to.

6. ☐ The drawings, filed on _____ are acceptable.

7. ☐ The proposed drawing correction, filed on _____ has been (7a) ☐ approved (7b) ☐ disapproved.

8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. 119(a)-(d) or (f).

a) ☐ All b) ☐ Some* c) ☐ None of the certified copies have

1 ☐ been received.

2 ☐ not been received.

3 ☐ been filed in Application No. _____.

4 ☐ been filed in reexamination Control No. _____.

5 ☐ been received by the International Bureau in PCT application No. _____.

* See the attached detailed Office action for a list of the certified copies not received.

9. ☐ Since the proceeding appears to be in condition for issuance of an *ex parte* reexamination certificate except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte* Quayle, 1935 C.D. 11, 453 O.G. 213.

10. ☐ Other: _____

cc: Requester (if third party requester)

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
90/014,746	**01/12/2022 03:52:07 PM ET**	**50348.65**

Title of Invention

PACKET FLOODING DEFENSE SYSTEM

Application Information

APPLICATION TYPE	Utility / ex parte reexam	PATENT #	7523497
CONFIRMATION #	9957	FILED BY	Theresa Evenbly
PATENT CENTER #	60484277	FILING DATE	05/03/2021
CUSTOMER #	31718	FIRST NAMED INVENTOR	- 7523497
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	William Ramey

Documents

TOTAL DOCUMENTS: 6

DOCUMENT		PAGES	DESCRIPTION	SIZE (KB)
2022-01-12_20227-0009REX000_ResponseNFOA-497_ver3.pdf		24	-	389 KB
2022-01-12_20227-0009REX000_ResponseNFOA-497_ver3-XI.A....pdf	(1-23)	23	Response after non-final action-owner timely	309 KB
2022-01-12_20227-0009REX000_ResponseNFOA-497_ver3-RXC/SR.pdf	(24-24)	1	Reexam Certificate of Service	122 KB
EX-3001.pdf		26	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	607 KB

EX-3002.pdf	4	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	456 KB
EX-3003.pdf	11	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	600 KB
EX-3004.pdf	9	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	289 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
2022-01-12_20227-0009REX000_ResponseNFOA-497_ver3.pdf	292F8BB3F23898AC686F023D8011FF0D6FFBE72A7636E3BB2499AAB172077296012A9AE03D0FEC6E9DC80697D4C83BD010C9B4D55D6B8E888ED47AE464D59847
2022-01-12_20227-0009REX000_ResponseNFOA-497_ver3-XI.A....pdf	5EA0A851DFD77C2685164C354F71342876DF93C3882947571DF0CEDF1907D4544FEAF314A9BDBD28E5DA604736436F9F480BF67434B38CB789CFE062D45750A1
2022-01-12_20227-0009REX000_ResponseNFOA-497_ver3-RXC/SR.pdf	7E24DD62DB4AFE3BF583F12BC97A9E988B9825CD9A0060814D09048AB948E93F94E3CA8BEA80C11F69A9A2CBF45AFA3544C5DE0F9DD9B51E6F02ADCFD486EE45
EX-3001.pdf	F17C66687C1ECFF5FFE82D3F07919284979D655534FA99AB963A42A03ED9B10A063F6B889691CBD0C1AF4B6FAAADD4EF5907A536D2FDAC3F6AEE9FF55E32774A
EX-3002.pdf	CE5ABA8E126B2F2FDEBE410E485CFAF26D6A1AAAC202ACC73EBCF10A0B0025A81A7FC171A98193D409F09D8AC14B4F15BA1388FDC0104215B82C7037E02BF0B7
EX-3003.pdf	99BCA956AFE1EE3BD9C6D404505664BA011EB11394D4383BEBE4A841E1EE171127B262FB6527FE1915FDD0FB412029CE8FF81BCF09DCACCB80C5DB60D681475C
EX-3004.pdf	CD7E580CBC41B08791F402996FBABEE3171064DD1862DCED

959FBE6FEC65E873A35567AE48AC91ABA960D50D74029FE3F
D6262D31ED786DCDB3FAD769D37CEC6

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Donald N. Cohen	Group Art Unit: 3992
Appl. No.: 10/841,064	Examiner: Larose, Colin M
Filed: May 7, 2004	Confirmation No: 9957
U.S. Patent No. 7,523,497 Issue Date: April 21, 2009 Reexamination Control No. 90/014,746	Atty. Dkt. No.: 20227.0009.REEX00
Title: PACKET FLOODING DEFENSE SYSTEM	

Mail Stop "Ex Parte Reexam"
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted today via the Office electronic filing system (EFS-Web) in accordance with 37 CFR §1.8.

Date: January 12, 2022 Signature: /Theresa M. Evenbly/
Printed Name: Theresa M. Evenbly

RESPONSE TO NON-FINAL OFFICE ACTION PURSUANT TO 37 C.F.R.§ 1.111 and 1.550

Enclosed herewith is PacSec3 LLC's Response pursuant to 37 C.F.R § 1.111 and 1.550 to No-Final Office Action filed on November 12, 2021.

I. STATUS OF THE CLAIMS

Claims 1-18 stand issued in U.S. Patent No. 7,523,497 of which claims 1, 4, 7, 10, 13 and 16 are subject to reexamination. Claims 2-3, 5-6, 8-9, 11-12, 14-15, and 17-18 are not subject to reexamination. Of those claims subject to reexamination, claims 1, 4, 7, 13 and 16 are rejected, claim 10 is confirmed patentable. The Patent Owner has not presently amended the claims.

II. OVERVIEW OF THE OFFICE ACTION

In the Non-Final Office Action in Ex Part Reexamination filed on November 12, 2021 ("NFOA"), the Examiner rejects claims 1, 4, 7, 13 and 16 on the following grounds:

Ground 1: Claims 1, 4, 13 and 16 are rejected under 35 U.S.C.§ 102(e) as being anticipated by Maher (U.S. 7,058,974).

Ground 2: Claim 7 is rejected under 35 U.S.C.§ 103(a) as obvious over Maher (U.S. 7,058,974) in view of Savage ("Practical Network Support for IP Traceback").

Patent Owner disagrees with Examiner's assessment. Patent Owner respectfully traverses these grounds of rejection and requests entry of the present Response and Reconsideration of the rejection in view of the arguments presented herein.

III. SUMMARY OF THE '497 PATENT

U.S. Patent No. 7,523,497 ("the '497 Patent") is directed to a system to defend against and resist packet flooding Distributed Denial of Service (DDoS) attacks for a network. '497 Patent, 2: 6-14

Previous commercial system exchanges rate request and rate response messages between data senders and receivers to allow the sender to adjust the data rate to avoid congestion and to control the data flow. But the typical DDoS attacker will falsify the source address to confound the defense when the defense relies upon information the attacker controls, such as the source address. '497 Patent, 1: 49-2:5

The system of the '497 Patent comprises a plurality of host computers, routers, communication lines and transmitted data packets. The system includes means for classifying data packets received at a host computer, as are means for associating a maximum acceptable processing rate with each class of data packet received at the computer. Means are also provided for the computer to find information for packets it receives regarding the path by which the packets came to the computer. Thus, the computer can use the information to allocate the processing rate available for packets of each class in a desired way.

IV. Claim Construction

During reexamination ordered under 35 U.S.C. 304, claims are given the broadest reasonable interpretation consistent with the specification and limitations

in the specification are not read into the claims *(In re Yamamoto,* 740 F.2d 1569, 222 USPQ934 (Fed. Cir. 1984)). (Ex. 3001 at ¶16).

The Examiner states that the following limitation should be interpreted under pre-AIA 35 U.S.C.§ 112, sixth paragraph.

Functional Phrase #1 (claim 1): means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;

Functional Phrase #2 (claim 1): means for associating a maximum acceptable processing rate with each class of data packet received at said computer;

Functional Phrase #3 (claim 1): means for said computer to find information for packets it receives regarding the path by which said packets came to said 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;

Functional Phrase #4 (claim 1): means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate.

Functional Phrase #5 (claim 4): means for classifying data packets received at a router into wanted data packets and unwanted data packets;

Functional Phrase #6 (claim 4): means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

Cloudflare, Inc. Exhibit 1003 Page 82

Functional Phrase #7 (claim 4): means for said router to find information for packets it receives regarding the path by which said packets came to 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;

Functional Phrase #8 (claim 4): means in said router for said router to use said information to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable transmission rate.

Functional Phrase #9 (claim 13): means for 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;

Functional Phrase #10 (claim 13): means for classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;

Functional Phrase #11 (claim 13): means for assigning a maximum acceptable processing rate to each class of data packet;

Functional Phrase #12 (claim 13): means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets.

Functional Phrase #13 (claim 16): means for a router to determine a path by which said packets came to said router via packet marks provided by routers leading to

Cloudflare, Inc. Exhibit 1003 Page 83

said router; said path comprising all routers in said network via which said packets are routed to said computer;

Functional Phrase #14 (claim 16): means for classifying data packets received at said router into wanted data packets and unwanted data packets by path;

Functional Phrase #15 (claim 16): means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

Functional Phrase #16 (claim 16): means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate.

The Examiner further states Functional Phrase #1, Functional Phrase #2, Functional Phrase #3, Functional Phrase #4, Functional Phrase #9, Functional Phrase #10, Functional Phrase #11, and Functional Phrase #12 correspond to a computer, while Functional Phrase #5, Functional Phrase #6, Functional Phrase #7, Functional Phrase #8, Functional Phrase #13, Functional Phrase #14, Functional Phrase #15, and Functional Phrase #16 correspond to a router, since no special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent.

Sufficient structure exists when the claim language specifies the exact structure that performs the function in question without need to resort to other portions of the specification or extrinsic evidence for an adequate understanding of

the structure. *Altiris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1376, 65 USPQ2d 1865, 1874 (Fed. Cir. 2003).

Patent owner respectively submits that Functional Phrases #1-16 do not invoke pre-AIA 35 U.S.C.§ 112, sixth paragraph, since sufficient structure exists in "means" of Functional Phrases #1-16.

"means" in Functional Phrases #1-4, 9-12 correspond to host computers 18 in Figs.1-9. A host computer has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. The user interface, specialized software, network address, protocol stack of the host computer provides sufficient structure to perform the functions in Functional Phrases #1-4, 9-12. Therefore, "means" in Functional Phrases #1-4, 9-12 do not merely recite general computers having basic functions, but recite host computers having the ability to perform the functions in Functional Phrases #1-4, 9-12. Ex. 3001, at ¶ 34.

Similarly, "means" in Functional Phrases #5-8, 13-16 correspond to routers 22 in Figs.1-9. A router is a piece of electronic equipment that connects computer networks to each other, and sends information between networks. A router may have interfaces for different types of physical layer connections, such as copper cables, fiber optic, or wireless transmission. It can also support different network layer transmission standards. Each network interface is used to enable data packets

to be forwarded from one transmission system to another. The hardware and interfaces of the router provide sufficient structure to perform the functions in Functional Phrases #5-8, 13-16. Therefore, "means" in Functional Phrases #5-8, 13-16 do not merely recite general routers having basic functions but recite routers having the ability to perform the functions in Functional Phrases #5-8, 13-16. Ex. 3001, at ¶ 35.

To the extent that pre-AIA 35 U.S.C.§ 112, sixth paragraph can apply on Functional Phrases #1-16, the specification of the '497 Patent discloses sufficient structure for executing the corresponding functions in Functional Phrases #1-16.

Construction of a means-plus-function limitation includes two steps. "First, the court must determine the claimed function. Second, the court must identify the corresponding structure in the written description of the patent that performs the function." *Applied Med. Res. Corp. v. U.S. Surgical Corp.*, 448 F.3d 1324, 1332 (Fed. Cir. 2006).

In a means-plus-function claim 'in which the disclosed structure is a computer, or microprocessor, programmed to carry out an algorithm, the disclosed structure is not a general-purpose computer, but rather the special purpose computer programmed to perform the disclosed algorithm. *WMS Gaming, Inc. v. Int'l Game Tech.*, 184 F.3d 1339, 1349 (Fed. Cir. 1999).

The specification can express the algorithm "in any understandable terms including as a mathematical formula, in prose, or as a flow chart, or in any other manner that provides sufficient structure." *Finisar Corp. v. DirecTV Grp., Inc.*,523 F.3d 1323, 1340 (Fed. Cir. 2008).

Regarding Functional Phrases #1, 5, 10,14, "means for classifying data packets received at a/said host computer/router into wanted data packets and unwanted data packets/by path". The '497 Patent specification clearly links the function to the description as follows:

Even if the traffic is not reduced, the distinction between "wanted" and "unwanted" packets plays an important role in "reasonable' allocation. **For a site there are normally some packets (in fact, the great majority) that are expected in a very strong sense.** It is reasonable to process these at the highest possible rate. **All other packets are not exactly unwanted**, but the site is willing to process them at only a limited rate. A reasonable approach is to schedule these as described above (using the places from which they were forwarded) at a limited rate, and regard as "unwanted those that end up being significantly delayed (or discarded). '497 Patent, 3: 13-23. Ex. 3001, at ¶ 38.

Therefore, the '497 Patent specification discloses an algorithm to carry out the function "classifying data packets received at a/said host computer/router into

wanted data packets and unwanted data packets/by path" in Functional Phrases #1, 5, 10,14.

Regarding Functional Phrases #2, 6, 11,15, "means for assigning / associating a maximum acceptable processing / transmission rate to each class of data packet", the '497 Patent specification clearly links the function to the description as follows:

The final step in the defense is that cooperating routers will **limit the rate** at which they forward packets to places that so request. This may not be essential in the allocation of service, but it is useful for limiting the bandwidth used by "unwanted" packets. The rate-limiting request is to be made when a site detects a high rate of unwanted packets coming from one place. This helps the site because it no longer has to process as many unwanted packets. It helps the network by freeing some of the bandwidth for other use. '497 Patent, 3: 4-12. Ex. 3001, at ¶ 40.

Therefore, the '497 Patent specification discloses an algorithm to carry out the function "assigning / associating a maximum acceptable processing / transmission rate to each class of data packet" in Functional Phrases #2, 6, 11,15.

Regarding Functional Phrase #3, 7, 9, 13, "means for said computer/router to find information for packets it receives regarding the path by which said packets came to said computer/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", the '497 Patent specification clearly links the function to the description as follows:

Routers will supply data about the forwarding path of the packets that arrive at a site. The site can use this data to allocate service as described above among the packets that arrive. This would solve the problem of unfair service if the packets that arrived were a fair sample of those that were sent to the site. '497 Patent, 2: 54-59. Ex. 3001, at ¶ 42.

Therefore, the '497 Patent specification discloses an algorithm to carry out the function "finding information for packets it receives regarding the path by which said packets came to said computer/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"" in Functional Phrases #3, 7, 9,13.

Regarding Functional Phrases #4, 8, 12, 16, "means in said computer/router for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate", the '497 Patent specification clearly links the function to the description as follows:

The final step in the defense is that cooperating routers will **limit the rate** at which they forward packets to places that so request. This may not be essential in the allocation of service, but it is useful for **limiting the bandwidth used by "unwanted packets. The rate-limiting request is to be made when a site detects**

a high rate of unwanted packets coming from one place. This helps the site because it no longer has to process as many unwanted packets. It helps the network by freeing some of the bandwidth for other use. '497 Patent, 3: 4-12. Ex. 3001, at ¶ 44.

Therefore, the '497 Patent specification discloses an algorithm to carry out the function "using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate" in Functional Phrases #4, 8, 12, 16.

Therefore, even if the Functional Phrases #1-16 should be interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph, there were specific algorithms for executing the claimed function disclosed in the specification of the '497 Patent. "means" in Functional Phrases #1-16 should be considered to be computers/routers that have been specially programmed to execute the claimed functions, rather than general-purpose computers/routers. Ex. 3001, at ¶ 45.

V. CLAIM REJECTIONS

A. Ground 1: Maher Fails to anticipate Claims 1, 4, 13 and 16.

Under Ground 1, the Office action rejects Claims 1, 4, 13 and 16 under 35 U.S.C.§ 102(e) as being anticipated by Maher. Patent Owner respectfully submits that Maher fails to teach or suggest each and every limitation of Claims 1, 4, 13 and

16 and requests that the rejections of Claims 1, 4, 13 and 16 under Ground 1 be withdrawn.

Based on the interpretation under pre-AIA 35 U.S.C.§ 112, sixth paragraph, the Examiner states that the various means-plus-function terms in claims1, 4, 13 and 16 should be construed as general-purpose computers/routers. Accordingly, claims 1 and 13 are interpreted as a packet flooding defense system that comprises one or more computers respectively; claims 4 and 16 are interpreted as a packet flooding defense system that comprises one or more computers respectively. Maher discloses a packet flooding system for a network comprising a plurality host computers and routers, thus, claims 1, 4, 13 and 16 are anticipated by Maher.

As set forth above, since the '497 Patent's specification discloses specific algorithms for executing the claimed function in claims1, 4, 13 and 16, "means" in claims 1, 4, 13 and 16 should be considered to be computers/routers that have been specially programmed to execute the claimed functions, rather than general-purpose computers/routers. Accordingly, whether Maher discloses computers/routers that performs the algorithm disclosed in the specification of the '497 Patent', or the equivalent should be considered to determine whether claims 1,4, 13 and 16 would have been anticipated by Maher. Ex. 3001, at ¶ 46.

Regarding claims 1, and 4, Maher is directed to "a method and apparatus for preventing denial of service type attacks on data networks", the apparatus includes

a traffic flow scanning engine 140 and a quality-of-service processor. Maher does not disclose "to find information for packets it receives regarding the path by which said packets came to said computer/router via packet marks provided by routers leading to said host computer", not to mention "said path comprising all routers in said network via which said packets are routed to said computer" as required by claim 1.

The Examiner states that Maher teaches classifying data packets "by path" since the source of the packets is taken into consideration when classifying them. Page 7, *Ex Parte* Reexamination of U.S. 7,523,497-Non-final Office Action, Nov. 12, 2021. "Since the source of the packets is a **partial path information**". Page 6, *Id.*

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 3002, 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. 3003, 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. 3003 at 35-36; Ex. 3001 at ¶ 48.

According to ordinary meaning, the term "path" is a **link** between two nodes 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 words of the claim 1 itself also recite "said path comprising all routers in said network via which said packets are routed to said computer". Ex. 3001, at ¶ 49.

Maher discloses that "the quality-of-service queues 132 also allow network apparatus 100 to manage network attacks such as denial of service (DoS) attacks. Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the contents contain valid network traffic between known sources and destinations. Traffic flows that have not been verified because they are from unknown Sources or because they are new unclassified flows can be assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic. Since most DoS attacks send either new session information, data from spoofed sources, or meaningless data, network apparatus 100 would assign those traffic flows to low quality traffic queues". Maher, 7:54-67. Ex. 3001, at ¶ 50.

The written description of Maher shows that Maher teaches classifying data packets "by source". Although "source" (when true and accurate) can be recognized

as a part of a path, "source" does not include a link, "source" cannot, by itself, be recognized as a path. When falsified by the attacker, "source" may have no relationship to the real path taken by the packet. Therefore, Maher does not teach " to find information for packets it receives regarding the path by which said packets came to said computer/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" as required by claims 1 and 4. Ex. 3001, at ¶ 51.

Similarly, Maher does not teach "to determine a path by which said packets came to [a host computer] /[said router] via packet marks provided by routers leading to said router; said path comprising all routers in said network via which said packets are routed to said computer" as required by claims 13 and 16. Ex. 3001, at ¶ 52.

Therefore, as a content scanning method for packet flood attacks, Maher does not disclose, anticipate claims 1, 4, 13 and 16 of the '497 Patent. Ex. 3001, at ¶ 53.

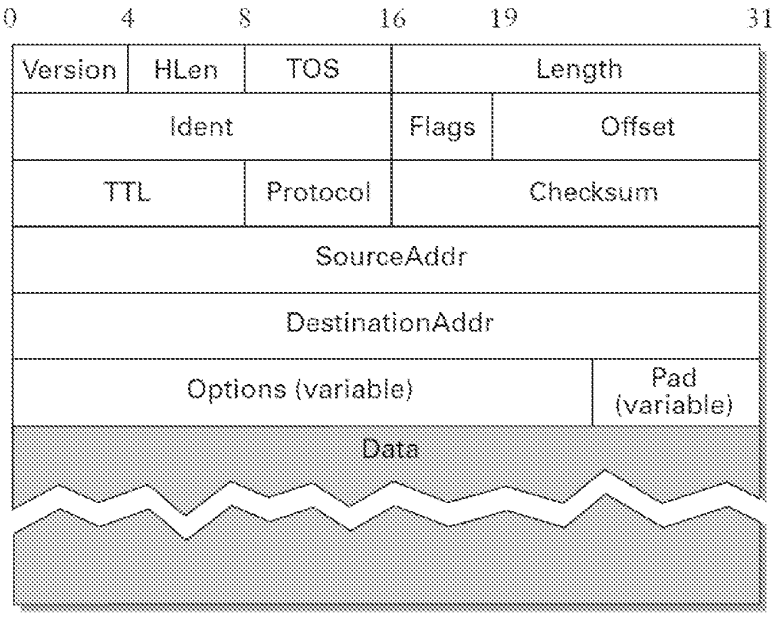
B. <u>Ground 2</u>: The combination of Maher and Savage fails to render obvious Claim 7.

Under Ground 2, the Office action rejects Claim 7 under 35 U.S.C.§ 103(a) as obvious over Maher in view of Savage. Patent Owner respectfully submits that neither Maher nor Savage, whether considered alone or in combination, teach or suggest each and every limitation of Claim 7, and requests that the rejections of Claim 7 under Ground 2 be withdrawn.

Regarding the step "classifying data packets received at said host computer into wanted data packets and unwanted data packets by path", the Examiner states that Maher discloses "Classifying data packets received at said host computer into wanted data packets and unwanted data packets by path **based on whether the packets are transmitted between known sources and destinations, *i.e.*, via a known path**; the packets are considered "wanted" or "unwanted" to the extent that it is desirable or unfavorable for packets to flow **between known sources and destinations,** and it is undesirable or unfavorable for packets to flow from unverified sources (Maher, 7:54-8:3). Page 22, *Ex Parte* Reexamination of U.S. 7,523,497-Non-final Office Action, Nov. 12, 2021.

The disclosure of Maher in columns 7:54-8:3 recites "Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the **contents contain valid network traffic between known sources and destinations.** Traffic flows that have not been verified because they are from unknown sources or because they are new unclassified flows can be assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic. Since most DDoS attacks send either new session information, data from spoofed sources, or meaningless data, network apparatus 100 would assign those traffic flows to low quality traffic queues".

The format of a data packet is described in the book "Computer Networks: A System Approach" as follows (Ex.3004, at 240), Ex. 3001, at ¶ 57.



The last two required fields in the header are the SourceAddr and the DestinationAddr for the packet. The latter is the key to datagram delivery: Every packet contains a full address for its intended destination so that forwarding decisions can be made at each router. The source address is required to allow recipients to decide if they want to accept the packet and to enable them to reply. *Id.*, at 241. Ex. 3001, at ¶ 58.

The packets include information of sources and destinations, but do not include information about path the packets pass through, since the path need to be determined by routers the packets pass through. Scanning the contents of the packets

cannot get information of the path through which the packets travels. **The Maher system has no ability to determine paths the packets travel.** Therefore, "valid network traffic between known sources and destinations" in Maher does not include "a known path" as posited by the Examiner, even if the source address were true and accurate, which it is not likely to be for DDoS attack packets. Ex. 3001, at ¶ 59.

Following the description "Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the contents contain valid network traffic between known sources and destinations". Maher further discloses "Traffic flows that have not been verified because they are from unknown sources or because they are new unclassified flows can be assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic". The context in the specification of Maher shows that "known sources and destinations" means the networks apparatus 100 knows whether the sources and destinations are verified. Ex. 3001, at ¶ 60.

As set forth above, a path must include a link such as a series of routers or packet switches. Maher discloses sources and destinations, although "source" and "destination" can be recognized as a part of a path, "source" and "destination" do not include a link, "source" and "destination" cannot be recognized as a path. Thus, Maher 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. Ex. 3001, at ¶ 61.

Maher discloses "Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the contents contain valid network traffic between known sources and destinations". The "quality of service" attribute driving resource allocation is determined exclusively by whether the flows are verified or not. In contrast, the '497 Patent discloses bandwidth or other resource allocation based on classification of packets into "wanted" and "unwanted" packets as a property that is determined by the end point based on the usefulness of the packets. That determination is entirely independent of the true path taken by those packets through the network to get to the end point. The '497 Patent specification clearly makes this distinction as follows:

Even if the traffic is not reduced, the distinction between "wanted" and "unwanted" packets plays an important role in "reasonable' allocation. **For a site there are normally some packets (in fact, the great majority) that are expected in a very strong sense.** It is reasonable to process these at the highest possible rate. **All other packets are not exactly unwanted**, but the site is willing to process them at only a limited rate. A reasonable approach is to schedule these as described above (using the places from which they were forwarded) at a limited rate, and regard as

"unwanted those that end up being significantly delayed (or discarded). '497 Patent, 3: 13-23. Ex. 3001, at ¶ 63.

Savage describes a technique for tracing anonymous packet flooding attacks on the Internet back towards their source. The '497 Patent teaches how path information can be utilized by the host computer endpoint to classify packets, and to allocate "fair service" to every path through which traffic is being forwarded to the enterprise. This part of the invention proactively DEFENDS the enterprise network against packet flood DDoS attacks. On the contrary, Savage is exclusively a traceback method, it does not disclose any method to detect when an attack may be taking place or how to defend against it. Thus, Savage does not disclose the limitation "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path" as required by Claim 7. Ex. 3001, at ¶ 66.

Savage discloses the limitation of using probabilistic packet marks to encode path. Savage discloses no method to include the path encoding in the packets during transit to their destinations, where that path can then be utilized to defend against DDoS attacks. Being probabilistic in nature, Savage discloses no method for all packets to have path encoding marks in them. Therefore, there is no guarantee in Savage that the end points will have the true path data in all packets when they do arrive to decide how to allocate fair service. Therefore, nothing in the invention of

Maher, can address this problem by simply extending the notion of "source" to include probabilistic packet marks as taught by Savage. Ex. 3001, at ¶ 68.

Therefore, neither Maher nor Savage, whether considered alone or in combination, teach or suggest at least the step "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path" of Claim 7, Maher and Savage do not render Claim 7 of the '497 Patent obvious. Ex. 3001, at ¶ 69.

VI. LIST OF EXHIBITS

Exhibit No.	**Document**
3001	Declaration of Swamy Narayanaswamy with Ex. A Curriculum Vitae
3002	Microsoft Computer Dictionary
3003	Computer Networking: A top-down Approach
3004	Computer Networks: A System Approach

VII. CONCLUSION

Therefore, the Examiner should find Claims 1, 4, 7, 13 and 16 are patentable over the prior art.

Ramey & Schwaller, LLP
5020 Montrose Blvd., Ste. 800

Respectfully submitted,
/William P. Ramey III/

Houston, Texas 77006
(713) 426-3923 (telephone)

William P. Ramey, III
Reg. No.: 44,295
Attorney for Applicant

Cloudflare, Inc. Exhibit 1003 Page 101

CERTIFICATE OF SERVICE

The undersigned certifies that copies of the following,

1) Response to Non-Final Office Action Pursuant to 37 C.F.R.§ 1.111 and 1.550
2) Exhibit 3001- Declaration of Swamy Narayanaswamy with Ex. A Curriculum Vitae
3) Exhibit 3002 – Microsoft Computer Dictionary
4) Exhibit 3003 - Computer Networking: A top-down Approach
5) Exhibit 3004 - Computer Networks: A System Approach

in their entirety were served on:

Raghav Bajaj
Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, TX 75219
raghav.bajaj@haynesboone.com

the attorney of record, in accordance with 37 C.F.R. § 1.510(b)(5), on the 12th day of January 2022.

Dated:

William P. Ramey, III
Registration No.: 44,295

Cloudflare, Inc. Exhibit 1003 Page 102

Exhibit 3001

Declaration of Dr. Swamy Narayanaswamy with Ex. A Curriculum Vitae

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Donald N. Cohen	Group Art Unit: 3992
Appl. No.: 10/841,064	Examiner: Larose, Colin M
Filed: May 7, 2004	Confirmation No: 9957
U.S. Patent No. 7,523,497 Issue Date: April 21, 2009 Reexamination Control No. 90/014,746	Atty. Dkt. No.: 20227.0009.REEX00
Title: PACKET FLOODING DEFENSE SYSTEM	

Mail Stop "Ex Parte Reexam"
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION OF SWAMY NARAYANASWAMY PURSUANT TO 37 CFR 1.132

Cloudflare, Inc. Exhibit 1003 Page 104

I, Swamy Narayanaswamy, do hereby declare as follows:

I. INTRODUCTION

1. I have been retained as an expert on behalf of PacSec 3 LLC ("Patent Owner" or "PacSec3") in this reexamination proceeding of U.S. Patent No. 7,523,497 ("the '497 Patent"). The proceeding was initiated by Requester Unified Patents, LLC ("Requester" or "Unified Patents").

2. I have set forth my professional qualifications and relevant experience in Section II of this Declaration, and a copy of my curriculum vitae is available at Attachment A.

3. I have been asked to provide my expert opinions regarding the validity or invalidity of claims 1, 4, 7, 10, 13, and 16 of the '497 Patent.

4. The November 11, 2021, Non-final Office Action rejected claims 1, 4, 7, 13, and 16 based on the following references: (November 11, 2021, Non-final Office Action at page 3).

Reference	Exhibit
Savage et al., "Practical Network Support for IP Traceback," SIGCOMM '00: Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2000, pp. 295-306 ("Savage")	1005

U.S. Patent No. 7,058,974 to Maher *et al.* ("Maher")	1006

5. As set forth in this Declaration, I do not agree that the identified references or combinations of references anticipate or render unpatentable the challenged claims of the '497 Patent.

6. In forming the opinions that I express in this Declaration, I have considered, among other things, the materials cited or discussed in this Declaration, the '497 Patent, the November 12, 2021 Non-final Office Action, the corresponding file history, Unified Patent's Request for Reexamination, Madisetti's Declaration, the references and exhibits on which Requester and Madisetti rely, and the Order Granting Reexamination of U.S. Patent 7,523,497. Additionally, I have relied on my own knowledge, training, and more than 20 years of experience in analyzing electronics and software. I am a co-author of 8 U.S. Patents.

7. I am being compensated for my time in connection with this Request at my standard consulting rate, and my compensation is not affected by the outcome of this matter.

A. Background and Qualifications

8. I am currently the Chief Technology Officer and co-founder of CalQLogic.

9. I received a Ph.D. in Computer Science from the University of Southern California in 1985; a Master of Science in Computer Science from the University

of Nebraska-Lincoln in 1980, and a Bachelor of Technology in Electronics from the Indian Institute of Technology in 1978.

10. From 2017-Present, I served as the Chief Technology Officer and co-founder of CalQLogic. From 2004-Present, I have served as an adjunct professor at Loyola Marymount University, USC, and UCLA Extension. From 1995-2017, I serve as the Chief Technology Officer and co-founder of Cs3 Inc. From 1985-1995, I serve as a computer scientist at the USC/Information Sciences Institute.

11. I have more than 20 years of experience in analyzing electronics and software.

12. I have been a speaker and panelist at various industry panels and workshops, particularly as it relates to cybersecurity and data analytics.

13. I am a co-author of 4 U.S. Patents.

14. Additional details regarding my background and qualifications are set forth in my curriculum vitae in Attachment A.

15. U.S. Patent No. 7,523,497 ("the '497 Patent") is directed to a system to defend against and resist packet flooding Distributed Denial of Service (DDoS) attacks for a network having a plurality of host computers, routers, communication lines and transmitted data packets, the system includes means for 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; means for classifying data packets received at said host computer into wanted data packets and unwanted data packets by path; means for assigning a maximum acceptable processing rate to each class of data packet; and means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets.

II. Claim Construction

16. During reexamination ordered under 35 U.S.C. 304, claims are given the broadest reasonable interpretation consistent with the specification and limitations in the specification are not read into the claims *(In re Yamamoto,* 740 F.2d 1569, 222 USPQ934 (Fed. Cir. 1984)).

17. The Examiner states that the following limitations should be interpreted under pre-AIA 35 U.S.C.§ 112, sixth paragraph.

18. **Functional Phrase #1 (claim 1):** "means for classifying data packets received at a host computer into wanted data packets and unwanted data packets" is interpreted as a computer.

19. **Functional Phrase #2 (claim 1):** "means for associating a maximum acceptable processing rate with each class of data packet received at said computer" is interpreted as a computer.

20. **Functional Phrase #3 (claim 1):** "means for said computer to find information for packets it receives regarding the path by which said packets came

Cloudflare, Inc. Exhibit 1003 Page 108

to said 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" is interpreted as a computer.

21. **Functional Phrase #4 (claim 1):** "means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate" is interpreted as a computer".

22. **Functional Phrase #5 (claim 4):** "means for classifying data packets received at a router into wanted data packets and unwanted data packets" is interpreted as a router.

23. **Functional Phrase #6 (claim 4):** "means for associating a maximum acceptable transmission rate with each class of data packet received at said router" is interpreted as a router.

24. **Functional Phrase #7 (claim 4):** "means for said router to find information for packets it receives regarding the path by which said packets came to 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" is interpreted as a router.

25. **Functional Phrase #8 (claim 4):** "means in said router for said router to use said information to allocate the transmission rate for unwanted data packets to be

Cloudflare, Inc. Exhibit 1003 Page 109

less than equal to said maximum acceptable transmission rate" is interpreted as a router.

26. **Functional Phrase #9 (claim 13):** "means for 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" is interpreted as a computer.

27. **Functional Phrase #10 (claim 13):** "means for classifying data packets received at said host computer into wanted data packets and unwanted data packets by path" is interpreted as a computer.

28. **Functional Phrase #11 (claim 13):** "means for assigning a maximum acceptable processing rate to each class of data packet' is interpreted as a computer.

29. **Functional Phrase #12 (claim 13):** "means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets" is interpreted as a computer.

30. **Functional Phrase #13 (claim 16):** "means for a router to determine a path by which said packets came to said router via packet marks provided by routers leading to said router; said path comprising all routers in said network via which said packets are routed to said computer" is interpreted as a router.

31. **Functional Phrase #14 (claim 16):** "means for classifying data packets received at said router into wanted data packets and unwanted data packets by path" is interpreted as a router.

32. **Functional Phrase #15 (claim 16):** "means for associating a maximum acceptable transmission rate with each class of data packet received at said router" is interpreted as a router.

33. **Functional Phrase #16 (claim 16):** "means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate" is interpreted as a router.

34. "means" in Functional Phrases #1-4, 9-12 correspond to host computers 18 in Figs.1-9. A host computer has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. The user interface, specialized software, network address, protocol stack of the host computer provides sufficient structure to perform the functions in Functional Phrases #1-4, 9-12. Therefore, "means" in Functional Phrases #1-4, 9-12 do not merely recite general computers having basic functions, but instead are directed towards host computers having the ability to perform the functions in Functional Phrases #1-4, 9-12.

35. Similarly, "means" in Functional Phrases #5-8, 13-16 correspond to routers 22 in Figs.1-9. A router is a piece of electronic equipment that connects computer

networks to each other and sends information between networks. A router may have interfaces for different types of physical layer connections, such as copper cables, fiber optic, or wireless transmission. It can also support different network layer transmission standards. Each network interface is used to enable data packets to be forwarded from one transmission system to another. The hardware and interfaces of the router provide sufficient structure to perform the functions in Functional Phrases #5-8, 13-16. Therefore, "means" in Functional Phrases #5-8, 13-16 do not merely recite general routers having basic functions, but rather recite routers having the ability to perform the functions in Functional Phrases #5-8, 13-16.

36. Further, the specification of the '497 Patent discloses sufficient structure for executing the corresponding functions in Functional Phrases #1-16.

37. Regarding Functional Phrases #1, 5, 10,14, "means for classifying data packets received at a/said host computer/router into wanted data packets and unwanted data packets/by path". The '497 Patent specification clearly links the function to the description as follows:

38. Even if the traffic is not reduced, the distinction between "wanted" and "unwanted packets" plays an important role in "reasonable' allocation. **For a site there are normally some packets (in fact, the great majority) that are expected in a very strong sense.** It is reasonable to process these at the highest possible rate.

All other packets are not exactly unwanted, but the site is willing to process them at only a limited rate. A reasonable approach is to schedule these as described above (using the places from which they were forwarded) at a limited rate, and regard as "unwanted those that end up being significantly delayed (or discarded). '497 Patent, 3: 13-23.

39. Regarding Functional Phrases #2, 6, 11,15, "means for assigning / associating a maximum acceptable processing / transmission rate to each class of data packet", the '497 Patent specification clearly links the function to the description as follows:

40. The final step in the defense is that cooperating routers will **limit the rate** at which they forward packets to places that so request. This may not be essential in the allocation of service, but it is useful for limiting the bandwidth used by "unwanted" packets. The rate-limiting request is to be made when a site detects a high rate of unwanted packets coming from one place. This helps the site because it no longer has to process as many unwanted packets. It helps the network by freeing some of the bandwidth for other use. '497 Patent, 3: 4-12.

41. Regarding Functional Phrase #3, 7, 9, 13, "means for said computer/router to find information for packets it receives regarding the path by which said packets came to said computer/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", the '497 Patent specification clearly links the function to the description as follows:

42. Routers will supply data about the forwarding path of the packets that arrive at a site. The site can use this data to allocate service as described above among the packets that arrive. This would solve the problem of unfair service if the packets that arrived were a fair sample of those that were sent to the site. '497 Patent, 2: 54-59.

43. Regarding Functional Phrases #4, 8, 12, 16, "means in said computer/router for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate", the '497 Patent specification clearly links the function to the description as follows:

44. The final step in the defense is that cooperating routers will **limit the rate** at which they forward packets to places that so request. This may not be essential in the allocation of service, but it is useful for **limiting the bandwidth used by "unwanted packets. The rate-limiting request is to be made when a site detects a high rate of unwanted packets coming from one place. This helps the site because it no longer has to process as many unwanted packets.** It helps the network by freeing some of the bandwidth for other use. '497 Patent, 3: 4-12.

Cloudflare, Inc. Exhibit 1003 Page 114

45. Therefore, even if the Functional Phrases #1-16 should be interpreted under pre-AIA 35 U.S.C.§ 112, sixth paragraph, there were specific algorithms for executing the claimed function disclosed in the specification of the '497 Patent. "means" in Functional Phrases #1-16 should be considered to be computers/routers that have been specially programmed to execute the claimed functions, rather than general-purpose computers/routers.

III. CLAIMS 1, 4, 7, 13, AND 16 ARE PATENTABLE OVER THE REFERENCES INCLUDED IN THE NON-FINAL OFFICE ACTION

A. Challenged Claims 1, 4, 13 and 16 are Patentable Over Maher

46. As set forth above, since the '497 Patent's specification discloses specific algorithms for executing the claimed function in claims 1, 4, 13 and 16, "means" in claims 1, 4, 13 and 16 should be considered as computers/routers that have been specially programmed to execute the claimed functions, rather than general-purpose computers/routers. Accordingly, whether Maher discloses computers/routers that performs the algorithm disclosed in the specification of the '497 Patent', or the equivalent should be considered to determine whether claims 1, 4, 13 and 16 would have been anticipated by Maher.

47. The Examiner states that Maher teaches classifying data packets "by path" since the source of the packets is taken into consideration when classifying them. Page 7, *Ex Parte* Reexamination of U.S. 7,523,497-Non-final Office Action, Nov.

12, 2021. "Since the source of the packets is a **partial path information**". Page 6, *Id.*

48. 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 3002, 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. 3003, 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. 3003, at 35-36.

49. According to ordinary meaning, the term "path" is a **link** between two nodes 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 words of the claim 1 of the '497 Patent also recite "said path comprising all routers in said network via which said packets are routed to said computer".

50. Maher recites: "the quality of service queues 132 also allow network apparatus 100 to manage network attacks such as denial of service (DoS) attacks.

Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the contents contain valid network traffic between known sources and destinations. Traffic flows that have not been verified because they are from unknown Sources or because they are new unclassified flows can be assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic. Since most DoS attacks send either new session information, data from spoofed sources, or meaningless data, network apparatus 100 would assign those traffic flows to low quality traffic queues". Maher, 7:54-67.

51. The written description of Maher shows that Maher teaches classifying data packets "by source". Although "source" (when true and accurate) can be recognized as a part of a path, "source" does not include a link, "source" cannot, by itself, be recognized as a path. When falsified by the attacker, "source" may have no relationship to the real path taken by the packet. Therefore, Maher does not teach "to find information for packets it receives regarding the path by which said packets came to said computer/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" as required by claims 1 and 4.

52. Similarly, Maher does not teach "to determine a path by which said packets came to [a host computer] / [said router] via packet marks provided by routers leading

to said router; said path comprising all routers in said network via which said packets are routed to said computer" as required by claims 13 and 16.

53. Therefore, as a content scanning method for packet flood attacks, Maher does not disclose, anticipate claims 1, 4, 13 and 16 of the '497 Patent.

B. Challenged Claim 7 is Patentable Over Maher and Savage

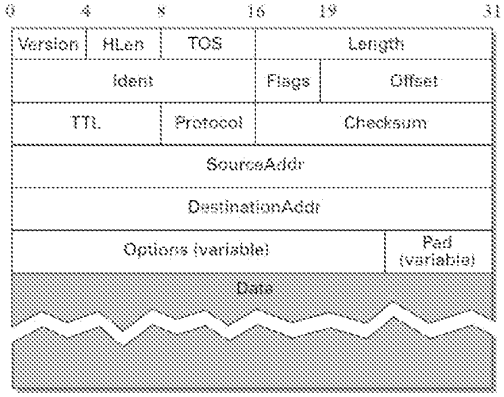
54. Neither Maher nor Savage, whether considered alone or in combination, teach or suggest at least the step "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path" of Claim 7.

55. The Examiner states that Maher disclose "Classifying data packets received at said host computer into wanted data packets and unwanted data packets by path **based on whether the packets are transmitted between known sources and destinations, *i.e.*, via a known path**; the packets are considered "wanted" or "unwanted" to the extent that it is desirable or unfavorable for packets to flow **between known sources and destinations,** and it is undesirable or unfavorable for packets to flow from unverified sources (Maher, 7:54-8:3). Page 22, *Ex Parte* Reexamination of U.S. 7,523,497-Non-final Office Action, Nov. 12, 2021.

56. The disclosure of Maher in columns 7:54-8:3 recites "Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the **contents contain valid network traffic between known sources and destinations.** Traffic flows that have not been verified because they

are from unknown sources or because they are new unclassified flows can be assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic. Since most DDoS attacks send either new session information, data from spoofed sources, or meaningless data, network apparatus 100 would assign those traffic flows to low quality traffic queues".

57. The format of a data packet is described in the book "Computer Networks: A System Approach" as follows (Ex.3004, at 240)



58. The last two required fields in the header are the SourceAddr and the DestinationAddr for the packet. The latter is the key to datagram delivery: Every packet contains a full address for its intended destination so that forwarding decisions can be made at each router. The source address is required to allow recipients to decide if they want to accept the packet and to enable them to reply. *Id.*, page 241.

59. The packets include information of sources and destinations, but do not include information about path the packets pass through, since the path need to be determined by routers the packets pass through. Scanning the contents of the packets cannot get information of the path through which the packets pass through. **Maher has no ability to determine paths the packets travel.** Therefore, "valid network traffic between known sources and destinations" in Maher does not include "a known path" as explained by the Examiner, even if the source address were true and accurate, which it is not likely to be for DDoS attack packets.

60. Following the description "Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the contents contain valid network traffic between known sources and destinations". Maher further discloses "Traffic flows that have not been verified because they are from unknown sources or because they are new unclassified flows can be assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic". The context in the specification of Maher shows that "known sources and destinations" means the networks apparatus 100 knows whether the sources and destinations are verified.

61. As set forth above, a path must include a link such as a series of routers or packet switches. Maher discloses sources and destinations, although "source" and "destination" can be recognized as a part of a path, "source" and "destination" do

not include a link, "source" and "destination" cannot be recognized as a path. Thus, Maher 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.

62. Maher discloses "Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the contents contain valid network traffic between known sources and destinations". The "quality of service" attribute driving resource allocation is determined exclusively by whether the flows are verified or not. In contrast, the 487 Patent discloses bandwidth or other resource allocation based on classification of packets into "wanted" and "unwanted" packets as a property that is determined by the end point based on the usefulness of the packets. That determination is entirely independent of the true path taken by those packets through the network to get to the end point. The '497 Patent specification clearly makes this distinction as follows:

63. Even if the traffic is not reduced, the distinction between "wanted" and "unwanted" packets plays an important role in "reasonable' allocation. **For a site there are normally some packets (in fact, the great majority) that are expected in a very strong sense.** It is reasonable to process these at the highest possible rate. **All other packets are not exactly unwanted**, but the site is willing to process them at only a limited rate. A reasonable approach is to schedule these as described above (using the places from which they were forwarded) at a limited rate, and regard as

"unwanted those that end up being significantly delayed (or discarded). '497 Patent, 3: 13-23.

62. Savage describes a technique for tracing anonymous packet flooding attacks on the Internet back towards their source. (Ex. 1005 at Abstract). Fig. 1 of Savage is shown below. (Ex. 1005 at Figure 1.)

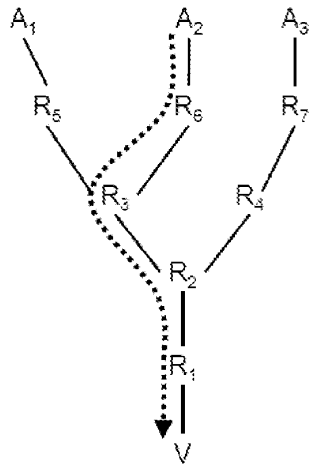


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

63. The '497 Patent teaches how path information can be utilized by the host computer endpoint to classify packets, and to allocate "fair service" to every path through which traffic is being forwarded to the enterprise. This part of the invention proactively DEFENDS the enterprise network against packet flood DDoS attacks. On the contrary, Savage is exclusively a traceback method, it does not disclose any method to detect when an attack may be taking place or how to defend against it.

Thus, Savage does not disclose the limitation "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path" as required by Claim 7.

64. Further, since Savage is exclusively a traceback method, it does not disclose any method to detect when an attack may be taking place or how to defend against it. Savage does not disclose the limitation "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path" as required by claim 7 of the '497 Patent.

65. Savage discloses the limitation of using probabilistic packet marks to encode path. Savage discloses no method to include the path encoding in the packets during transit to their destinations, where that path can then be utilized to defend against DDoS attacks. Being probabilistic in nature, Savage discloses no method for all packets to have path encoding marks in them. Therefore, there is no guarantee in Savage that the end points will have the true path data in all packets when they do arrive to decide how to allocate fair service. Therefore, nothing in the invention of Maher, can address this problem by simply extending the notion of "source" to include probabilistic packet marks as taught by Savage.

66. Therefore, Maher and Savage alone or in combination do not render claim 7 of the '497 Patent obvious.

Cloudflare, Inc. Exhibit 1003 Page 123

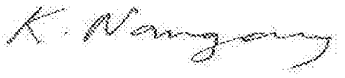
IV. CONCLUSION

67. All Challenged Claims are patentable over the prior art cited in the Non-final Office Action for Reexamination.

68. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Date:
1/11/2022

Respectfully submitted,



Swamy Narayanaswamy

Declaration of Dr. Swamy Narayanaswamy

Exhibit A

Curriculum Vitae of Dr. Swamy Narayanaswamy

Curriculum Vitae

(323) 336-3006 **Dr. Swamy Narayanaswamy** swamy@calqlogic.com
LinkedIn: https://www.linkedin.com/in/knarayanaswamy

Software Development Skill Suite:

- *Modeling and Methods:* UML, Rapid Application Development, Agile development, DevOps
- *Cloud, Micro-services and Containers:* Docker, Kubernetes, and scalable cloud delivery of solutions
- *Machine/Deep Learning, Data Science:* Scikit-Learn, PyTorch, TensorFlow, Keras, Anaconda, Jupyter;
- *Application Languages:* Python, R, Java, C++, C#, Common Lisp;
- *Platforms:* Jupyter, Eclipse, NetBeans IDE, Web2Py, and .NET framework

Professional Interests:

- ✓ **Applying machine / deep learning** & data science to build technologies that improve business outcomes;
- ✓ Experienced in the practical pitfalls/problems of **deploying data-driven solutions into real businesses**;
- ✓ **Master developer in the platforms listed,** with wide experience from soup to nuts in software creation;
- ✓ **Proven architect and leader**, with experience managing technical teams to deliver results effectively;
- ✓ **Teaching courses / mentoring developers** in my areas of expertise (machine learning, data science, AI)

Professional Experience:

2017- Present Chief Technology Officer and co-founder, CalQLogic. ,

- Spear-heading the company's emergence in the real-time analytics marketplace. The platform leverages advanced methods to support D-I-Y analytics over disparate data sources over the Internet and Intranet. The product targets pharma, IOT, supply chain, and other markets.
- Developing / Managing Data Analytics / Machine Learning Consulting projects for clients:
- ✓ Prototyped machine learning solutions for a healthcare startup focused on special needs children. Used Python and Scikit-Learn to build a solution with automatic document OCR, content classification, and extraction of critical data.
- ✓ Working with a medical device startup (using Python / TensorFlow) on its backend deep learning strategy to improve automated diagnostics using machine learning algorithms and models as needed by their executives.
- ✓ Assisting a literature monitoring company in leveraging machine learning to detect deep structure within technical papers in different domains. Leveraging various supervised learning models; and Deep Learning neural networks. Utilized Python/Scitkit Learn

1995 – 2017 Chief Technology Officer and co-founder, Cs3 Inc. ,

Spear-heading the company's technology direction and development of product suite.
Principal Investigator for several R&D projects leading to new products:

"Detection and Containment of Computer Epidemics through Correlation of Communication Anomalies" Department of Homeland Security (2004 – present)
"Attack Attribution Techniques for Heterogeneous, Non-Cooperative Infrastructure" Advanced Research and Development Activity (2003 - present)
"An Event Monitoring Framework for Automatic Network Diagnosis for Defense" Defense Advanced Research Projects Agency (1999-2002)
"Software Evolution Through Automatic Monitoring" DARPA (1996-1999)
"Automatic Monitoring of Software Requirements" NSF, (1996-1997)

- Led Product development for Sonario (a HR Talent management solution) for a client Iscomp Systems / Levinson Institute, that is now in production at corporations;
- Spearheaded Cs3's flagship DDoS defense products under the brand name ManaNet. Conceptualized the products and managed the development of these breakthrough technologies. Presented the technology at multiple venues. Guided the acquisition of 4 US Patents in cybersecurity / DDoS defense;

Cloudflare, Inc. Exhibit 1003 Page 126

1985 - 1995	Computer Scientist, USC/Information Sciences Institute, Co-developer/maintainer of domain modeling environment to apply AI methods to software Development in developing rapid prototypes of software using formal specifications; Providing automated support for evolution of software using Artificial Intelligence methods; Author of about 20 research publications in conferences and journals
2004 – Present	Adjunct Professor at Loyola Marymount University / USC / UCLA Extension Developed and taught AI / Machine Learning courses for grads/undergrads. Taught the capstone AI course offerings for over 5 years at USC. Developed several advanced curricula in OO programming,

Education:

1980 - 1985	University of Southern California, Los Angeles, CA. PhD, Computer Science. (May 1985);
1978 - 1980	University of Nebraska-Lincoln, NE Master of Science, Computer Science.
1973 - 1978	Indian Institute of Technology, Madras, India Bachelor of Technology, Electronics.

Professional Activities:

Speaker and Panelist:

- Multiple appearances in various industry panels and workshops particularly as it relates to cybersecurity, data analytics and business applications of machine learning, IOT, etc. (e.g., Digital Growth Summit). I have contributed to multiple books on my areas within my core competencies.

Program Committees:

- International Symp. on Object Technologies for Advanced Software, Kanazawa, Japan, January, 1996.
- 9th International Software Process Workshop, Airlie, Virginia, October, 1994.
- 1st Int'l Workshop on Process-Centered Software Environments, Boulder, Colorado, October 1993.

Organizer:

- OOPSLA Workshop on Are CASE Frameworks ready for Prime-Time? Austin, Texas, October 1995.

Reviewer:

Reviewed several technical articles for

- International Conference on Software Engineering.
- International Conference on the Software Process.
- IEEE Transactions on Software Engineering.
- IEEE Transactions on Software Engineering and Methodology.
- Journal of Systems and Software, IEEE Transactions on Knowledge Engineering

Awards and Honors:

- Co-author of 8 US Patents in cooperation with the rest of my technology team;
- Led Cs3 to several key R&D contracts in national competitions against much larger corporate juggernauts;
- Governor's Gold Medal, Graduating Class of 1978. Indian Institute of Technology, Madras (One of the 5 elite technology schools in India)

Professional Affiliations:

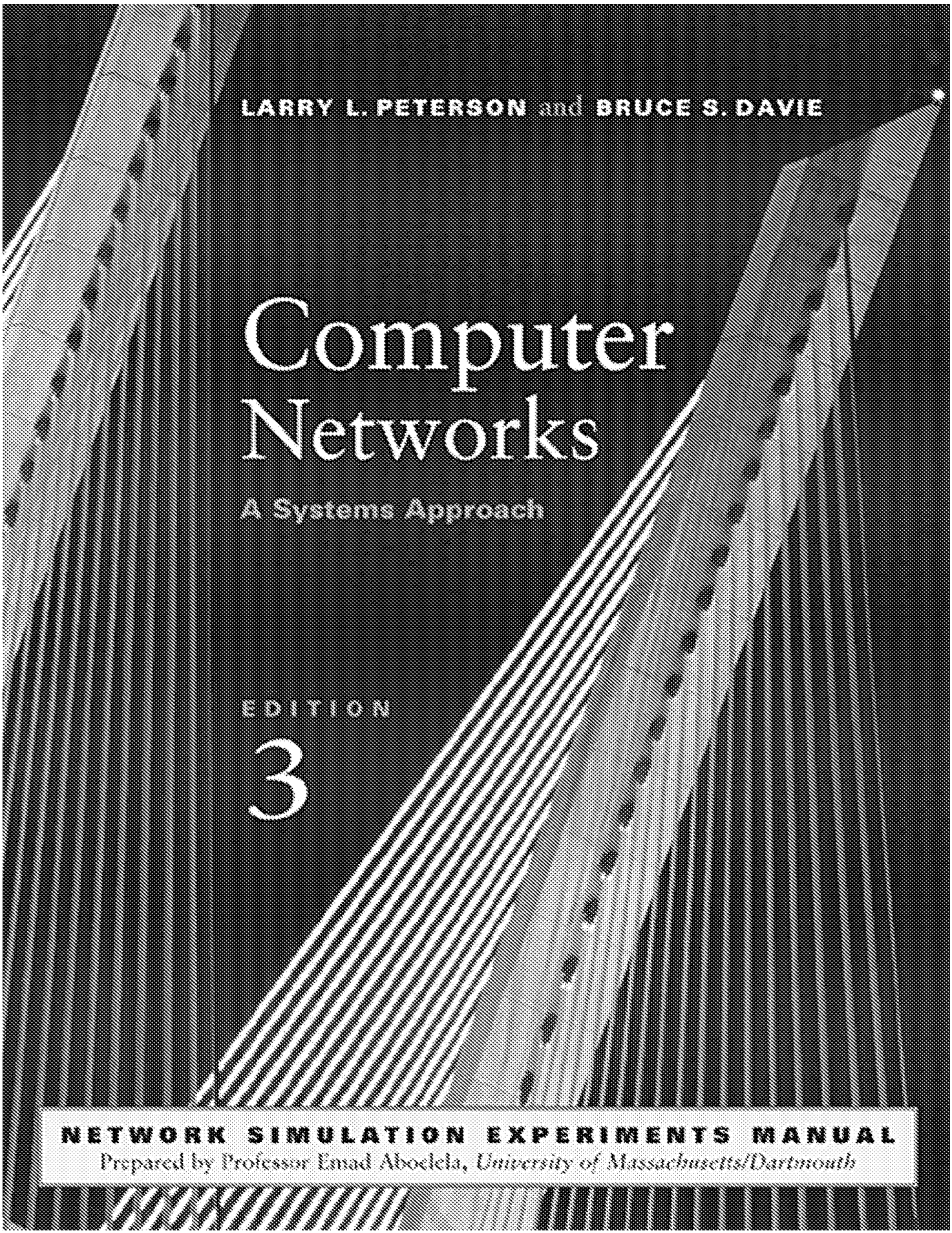
- Member of ACM and IEEE.

Publications:

1. *Using First Order Logic to Query Heterogeneous Internet Data Sources*, Soft Computing and Software Engineering Conference, March 2015, Berkeley, CA. (Selected Best Paper at the Conference), https://www.sciencedirect.com/science/article/pii/S1877050915025661
2. *Key Concepts to Support Creation of Powerful IOT Apps*, Invited Paper, CIO Review Magazine, December 2014, http://magazine.cioreview.com/December-2014/IoT/
3. *Attack Attribution in Non-Cooperative Networks*, IEEE Conference on Information Assurance, August, 2004
4. *Defending Government Networks Against Distributed Denial of Service Attacks,* with Donald Cohen, Cs3 Inc White Paper, http://www.cs3-inc.com/government-ddos-threat-and-solutions.pdf.
5. *Changes to IP to Eliminate Source Forgery, with Donald Cohen*, Cs3 White Paper, http://www.cs3-inc.com/sf.PDF.
6. *A Fair Service Approach to Defending Against Packet Flooding Attacks on the Internet*, with Donald Cohen, Cs3 White Paper, http://www.cs3-inc.com/ddos.PDF.
7. *Relations as Abstraction for C ++ Programming*, with Neil Goldman and Donald Cohen Object-Oriented Programming Systems & Languages (OOPSLA 95).
8. CSCW 94 Workshop to Explore Relationships between Research in Computer Supported Cooperative Work & Software Process — Workshop Report, with Balachander Krishnamurthy, ACM Software Engineering Notes, April 1995.
9. *Process Formalism/Tools/Architecture — Implications for Humans*, (Session Summary), Proceedings of the International Software Process Workshop (ISPW 9), October 1994.
10. *Adding Performance Information to ADT Interfaces: Why and How*, with Neil Goldman and Donald Cohen, SIGPLAN Workshop on Interface Definition Languages, Portland, Oregon, January 1994.
11. *Interactive Elaborations of Generic Designs*, with Lewis Johnson and Robert Balzer, Proceedings of the Knowledge-Based Software Engineering, December, 1993.
12. *Mechanism for Generic Process Support*, with Robert Balzer, Proceedings of the First ACM Symposium on the Foundations of Software Engineering, December, 1993.
13. *PSEE Architectures: ISPW8 Session Summary*, with Maria Penedo, Proceedings of the 8th International Software Process Workshop, March, 1993.
14. *Just What is a Process-Sensitive Software Engineering Environment?*, Proceedings of the Workshop on Process-Sensitive Software Engineering Environments, September, 1992.
15. *Lazy Consistency: A Basis for Cooperative Software Development*, with Neil Goldman, Proceedings of the Computer Supported Cooperative Work Conference, November, 1992.
16. *Software Evolution Based on Iterative Prototyping*, with Neil Goldman, Proceedings of the 14th International Conference on Software Engineering, May, 1992.
17. *Team Coordination: Information Sharing + Policies*, with Neil Goldman, Proceedings of the 7th International Software Process Workshop, 1991.
18. *A Flexible Framework to Support Cooperative Distributed Software Development*, with Neil Goldman, Journal of Systems and Software, October, 1991.
19. *A Logical Framework to Support Cooperative Software Development,* with Donald Cohen, Proceedings of the 6th International Software Process Workshop, 1990.
20. *A Text-Based Representation for Program Variants*, Proceedings of the Second International Workshop on Software Configuration Management, 1989.
21. *Static-Analysis Based Program Evolution Support in the Common Lisp Framework*, Proceedings of the 10th International Conference on Software Engineering, April, 1988.
22. *An Incremental Mechanism for Schema Evolution in Engineering Domains*, with K.V. Bapa Rao, Proceedings of the International Conference on Data Engineering, February 1988.
23. *Version Control in the Common Lisp Framework*, Proceedings of First International Workshop on Software Version and Configuration Control, 1988.
24. *Static Analysis: An Aid to Program Maintenance and Development*, Hawaii International Conference on System Sciences, January, 1988.
25. *Maintaining Configurations of Evolving Systems*, with Walt Scacchi, IEEE Transactions on Software Engineering, SE-13, No. 3, 1987.
26. *A Database Foundation to Support Software System Evolution*, With Walt Scacchi, Journal of Systems and Software, May, 1987.
27. *An Environment for the Development and Maintenance of Large Software Systems*, SOFTFAIR II, Second Conference on Software Development Tools, Techniques, and Alternatives, December, 1985.
28. *An Approach to Information Management for CAD/VLSI Applications*, with Dennis Mcleod and K.V. Bapa Rao, Proceedings of the ACM SIGMOD, 1983.

Exhibit 3004

Computer Networks: A System Approach



Cloudflare, Inc. Exhibit 1003 Page 130

THIRD EDITION

COMPUTER NETWORKS

A Systems Approach

Cloudflare, Inc. Exhibit 1003 Page 131

The Morgan Kaufmann Series in Networking
Series Editor, David Clark, M.I.T.

Computer Networks: A Systems Approach, 3e
Larry L. Peterson and Bruce S. Davie
Network Architecture, Analysis, and Design, 2e
James D. McCabe
MPLS Network Management: MIBs, Tools, and Techniques
Thomas D. Nadeau
Developing IP-Based Services: Solutions for Service Providers and Vendors
Monique Morrow and Kateel Vijayananda
Telecommunications Law in the Internet Age
Sharon K. Black
Optical Networks: A Practical Perspective, 2e
Rajiv Ramaswami and Kumar N. Sivarajan
Internet QoS: Architectures and Mechanisms
Zheng Wang
TCP/IP Sockets in Java: Practical Guide for Programmers
Michael J. Donahoo and Kenneth L. Calvert
TCP/IP Sockets in C: Practical Guide for Programmers
Kenneth L. Calvert and Michael J. Donahoo
Multicast Communication: Protocols, Programming, and Applications
Ralph Wittmann and Martina Zitterbart
MPLS: Technology and Applications
Bruce Davie and Yakov Rekhter
High-Performance Communication Networks, 2e
Jean Walrand and Pravin Varaiya
Internetworking Multimedia
Jon Crowcroft, Mark Handley, and Ian Wakeman
Understanding Networked Applications: A First Course
David G. Messerschmitt
Integrated Management of Networked Systems: Concepts, Architectures, and their Operational Application
Heinz-Gerd Hegering, Sebastian Abeck, and Bernhard Neumair
Virtual Private Networks: Making the Right Connection
Dennis Fowler
Networked Applications: A Guide to the New Computing Infrastructure
David G. Messerschmitt
Modern Cable Television Technology: Video, Voice, and Data Communications
Walter Ciciora, James Farmer, and David Large
Switching in IP Networks: IP Switching, Tag Switching, and Related Technologies
Bruce S. Davie, Paul Doolan, and Yakov Rekhter
Wide Area Network Design: Concepts and Tools for Optimization
Robert S. Cahn
Frame Relay Applications: Business and Technology Case Studies
James P. Cavanagh

For further information on these books and for a list of forthcoming titles, please visit our website at http://www.mkp.com

THIRD EDITION

Larry L. Peterson & Bruce S. Davie

COMPUTER NETWORKS

A Systems Approach

MORGAN KAUFMANN PUBLISHERS

AN IMPRINT OF ELSEVIER SCIENCE

AMSTERDAM BOSTON LONDON NEW YORK
OXFORD PARIS SAN DIEGO SAN FRANCISCO
SINGAPORE SYDNEY TOKYO

Cloudflare, Inc. Exhibit 1003 Page 133

that if something goes wrong and the packet gets lost, corrupted, misdelivered, or in any way fails to reach its intended destination, the network does nothing—it made its best effort, and that is all it has to do. It does not make any attempt to recover from the failure. This is sometimes called an *unreliable* service.

Best-effort, connectionless service is about the simplest service you could ask for from an internetwork, and this is a great strength. For example, if you provide best-effort service over a network that provides a reliable service, then that's fine—you end up with a best-effort service that just happens to always deliver the packets. If, on the other hand, you had a reliable service model over an unreliable network, you would have to put lots of extra functionality into the routers to make up for the deficiencies of the underlying network. Keeping the routers as simple as possible was one of the original design goals of IP.

The ability of IP to "run over anything" is frequently cited as one of its most important characteristics. It is noteworthy that many of the technologies over which IP runs today did not exist when IP was invented. So far, no networking technology has been invented that has proven too bizarre for IP; it has even been claimed that IP can run over a network that transports messages using carrier pigeons.

Best-effort delivery does not just mean that packets can get lost. Sometimes they can get delivered out of order, and sometimes the same packet can get delivered more than once. The higher-level protocols or applications that run above IP need to be aware of all these possible failure modes.

Packet Format

Clearly, a key part of the IP service model is the type of packets that can be carried. The IP datagram, like most packets, consists of a header followed by a number of bytes of data. The format of the header is shown in Figure 4.3. Note that we have adopted a different style of representing packets than the one we used in previous chapters. This is because packet formats at the internetworking layer and above, where we will be focusing our attention for the next few chapters, are almost invariably designed to align on 32-bit boundaries to simplify the task of processing them in software. Thus, the common way of representing them (used in Internet *Requests for Comments*, for example) is to draw them as a succession of 32-bit words. The top word is the one transmitted first, and the leftmost byte of each word is the one transmitted first. In this representation, you can easily recognize fields that are a multiple of 8 bits long. On the odd occasion when fields are not an even multiple of 8 bits, you can determine the field lengths by looking at the bit positions marked at the top of the packet.

Looking at each field in the IP header, we see that the "simple" model of best-effort datagram delivery still has some subtle features. The Version field specifies the

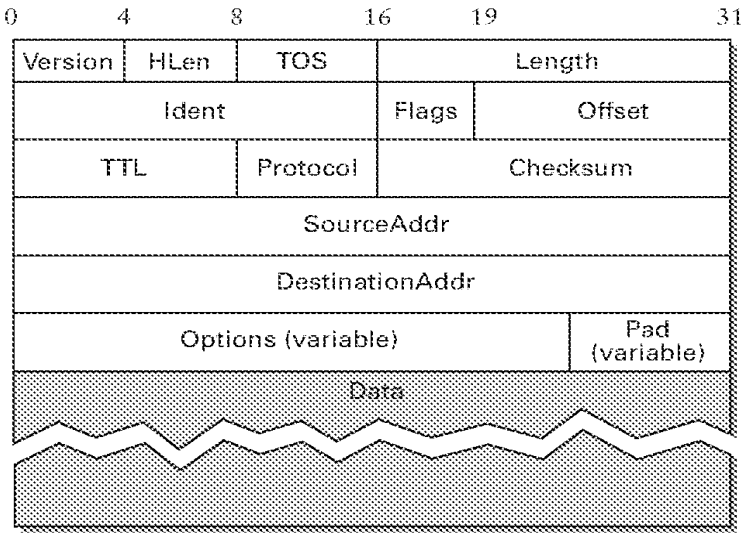


Figure 4.3 IPv4 packet header.

version of IP. The current version of IP is 4, and it is sometimes called IPv4.[1] Observe that putting this field right at the start of the datagram makes it easy for everything else in the packet format to be redefined in subsequent versions; the header processing software starts off by looking at the version and then branches off to process the rest of the packet according to the appropriate format. The next field, HLen, specifies the length of the header in 32-bit words. When there are no options, which is most of the time, the header is 5 words (20 bytes) long. The 8-bit TOS (type of service) field has had a number of different definitions over the years, but its basic function is to allow packets to be treated differently based on application needs. For example, the TOS value might determine whether or not a packet should be placed in a special queue that receives low delay. We discuss the use of this field (and a new name for it) in more detail in Section 6.5.3.

The next 16 bits of the header contain the Length of the datagram, including the header. Unlike the HLen field, the Length field counts bytes rather than words. Thus, the maximum size of an IP datagram is 65,535 bytes. The physical network over which IP is running, however, may not support such long packets. For this reason, IP supports a fragmentation and reassembly process. The second word of the header contains information about fragmentation, and the details of its use are presented under "Fragmentation and Reassembly" below.

[1]The next major version of IP, which is discussed later in this chapter, has a new version number 6 and is known as IPv6. The version number 5 was used for an experimental protocol called ST-II that was not widely used.

Moving on to the third word of the header, the next byte is the TTL (time to live) field. Its name reflects its historical meaning rather than the way it is commonly used today. The intent of the field is to catch packets that have been going around in routing loops and discard them, rather than let them consume resources indefinitely. Originally, TTL was set to a specific number of seconds that the packet would be allowed to live, and routers along the path would decrement this field until it reached 0. However, since it was rare for a packet to sit for as long as 1 second in a router, and routers did not all have access to a common clock, most routers just decremented the TTL by 1 as they forwarded the packet. Thus, it became more of a hop count than a timer, which is still a perfectly good way to catch packets that are stuck in routing loops. One subtlety is in the initial setting of this field by the sending host: Set it too high and packets could circulate rather a lot before getting dropped; set it too low and they may not reach their destination. The value 64 is the current default.

The Protocol field is simply a demultiplexing key that identifies the higher-level protocol to which this IP packet should be passed. There are values defined for TCP (6), UDP (17), and many other protocols that may sit above IP in the protocol graph.

The Checksum is calculated by considering the entire IP header as a sequence of 16-bit words, adding them up using ones complement arithmetic, and taking the ones complement of the result. This is the IP checksum algorithm described in Section 2.4. Thus, if any bit in the header is corrupted in transit, the checksum will not contain the correct value upon receipt of the packet. Since a corrupted header may contain an error in the destination address—and, as a result, may have been misdelivered—it makes sense to discard any packet that fails the checksum. It should be noted that this type of checksum does not have the same strong error detection properties as a CRC, but it is much easier to calculate in software.

The last two required fields in the header are the SourceAddr and the DestinationAddr for the packet. The latter is the key to datagram delivery: Every packet contains a full address for its intended destination so that forwarding decisions can be made at each router. The source address is required to allow recipients to decide if they want to accept the packet and to enable them to reply. IP addresses are discussed in Section 4.1.3—for now, the important thing to know is that IP defines its own global address space, independent of whatever physical networks it runs over. As we will see, this is one of the keys to supporting heterogeneity.

Finally, there may be a number of options at the end of the header. The presence or absence of options may be determined by examining the header length (HLen) field. While options are used fairly rarely, a complete IP implementation must handle them all.

Fragmentation and Reassembly

One of the problems of providing a uniform host-to-host service model over a heterogeneous collection of networks is that each network technology tends to have its own idea of how large a packet can be. For example, an Ethernet can accept packets up to 1500 bytes long, while FDDI packets may be 4500 bytes long. This leaves two choices for the IP service model: make sure that all IP datagrams are small enough to fit inside one packet on any network technology, or provide a means by which packets can be fragmented and reassembled when they are too big to go over a given network technology. The latter turns out to be a good choice, especially when you consider the fact that new network technologies are always turning up, and IP needs to run over all of them; this would make it hard to pick a suitably small bound on datagram size. This also means that a host will not send needlessly small packets, which wastes bandwidth and consumes processing resources by requiring more headers per byte of data sent. For example, two hosts connected to FDDI networks that are interconnected by a point-to-point link would not need to send packets small enough to fit on an Ethernet.

The central idea here is that every network type has a *maximum transmission unit* (MTU), which is the largest IP datagram that it can carry in a frame. Note that this value is smaller than the largest packet size on that network because the IP datagram needs to fit in the *payload* of the link-layer frame. Also, note that in ATM networks, the "frame" is the CS-PDU, not the ATM cell; the fact that CS-PDUs get segmented into cells is not visible to IP.

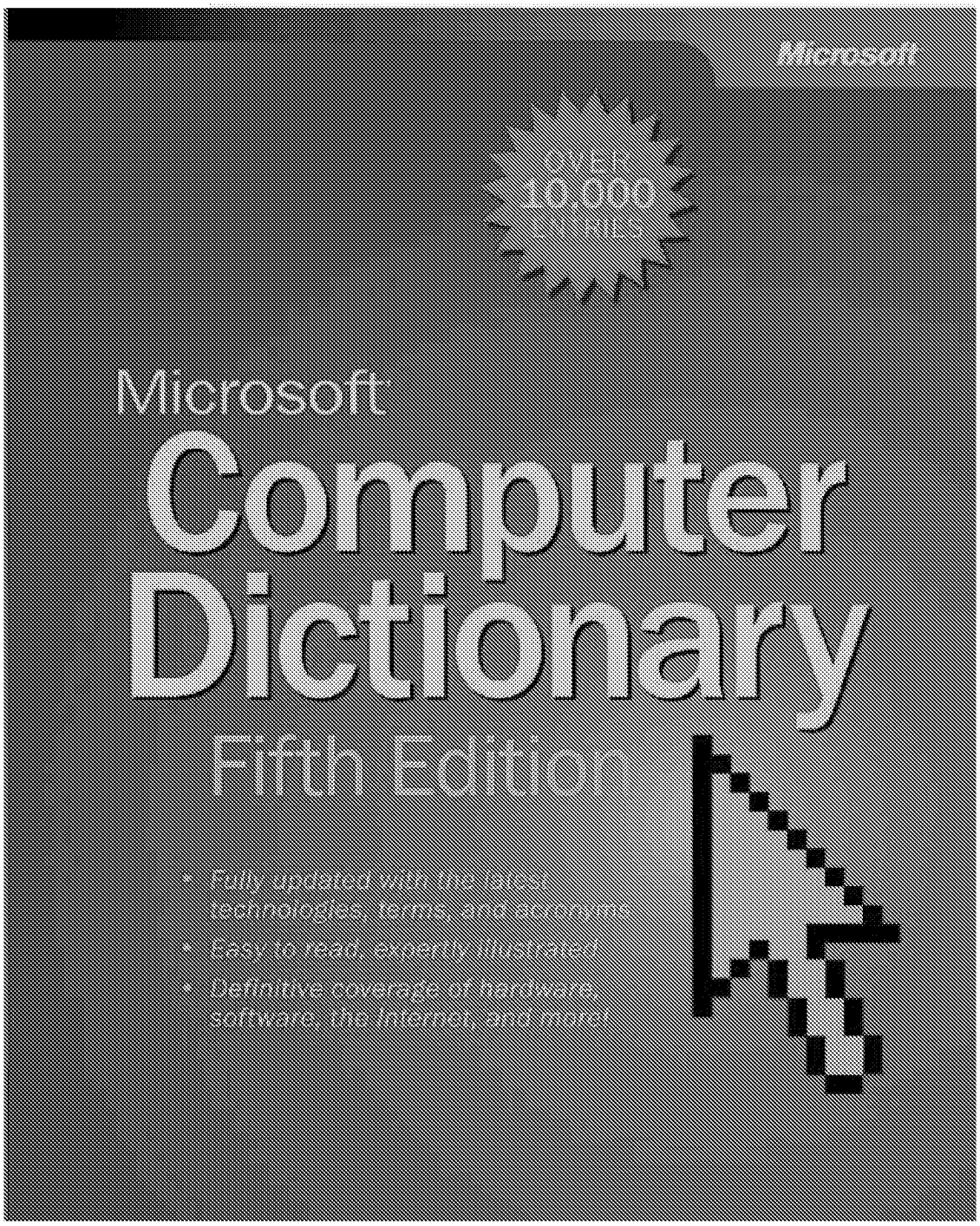
When a host sends an IP datagram, therefore, it can choose any size that it wants. A reasonable choice is the MTU of the network to which the host is directly attached. Then fragmentation will only be necessary if the path to the destination includes a network with a smaller MTU. Should the transport protocol that sits on top of IP give IP a packet larger than the local MTU, however, then the source host must fragment it.

Fragmentation typically occurs in a router when it receives a datagram that it wants to forward over a network that has an MTU that is smaller than the received datagram. To enable these fragments to be reassembled at the receiving host, they all carry the same identifier in the Ident field. This identifier is chosen by the sending host and is intended to be unique among all the datagrams that might arrive at the destination from this source over some reasonable time period. Since all fragments of the original datagram contain this identifier, the reassembling host will be able to recognize those fragments that go together. Should all the fragments not arrive at the receiving host, the host gives up on the reassembly process and discards the fragments that did arrive. IP does not attempt to recover from missing fragments.

To see what this all means, consider what happens when host H1 sends a datagram to host H8 in the example internet shown in Figure 4.1. Assuming that the MTU

Exhibit 3002

Microsoft Computer Dictionary


Microsoft
OVER
10,000
TERMS
DEFINED
Microsoft
Computer
Dictionary
Fifth Edition
• Fully updated with the latest technologies, terms, and acronyms
• Easy to read, expertly illustrated
• Definitive coverage of hardware, software, the Internet, and more!

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 2002 by Microsoft Corporation

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Cataloging-in-Publication Data
Microsoft Computer Dictionary.--5th ed.
p. cm.
ISBN 0-7356-1495-4
1. Computers--Dictionaries. 2. Microcomputers--Dictionaries.

AQ76.5.MS2267 2002
004'.03--dc21 2002219714

Printed and bound in the United States of America.

2 3 4 5 6 7 8 9 QWT 7 6 5 4 3 2

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to *mspinput@microsoft.com*.

Active Desktop, Active Directory, ActiveMovie, ActiveStore, ActiveSync, ActiveX, Authenticode, BackOffice, BizTalk, ClearType, Direct3D, DirectAnimation, DirectDraw, DirectInput, DirectMusic, DirectPlay, DirectShow, DirectSound, DirectX, Entourage, FoxPro, FrontPage, Hotmail, IntelliEye, IntelliMouse, IntelliSense, JScript, MapPoint, Microsoft, Microsoft Press, Mobile Explorer, MS-DOS, MSN, Music Central, NetMeeting, Outlook, PhotoDraw, PowerPoint, SharePoint, UltimateTV, Visio, Visual Basic, Visual C++, Visual FoxPro, Visual InterDev, Visual J++, Visual SourceSafe, Visual Studio, Win32, Win32s, Windows, Windows Media, Windows NT, Xbox are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Acquisitions Editor: Alex Blanton
Project Editor: Sandra Haynes

Body Part No. X08-41929

circumstances. Patching is a common means of adding a feature or a function to a program until the next version of the software is released. *Compare* hack (definition 2), kludge (definition 2).

path *n.* **1.** In communications, a link between two nodes in a network. **2.** A route through a structured collection of information, as in a database, a program, or files stored on disk. **3.** In programming, the sequence of instructions a computer carries out in executing a routine. **4.** In information processing, such as the theory underlying expert (deductive) systems, a logical course through the branches of a tree of inferences leading to a conclusion. **5.** In file storage, the route followed by the operating system through the directories in finding, sorting, and retrieving files on a disk. **6.** In graphics, an accumulation of line segments or curves to be filled or drawn.

path menu *n.* In windowed environments, the menu or drop box used to enter the universal naming convention path to a shared network resource.

pathname *n.* In a hierarchical filing system, a listing of the directories or folders that lead from the current directory to a file. *Also called:* directory path.

pattern recognition *n.* **1.** A broad technology describing the ability of a computer to identify patterns. The term usually refers to computer recognition of visual images or sound patterns that have been converted to arrays of numbers. **2.** The recognition of purely mathematical or textual patterns.

P

Pause key *n.* **1.** A key on a keyboard that temporarily stops the operation of a program or a command. The Pause key is used, for example, to halt scrolling so that a multiscreen listing or document can be read. **2.** Any key that creates a pause in an operation. For example, many game programs have a Pause key, often simply the P key, that temporarily suspends the game.

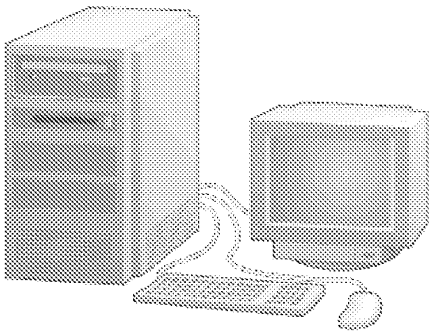
payload *n.* The effects caused by a virus or other malicious code. The payload of a virus may include moving, altering, overwriting, and deleting files, or other destructive activity. A virus or worm may contain more than one payload, each with a separate trigger.

PB *n. See* petabyte.

PB SRAM *n. See* pipeline burst static RAM.

PBX *n.* Acronym for Private Branch Exchange. An automatic telephone switching system that enables users within an organization to place calls to each other without going through the public telephone network. Users can also place calls to outside numbers.

PC *n.* **1.** A microcomputer that conforms to the standard developed by IBM for personal computers, which uses a microprocessor in the Intel 80x86 family (or compatible) and can execute the BIOS. See the illustration. *See also* 8086, BIOS, clone, IBM PC. **2.** A computer in IBM's Personal Computer line. *Also called:* IBM PC. *See also* PC-compatible (definition 1), personal computer.



PC.

PCB *n. See* printed circuit board.

PC board *n. See* printed circuit board.

PC Card *n.* An add-in card that conforms to the PCMCIA specification. A PC Card is a removable device, approximately the same size as a credit card, that is designed to plug into a PCMCIA slot. Release 1 of the PCMCIA specification, introduced in June 1990, specified a Type I card that is 3.3 millimeters thick and is intended to be used primarily as a memory-related peripheral. Release 2 of the PCMCIA specification, introduced in September 1991, specifies both a 5-millimeter-thick Type II card and a 10.5-millimeter-thick Type III card. Type II cards accommodate devices such as modems, fax, and network cards. Type III cards accommodate devices that require more space, such as wireless communications devices and rotating storage media (such as hard disks). *See also* PCMCIA, PCMCIA slot.

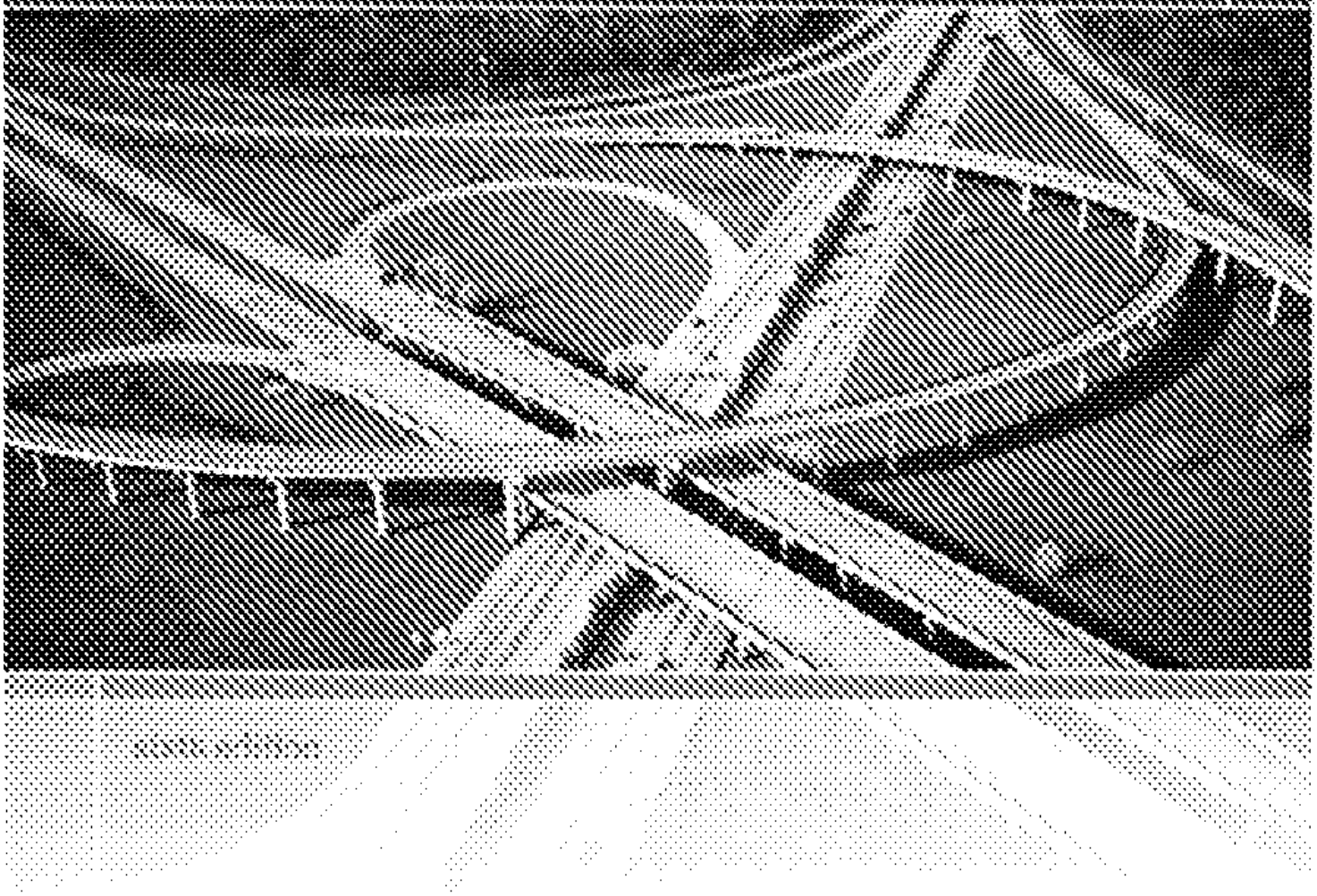
Cloudflare, Inc. Exhibit 1003 Page 141

Exhibit 3003

Computer Networking: A top-down Approach

Computer Networking

A Top-Down Approach



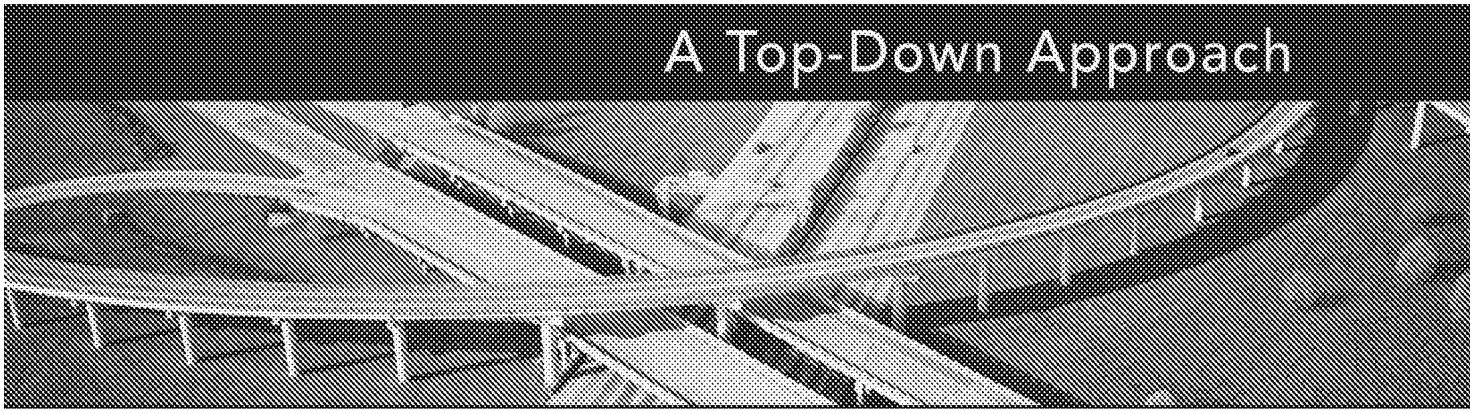
KUROSE | ROSS

Cloudflare, Inc. Exhibit 1003 Page 143

COMPUTER NETWORKING

SIXTH EDITION

A Top-Down Approach



JAMES F. KUROSE

University of Massachusetts, Amherst

KEITH W. ROSS

Polytechnic Institute of NYU

PEARSON

Boston Columbus Indianapolis New York San Francisco Upper Saddle River
Amsterdam Cape Town Dubai London Madrid Milan Munich Paris Montréal Toronto
Delhi Mexico City São Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo

Cloudflare, Inc. Exhibit 1003 Page 144

Vice President and Editorial Director, ECS: Marcia Horton
Editor in Chief: Michael Hirsch
Editorial Assistant: Emma Snider
Vice President Marketing: Patrice Jones
Marketing Manager: Yez Alayan
Marketing Coordinator: Kathryn Ferranti
Vice President and Director of Production: Vince O'Brien
Managing Editor: Jeff Holcomb
Senior Production Project Manager: Marilyn Lloyd
Manufacturing Manager: Nick Sklitsis
Operations Specialist: Lisa McDowell
Art Director, Cover: Anthony Gemmellaro
Art Coordinator: Janet Theurer/ Theurer Briggs Design
Art Studio: Patrice Rossi Calkin/ Rossi Illustration and Design
Cover Designer: Liz Harasymcuk
Text Designer: Joyce Cosentino Wells
Cover Image: ©Fancy/Alamy
Media Editor: Dan Sandin
Full-Service Vendor: PreMediaGlobal
Senior Project Manager: Andrea Stefanowicz
Printer/Binder: Edwards Brothers
Cover Printer: Lehigh-Phoenix Color

This book was composed in Quark. Basal font is Times. Display font is Berkeley.

Copyright © 2013, 2010, 2008, 2005, 2003 by Pearson Education, Inc., publishing as Addison-Wesley. All rights reserved. Manufactured in the United States of America. This publication is protected by Copyright, and permission should be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. To obtain permission(s) to use material from this work, please submit a written request to Pearson Education, Inc., Permissions Department, One Lake Street, Upper Saddle River, New Jersey 07458, or you may fax your request to 201-236-3290.

Many of the designations by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed in initial caps or all caps.

Library of Congress Cataloging-in-Publication Data
Kurose, James F.
Computer networking : a top-down approach / James F. Kurose, Keith W. Ross.—6th ed.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-13-285620-1
ISBN-10: 0-13-285620-4
1. Internet. 2. Computer networks. I. Ross, Keith W., 1956- II. Title.
TK5105.875.I57K88 2012
004.6—dc23

2011048215

10 9 8 7 6 5 4 3 2 1

PEARSON

ISBN-10: 0-13-285620-4
ISBN-13: 978-0-13-285620-1

We'll structure our overview of computer networks in this chapter as follows. After introducing some basic terminology and concepts, we'll first examine the basic hardware and software components that make up a network. We'll begin at the network's edge and look at the end systems and network applications running in the network. We'll then explore the core of a computer network, examining the links and the switches that transport data, as well as the access networks and physical media that connect end systems to the network core. We'll learn that the Internet is a network of networks, and we'll learn how these networks connect with each other.

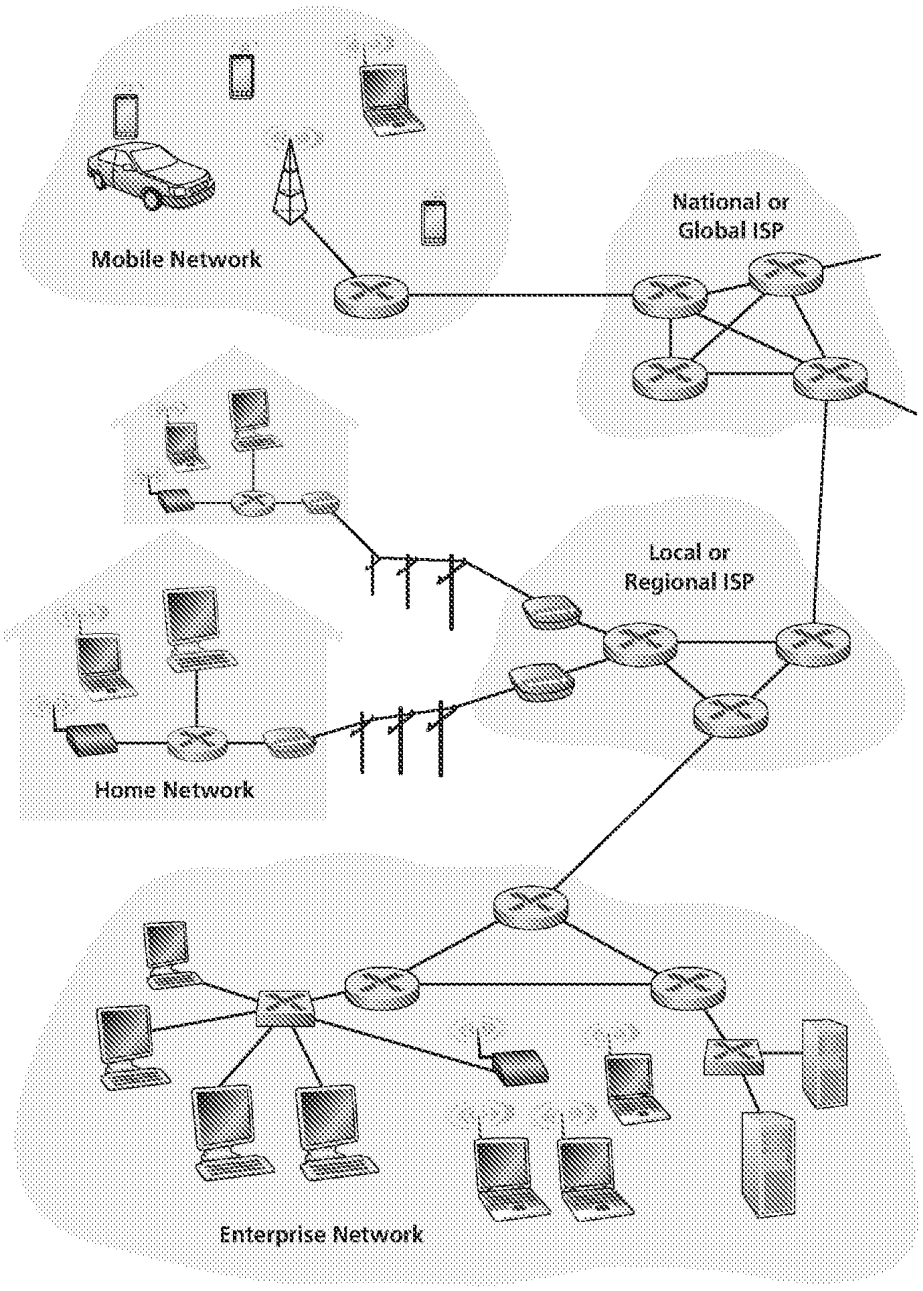
After having completed this overview of the edge and core of a computer network, we'll take the broader and more abstract view in the second half of this chapter. We'll examine delay, loss, and throughput of data in a computer network and provide simple quantitative models for end-to-end throughput and delay: models that take into account transmission, propagation, and queuing delays. We'll then introduce some of the key architectural principles in computer networking, namely, protocol layering and service models. We'll also learn that computer networks are vulnerable to many different types of attacks; we'll survey some of these attacks and consider how computer networks can be made more secure. Finally, we'll close this chapter with a brief history of computer networking.

1.1 What Is the Internet?

In this book, we'll use the public Internet, a specific computer network, as our principal vehicle for discussing computer networks and their protocols. But what *is* the Internet? There are a couple of ways to answer this question. First, we can describe the nuts and bolts of the Internet, that is, the basic hardware and software components that make up the Internet. Second, we can describe the Internet in terms of a networking infrastructure that provides services to distributed applications. Let's begin with the nuts-and-bolts description, using Figure 1.1 to illustrate our discussion.

1.1.1 A Nuts-and-Bolts Description

The Internet is a computer network that interconnects hundreds of millions of computing devices throughout the world. Not too long ago, these computing devices were primarily traditional desktop PCs, Linux workstations, and so-called servers that store and transmit information such as Web pages and e-mail messages. Increasingly, however, nontraditional Internet end systems such as laptops, smartphones, tablets, TVs, gaming consoles, Web cams, automobiles, environmental sensing devices, picture frames, and home electrical and security systems are being connected to the Internet. Indeed, the term *computer network* is beginning to sound a bit dated, given the many nontraditional devices that are being hooked up to the Internet. In Internet jargon, all of these devices are called **hosts** or **end systems**. As of July 2011, there were



Key:

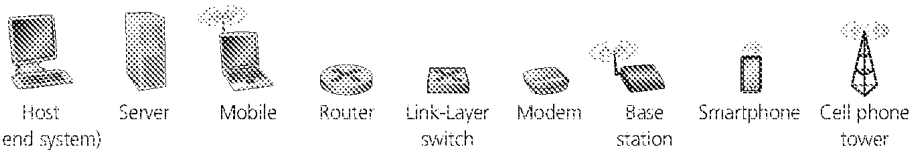


Figure 1.1 ◆ Some pieces of the Internet

nearly 850 million end systems attached to the Internet [ISC 2012], not counting smartphones, laptops, and other devices that are only intermittently connected to the Internet. Overall, more there are an estimated 2 billion Internet users [ITU 2011].

End systems are connected together by a network of **communication links** and **packet switches**. We'll see in Section 1.2 that there are many types of communication links, which are made up of different types of physical media, including coaxial cable, copper wire, optical fiber, and radio spectrum. Different links can transmit data at different rates, with the **transmission rate** of a link measured in bits/second. When one end system has data to send to another end system, the sending end system segments the data and adds header bytes to each segment. The resulting packages of information, known as **packets** in the jargon of computer networks, are then sent through the network to the destination end system, where they are reassembled into the original data.

A packet switch takes a packet arriving on one of its incoming communication links and forwards that packet on one of its outgoing communication links. Packet switches come in many shapes and flavors, but the two most prominent types in today's Internet are **routers** and **link-layer switches**. Both types of switches forward packets toward their ultimate destinations. Link-layer switches are typically used in access networks, while routers are typically used in the network core. 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. The exact amount of traffic being carried in the Internet is difficult to estimate but Cisco [Cisco VNI 2011] estimates global Internet traffic will be nearly 40 exabytes per month in 2012.

Packet-switched networks (which transport packets) are in many ways similar to transportation networks of highways, roads, and intersections (which transport vehicles). Consider, for example, a factory that needs to move a large amount of cargo to some destination warehouse located thousands of kilometers away. At the factory, the cargo is segmented and loaded into a fleet of trucks. Each of the trucks then independently travels through the network of highways, roads, and intersections to the destination warehouse. At the destination warehouse, the cargo is unloaded and grouped with the rest of the cargo arriving from the same shipment. Thus, in many ways, packets are analogous to trucks, communication links are analogous to highways and roads, packet switches are analogous to intersections, and end systems are analogous to buildings. Just as a truck takes a path through the transportation network, a packet takes a path through a computer network.

End systems access the Internet through **Internet Service Providers (ISPs)**, including residential ISPs such as local cable or telephone companies; corporate ISPs; university ISPs; and ISPs that provide WiFi access in airports, hotels, coffee shops, and other public places. Each ISP is in itself a network of packet switches and communication links. ISPs provide a variety of types of network access to the end systems, including residential broadband access such as cable modem or DSL,

high-speed local area network access, wireless access, and 56 kbps dial-up modem access. ISPs also provide Internet access to content providers, connecting Web sites directly to the Internet. The Internet is all about connecting end systems to each other, so the ISPs that provide access to end systems must also be interconnected. These lower-tier ISPs are interconnected through national and international upper-tier ISPs such as Level 3 Communications, AT&T, Sprint, and NTT. An upper-tier ISP consists of high-speed routers interconnected with high-speed fiber-optic links. Each ISP network, whether upper-tier or lower-tier, is managed independently, runs the IP protocol (see below), and conforms to certain naming and address conventions. We'll examine ISPs and their interconnection more closely in Section 1.3.

End systems, packet switches, and other pieces of the Internet run **protocols** that control the sending and receiving of information within the Internet. The **Transmission Control Protocol (TCP)** and the **Internet Protocol (IP)** are two of the most important protocols in the Internet. The IP protocol specifies the format of the packets that are sent and received among routers and end systems. The Internet's principal protocols are collectively known as **TCP/IP**. We'll begin looking into protocols in this introductory chapter. But that's just a start—much of this book is concerned with computer network protocols!

Given the importance of protocols to the Internet, it's important that everyone agree on what each and every protocol does, so that people can create systems and products that interoperate. This is where standards come into play. **Internet standards** are developed by the Internet Engineering Task Force (IETF)[IETF 2012]. The IETF standards documents are called **requests for comments (RFCs)**. RFCs started out as general requests for comments (hence the name) to resolve network and protocol design problems that faced the precursor to the Internet [Allman 2011]. RFCs tend to be quite technical and detailed. They define protocols such as TCP, IP, HTTP (for the Web), and SMTP (for e-mail). There are currently more than 6,000 RFCs. Other bodies also specify standards for network components, most notably for network links. The IEEE 802 LAN/MAN Standards Committee [IEEE 802 2012], for example, specifies the Ethernet and wireless WiFi standards.

1.1.2 A Services Description

Our discussion above has identified many of the pieces that make up the Internet. But we can also describe the Internet from an entirely different angle—namely, as *an infrastructure that provides services to applications*. These applications include electronic mail, Web surfing, social networks, instant messaging, Voice-over-IP (VoIP), video streaming, distributed games, peer-to-peer (P2P) file sharing, television over the Internet, remote login, and much, much more. The applications are said to be **distributed applications**, since they involve multiple end systems that exchange data with each other. Importantly, Internet applications

ISP multi-homes, it can continue to send and receive packets into the Internet even if one of its providers has a failure.

As we just learned, customer ISPs pay their provider ISPs to obtain global Internet interconnectivity. The amount that a customer ISP pays a provider ISP reflects the amount of traffic it exchanges with the provider. To reduce these costs, a pair of nearby ISPs at the same level of the hierarchy can **peer**, that is, they can directly connect their networks together so that all the traffic between them passes over the direct connection rather than through upstream intermediaries. When two ISPs peer, it is typically settlement-free, that is, neither ISP pays the other. As noted earlier, tier-1 ISPs also peer with one another, settlement-free. For a readable discussion of peering and customer-provider relationships, see [Van der Berg 2008]. Along these same lines, a third-party company can create an **Internet Exchange Point (IXP)** (typically in a stand-alone building with its own switches), which is a meeting point where multiple ISPs can peer together. There are roughly 300 IXPs in the Internet today [Augustin 2009]. We refer to this ecosystem—consisting of access ISPs, regional ISPs, tier-1 ISPs, PoPs, multi-homing, peering, and IXPs—as *Network Structure 4*.

We now finally arrive at *Network Structure 5*, which describes the Internet of 2012. Network Structure 5, illustrated in Figure 1.15, builds on top of Network Structure 4 by adding **content provider networks**. Google is currently one of the leading examples of such a content provider network. As of this writing, it is estimated that Google has 30 to 50 data centers distributed across North America, Europe, Asia, South America, and Australia. Some of these data centers house over one hundred thousand servers, while other data centers are smaller, housing only hundreds of servers. The Google data centers are all interconnected via Google's private TCP/IP network, which spans the entire globe but is nevertheless separate from the public Internet. Importantly, the Google private network only

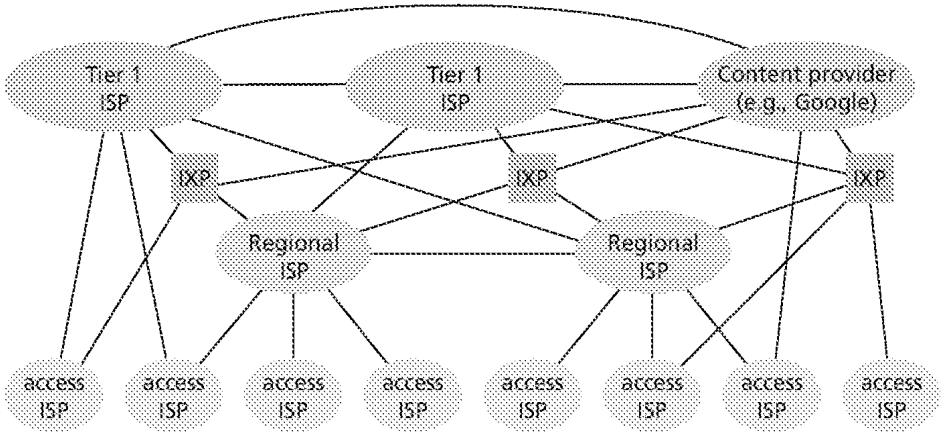


Figure 1.13 ◆ Interconnection of ISPs

carries traffic to/from Google servers. As shown in Figure 1.15, the Google private network attempts to "bypass" the upper tiers of the Internet by peering (settlement free) with lower-tier ISPs, either by directly connecting with them or by connecting with them at IXPs [Labovitz 2010]. However, because many access ISPs can still only be reached by transiting through tier-1 networks, the Google network also connects to tier-1 ISPs, and pays those ISPs for the traffic it exchanges with them. By creating its own network, a content provider not only reduces its payments to upper-tier ISPs, but also has greater control of how its services are ultimately delivered to end users. Google's network infrastructure is described in greater detail in Section 7.2.4.

In summary, today's Internet—a network of networks—is complex, consisting of a dozen or so tier-1 ISPs and hundreds of thousands of lower-tier ISPs. The ISPs are diverse in their coverage, with some spanning multiple continents and oceans, and others limited to narrow geographic regions. The lower-tier ISPs connect to the higher-tier ISPs, and the higher-tier ISPs interconnect with one another. Users and content providers are customers of lower-tier ISPs, and lower-tier ISPs are customers of higher-tier ISPs. In recent years, major content providers have also created their own networks and connect directly into lower-tier ISPs where possible.

1.4 Delay, Loss, and Throughput in Packet-Switched Networks

Back in Section 1.1 we said that the Internet can be viewed as an infrastructure that provides services to distributed applications running on end systems. Ideally, we would like Internet services to be able to move as much data as we want between any two end systems, instantaneously, without any loss of data. Alas, this is a lofty goal, one that is unachievable in reality. Instead, computer networks necessarily constrain throughput (the amount of data per second that can be transferred) between end systems, introduce delays between end systems, and can actually lose packets. On one hand, it is unfortunate that the physical laws of reality introduce delay and loss as well as constrain throughput. On the other hand, because computer networks have these problems, there are many fascinating issues surrounding how to deal with the problems—more than enough issues to fill a course on computer networking and to motivate thousands of PhD theses! In this section, we'll begin to examine and quantify delay, loss, and throughput in computer networks.

1.4.1 Overview of Delay in Packet-Switched Networks

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

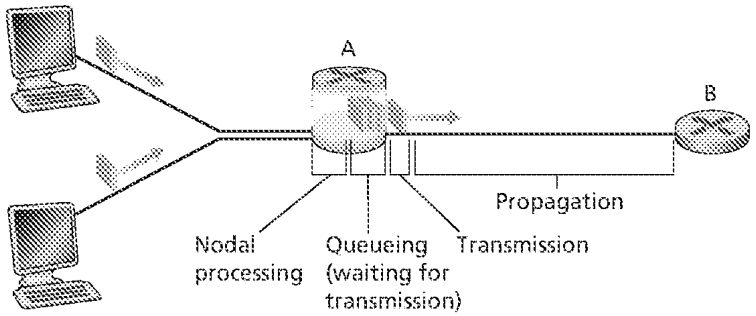


Figure 1.16 ◆ The nodal delay at router A

packet suffers from several types of delays at *each* node along the path. The most important of these delays are the **nodal processing delay, queuing delay, transmission delay,** and **propagation delay**; together, these delays accumulate to give a **total nodal delay**. The performance of many Internet applications—such as search, Web browsing, email, maps, instant messaging, and voice-over-IP—are greatly affected by network delays. In order to acquire a deep understanding of packet switching and computer networks, we must understand the nature and importance of these delays.

Types of Delay

Let's explore these delays in the context of Figure 1.16. As part of its end-to-end route between source and destination, a packet is sent from the upstream node through router A to router B. Our goal is to characterize the nodal delay at router A. Note that router A has an outbound link leading to router B. This link is preceded by a queue (also known as a buffer). When the packet arrives at router A from the upstream node, router A examines the packet's header to determine the appropriate outbound link for the packet and then directs the packet to this link. In this example, the outbound link for the packet is the one that leads to router B. A packet can be transmitted on a link only if there is no other packet currently being transmitted on the link and if there are no other packets preceding it in the queue; if the link is currently busy or if there are other packets already queued for the link, the newly arriving packet will then join the queue.

Processing Delay

The time required to examine the packet's header and determine where to direct the packet is part of the **processing delay**. The processing delay can also include other factors, such as the time needed to check for bit-level errors in the packet that occurred in transmitting the packet's bits from the upstream node to router A. Processing delays

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/014,746	05/03/2021	7523497	50348.65	9957

31718 7590 11/12/2021

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

EXAMINER	
LAROSE, COLIN M	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
11/12/2021	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE
SUITE 700
DALLAS, TX 75219

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/014,746* .

PATENT UNDER REEXAMINATION *7523497* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Office Action in Ex Parte Reexamination	**Control No.** 90/014,746	**Patent Under Reexamination** 7523497	
	Examiner Colin LaRose	**Art Unit** 3992	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

a. ☑ Responsive to the communication(s) filed on 17 August 2021.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

b. ☐ This action is made FINAL.

c. ☐ A statement under 37 CFR 1.530 has not been received from the patent owner.

A shortened statutory period for response to this action is set to expire 2 month(s) from the mailing date of this letter. Failure to respond within the period for response will result in termination of the proceeding and issuance of an *ex parte* reexamination certificate in accordance with this action. 37 CFR 1.550(d). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).** If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☐ Notice of References Cited by Examiner, PTO-892.
2. ☐ Information Disclosure Statement, PTO/SB/08.
3. ☐ Interview Summary, PTO-474.
4. ☐ _____.

Part II SUMMARY OF ACTION

1a. ☑ Claims 1,4,7,10,13 and 16 are subject to reexamination.
1b. ☑ Claims 2-3,5-6,8-9,11-12,14-15 and 17-18 are not subject to reexamination.
2. ☐ Claims _____ have been canceled in the present reexamination proceeding.
3. ☑ Claims 10 are patentable and/or confirmed.
4. ☑ Claims 1,4,7,13 and 16 are rejected.
5. ☐ Claims _____ are objected to.
6. ☐ The drawings, filed on _____ are acceptable.
7. ☐ The proposed drawing correction, filed on _____ has been (7a) ☐ approved (7b) ☐ disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the certified copies have
   1 ☐ been received.
   2 ☐ not been received.
   3 ☐ been filed in Application No. _____.
   4 ☐ been filed in reexamination Control No. _____.
   5 ☐ been received by the International Bureau in PCT application No. _____.
   * See the attached detailed Office action for a list of the certified copies not received.
9. ☐ Since the proceeding appears to be in condition for issuance of an *ex parte* reexamination certificate except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte* Quayle, 1935 C.D. 11, 453 O.G. 213.
10. ☐ Other: _____

cc: Requester (if third party requester)

NON-FINAL REJECTION (REEXAMINATION OF U.S. PATENT 7,523,497)

TABLE OF CONTENTS

I. ACKNOWLEDGEMENTS 2
II. STATUS OF CLAIMS 3
III. PRIORITY AND AIA STATUS 3
IV. PRIOR ART CITED HEREIN 4
V. RESPONSE TO PATENT OWNER'S STATEMENT AND REQUESTER'S REPLY 5
VI. DECLARATIONS CONSIDERED 7
VII. CLAIM INTERPRETATION – PHRASES INVOKING 35 U.S.C. § 112, SIXTH PARAGRAPH 8
VIII. CLAIM REJECTIONS – 35 USC § 102 (ANTICIPATION) 19
IX. CLAIM REJECTIONS – 35 USC § 103 (OBVIOUSNESS) 22
X. ALLOWABLE SUBJECT MATTER 25
XI. CONCLUSION 28

I. ACKNOWLEDGEMENTS

This non-final Office action addresses *ex parte* reexamination control no. 90/014,746 ("Instant Proceeding"). The Instant Proceeding is an *ex parte* reexamination of U.S. Patent No. 7,523,497 ("Patent Under Reexamination" or "'497 Patent") titled "PACKET FLOODING DEFENSE SYSTEM." The Patent Under Reexamination was filed on May 7, 2004 ("Non-Provisional Filing Date"), and assigned by the Office non-provisional U.S. patent application control number 10/841,064 ("Non-Provisional Application"), and issued on April 21, 2009, with claims 1-18 ("Originally Patented Claims").

On May 3, 2021, a third-party request to reexamine claims 1, 4, 7, 10, 13, and 16 was submitted ("Request").

On June 17, 2021, an order granting the request to reexamine the '497 Patent was issued in response to the Request ("Order").

On August 17, 2021, Patent Owner submitted an optional statement in response to the Order ("Patent's Owner Statement").

On October 15, 2021, Requester submitted a response to the Patent Owner's Statement ("Requester's Reply").

This non-final Office action is issued in response to the Patent Owner's Statement and Requester's Reply.

II. STATUS OF CLAIMS

Claims 1-18 are currently pending ("Pending Claims").

Claims 1, 4, 7, 10, 13, and 16 are currently examined ("Examined Claims").

Claims 2, 3, 5, 6, 8, 9, 11, 12, 14, 15, 17, and 18 are withdrawn from consideration.

Regarding the Examined Claims and as a result of this Office action:

Claims 1, 4, 13, and 16 are rejected under 35 U.S.C. § 102.

Claim 7 is rejected under 35 U.S.C. § 103.

Claim 10 is confirmed patentable.

III. PRIORITY AND AIA STATUS

Domestic Priority. Based upon a review of the '497 Patent, the Examiner finds that there is a claim for benefit of domestic priority under 35 U.S.C. §§ 120 or 119(e) to parent application

control no. 09/715,813 ("Parent Application"). To the extent the disclosure of the Parent Application supports the Pending Claims under 35 U.S.C. § 112, the supported claims receive benefit of an effective date of November 16, 2000, which is the filing date of the Parent Application.

AIA Status. Because the '497 Patent does not contain a claim having an effective date on or after March 16, 2013, the America Invents Act First Inventor to File ("AIA-FITF") provisions do not apply. Instead, the pre-AIA "First to Invent" provisions will govern this proceeding. See 35 U.S.C. § 100 (note). In the event the determination of the status of the application as subject to pre-AIA 35 U.S.C. §§ 102 and 103 is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

IV. PRIOR ART CITED HEREIN

The following prior art patents and printed publications are cited herein:

U.S. Patent 6,725,378 ("Schuba");

U.S. Patent 7,058,974 ("Maher"); and

"Practical Network Support for IP Traceback" ("Savage").

V. RESPONSE TO PATENT OWNER'S STATEMENT AND REQUESTER'S REPLY

Patent Owner's Optional Statement submitted August 17, 2021, and Requester's Reply submitted October 15, 2021, have been entered and considered.

Regarding the interpretation of claims 1, 4, 13, and 16, Requester notes that the Western District of Texas has issued a claim construction order in which the various means-plus-function terms of these claims were interpreted under 35 U.S.C. § 112, sixth paragraph, and were found to be indefinite. *See* Requester's Reply at pp. 15-16.

Based on an independent analysis of the claims, Examiner has determined that the various means-plus-function terms of claims 1, 4, 13, and 16 should be interpreted under § 112, sixth paragraph, and does not consider whether the claim are indefinite.[1] As explained below in Section VII, the recitation of "means" for executing a claimed function without reciting sufficient structure for performing the claimed function raises a presumption that the claimed element should be interpreted under § 112, sixth paragraph.

For purposes of examining claims 1, 4, 13, and 16 under 35 U.S.C. §§ 102 and 103 in light of Requester's cited prior art, the claims have been construed in accordance with § 112, sixth paragraph, and the corresponding structures of the various claimed means-plus-function elements are given below in Section VII.

Patent Owner's and Requester's remarks concerning claims 1, 4, 13, and 16 have been considered, but they are largely not applicable because they are based on the broadest reasonable

[1] In *ex parte* reexamination proceedings, compliance with 35 U.S.C. § 112, first and second paragraphs, are not issues that can be considered for original patent claims. *See* MPEP § 2258.II.

interpretation of claimed elements rather than the means-plus-function interpretation pursuant to § 112, sixth paragraph.

Claims 7 and 10 are method claims that are interpreted according to the broadest reasonable interpretation. According to Patent Owner, Savage allegedly does not disclose determining which packets are from attackers as opposed to non-attackers, and Savage allegedly does not disclose classifying packets into "wanted" and "unwanted" categories. *See* Patent Owner's Statement at pp. 5-8.

While these assertions appear to be true, Savage is not relied upon for such a teaching. As indicated in the § 103 rejection appearing below in Section IX, Maher is relied upon for teaching this limitation in claim 7, which recites, "classifying data packets … into wanted [] and unwanted data packets by path."

Maher is considered to teach this limitation of claim 7 inasmuch as Maher categorizes data packets as being "valid" versus "unverified" based at least on partial path information, such as the source of the packets. *See* Maher at, *e.g.*, columns 7:54–8:3. The amount of bandwidth ("quality of service") devoted to transmission of data packets is based on whether the packets are classified as valid or as unverified. *See id.* Maher's classification of data packets denotes which packets are "wanted" and which are "unwanted" in the sense that it is desirable and/or favorable for data packets to originate from valid sources, while it is undesirable and/or unfavorable for data packets to originate from unverified sources, and Maher devotes more bandwidth resources to the more desired/favored data packets than to the undesired/unfavored data packets.

Claim 10 is similar to claim 7, but the claim additionally specifies that the classifying of data packets is accomplished *via packet marks provided by routers leading to said host computer* by path.

As explained above, Maher teaches classifying data packets "by path" since the source of the packets is taken into consideration when classifying them. However, Maher does not appear to classify on the basis of packet marks provided by routers leading to said host computer, as claimed.

Savage does not appear to cure this deficiency because although Savage provides packet marks on data packets as they traverse various nodes, Savage is silent on performing any type of data packet classification.

Schuba, like Maher, classifies data packets on the basis of the source address and does not appear to take into consideration packet marks provided by routers. *See* Schuba at column 2:22-26 – "The corresponding source address of each SYN packet is classified in one of a plurality of different categories."

Accordingly, claim 10 is considered to distinguish from the combination of Maher and Savage, whereas claim 7 is rejected as being an obvious variant of Maher and Savage.

VI. DECLARATIONS CONSIDERED

On May 3, 2021, Requester submitted declarations by Dr. Vijay Madisetti (Exhibit 1003), Mr. Scott Delman (Exhibit 1009), Dr. Stefan Savage (Exhibit 1015), and Dr. Sylvia Hall-Ellis (Exhibit 1025). These declarations have been made of record and considered.

VII. CLAIM INTERPRETATION – PHRASES INVOKING 35 U.S.C. § 112, SIXTH PARAGRAPH

The following is a quotation of pre-AIA 35 U.S.C. 112, sixth paragraph:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

As explained in MPEP § 2181, subsection I, claim limitations that meet the following three-prong test will be interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph:

(A) the claim limitation uses the term "means" or a term used as a substitute for "means" that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning) for performing the claimed function;

(B) the term "means" or the generic placeholder is modified by functional language, typically, but not always linked by the transition word "for" (e.g., "means for") or another linking word or phrase, such as "configured to" or "so that"; and

(C) the term "means" or the generic placeholder is not modified by sufficient structure for performing the claimed function.

Use of the word "means" in a claim with functional language creates a rebuttable presumption that the claim limitation is to be treated in accordance with pre-AIA 35 U.S.C. § 112, sixth paragraph. The presumption that the claim limitation is interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph, is rebutted when the claim limitation recites sufficient structure to entirely perform the recited function.

Claim limitations in this application that use the word "means" are being interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph, except as otherwise indicated in an Office action. Conversely, claim limitations in this application that do not use the word "means" are not

being interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph, except as otherwise indicated in an Office action.

Such claim limitations that invoke § 112, sixth paragraph are:

Functional Phrase #1 (claim 1) – means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;

Functional Phrase #2 (claim 1) – means for associating a maximum acceptable processing rate with each class of data packet received at said computer;

Functional Phrase #3 (claim 1) – means for said computer to find information for packets it receives regarding the path by which said packets came to said 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; and

Functional Phrase #4 (claim 1) – means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate.

Functional Phrase #5 (claim 4) – means for classifying data packets received at a router into wanted data packets and unwanted data packets;

Functional Phrase #6 (claim 4) – means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

Functional Phrase #7 (claim 4) – means for said router to find information for packets it receives regarding the path by which said packets came to 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; and

Functional Phrase #8 (claim 4) – means in said router for said router to use said information to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable transmission rate.

Functional Phrase #9 (claim 13) – means for 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;

Functional Phrase #10 (claim 13) – means for classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;

Functional Phrase #11 (claim 13) – means for assigning a maximum acceptable processing rate to each class of data packet; and

Functional Phrase #12 (claim 13) – means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets.

Functional Phrase #13 (claim 16) – means for a router to determine a path by which said packets came to said router via packet marks provided by routers leading to said router; said path comprising all routers in said network via which said packets are routed to said computer;

Functional Phrase #14 (claim 16) – means for classifying data packets received at said router into wanted data packets and unwanted data packets by path;

Functional Phrase #15 (claim 16) – means for associating a maximum acceptable transmission rate with each class of data packet received at said router; and

Functional Phrase #16 (claim 16) – means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate.

Because these claim limitations are being interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph, they are being interpreted to cover the corresponding structure described in the specification as performing the claimed function, and equivalents thereof.

If Applicant does not intend to have any of these limitations interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph, Applicant may:

(1) amend the claim limitation(s) to avoid it/them being interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph (e.g., by reciting sufficient structure to perform the claimed function); or

(2) present a sufficient showing that the claim limitations recite sufficient structure to perform the claimed functions so as to avoid them being interpreted under pre-AIA 35 U.S.C. § 112, sixth paragraph.

Based upon a review of the '497 Patent, the Examiner concludes that the corresponding structures for the above-identified Functional Phrases are disclosed in the '497 Patent as follows:

Functional Phrase #1 (claim 1) – means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system includes means for classifying data packets 30 received at a host computer 18.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is

considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #2 (claim 1) – means for associating a maximum acceptable processing rate with each class of data packet received at said computer;

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system of FIG. 1 includes means for associating a maximum acceptable processing rate 34 with each class 38 of data packet 30 received at the computer 18.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #3 (claim 1) – means for said computer to find information for packets it receives regarding the path by which said packets came to said 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; and

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system of FIG. 1 includes means 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.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #4 (claim 1) – means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate.

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system of FIG. 1 includes a computer 18 that 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.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #5 (claim 4) – means for classifying data packets received at a router into wanted data packets and unwanted data packets;

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes means for classifying data packets 30 received at a router 22.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is

considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #6 (claim 4) – means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes means for associating a maximum acceptable processing rate 74 with each class 38 of data packet 30 received at the router 22.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #7 (claim 4) – means for said router to find information for packets it receives regarding the path by which said packets came to 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; and

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes means for the router 22 to find information for packets 30 it receives regarding the path 50 by which the packets 30 came to the router 22.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #8 (claim 4) – means in said router for said router to use said information to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable transmission rate.

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes a router 22 that can use the information to allocate the processing rate for each class 38 in a desired way.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #9 (claim 13) – means for 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;

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system of FIG. 1 includes means 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.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #10 (claim 13) – means for classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system includes means for classifying data packets 30 received at a host computer 18.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #11 (claim 13) – means for assigning a maximum acceptable processing rate to each class of data packet; and

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system of FIG. 1 includes means for associating a maximum acceptable processing rate 34 with each class 38 of data packet 30 received at the computer 18.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is

considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #12 (claim 13) – means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets.

– corresponds to a computer.

See the '497 Patent at column 6:1-25: the defense system of FIG. 1 includes a computer 18 that 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.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose computer, rather than a computer that has been specially programmed to execute the claimed function.

Functional Phrase #13 (claim 16) – means for a router to determine a path by which said packets came to said router via packet marks provided by routers leading to said router; said path comprising all routers in said network via which said packets are routed to said computer;

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes means for the router 22 to find information for packets 30 it receives regarding the path 50 by which the packets 30 came to the router 22.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is

considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #14 (claim 16) – means for classifying data packets received at said router into wanted data packets and unwanted data packets by path;

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes means for classifying data packets 30 received at a router 22.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #15 (claim 16) – means for associating a maximum acceptable transmission rate with each class of data packet received at said router; and

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes means for associating a maximum acceptable processing rate 74 with each class 38 of data packet 30 received at the router 22.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

Functional Phrase #16 (claim 16) – means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate.

– corresponds to a router.

See the '497 Patent at column 6:52-63: the defense system of FIG. 4 includes a router 22 that can use the information to allocate the processing rate for each class 38 in a desired way.

No special programming or algorithms for executing the claimed function appear to be disclosed in the specification of the '497 Patent, therefore, the corresponding structure is considered to be a general-purpose router, rather than a router that has been specially programmed to execute the claimed function.

If Applicant wishes to provide further explanation or dispute the Examiner's interpretation of the corresponding structure, Applicant must identify the corresponding structure with reference to the specification by page and line number, and to the drawing, if any, by reference characters in response to this Office action.

VIII. CLAIM REJECTIONS – 35 USC § 102 (ANTICIPATION)

The following is a quotation of the appropriate paragraphs of pre-AIA 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the

international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 4, 13, and 16 are rejected under 35 U.S.C. § 102(e) as being anticipated by Maher (U.S. 7,058,974).

Regarding **claim 1**, Maher discloses a packet flooding defense system (FIGS. 1a and 1b) for a network comprising a plurality of host computers (30), routers (22), communication lines (60) and transmitted data packets (*e.g.*, IP data), said system comprising:

one or more computers (30).

Note that the means-plus-function limitations of claim 1 have been interpreted in accordance with 35 U.S.C. § 112, sixth paragraph. As indicated above in Section VII, the corresponding structure for each of the means-plus-function limitations of claim 1 is a computer. Accordingly, claim 1 is interpreted as a packet flooding defense system that comprises one or more computers.

Regarding **claim 4**, Maher discloses a packet flooding defense system (FIGS. 1a and 1b) for a network comprising a plurality of host computers (30), routers (22), communication lines (60) and transmitted data packets (*e.g.*, IP data), said system comprising:

one or more routers (22).

Note that the means-plus-function limitations of claim 4 have been interpreted in accordance with 35 U.S.C. § 112, sixth paragraph. As indicated above in Section VII, the corresponding structure for each of the means-plus-function limitations of claim 4 is a router. Accordingly, claim 4 is interpreted as a packet flooding defense system that comprises one or more routers.

Regarding **claim 13**, Maher discloses a packet flooding defense system (FIGS. 1a and 1b) for a network comprising a plurality of host computers (30), routers (22), communication lines (60) and transmitted data packets (*e.g.*, IP data), said system comprising:

one or more computers (30).

Note that the means-plus-function limitations of claim 13 have been interpreted in accordance with 35 U.S.C. § 112, sixth paragraph. As indicated above in Section VII, the corresponding structure for each of the means-plus-function limitations of claim 13 is a computer. Accordingly, claim 13 is interpreted as a packet flooding defense system that comprises one or more computers.

Regarding **claim 16**, Maher discloses a packet flooding defense system (FIGS. 1a and 1b) for a network comprising a plurality of host computers (30), routers (22), communication lines (60) and transmitted data packets (*e.g.*, IP data), said system comprising:

one or more routers (22).

Note that the means-plus-function limitations of claim 16 have been interpreted in accordance with 35 U.S.C. § 112, sixth paragraph. As indicated above in Section VIIf, the corresponding structure for each of the means-plus-function limitations of claim 16 is a router. Accordingly, claim 16 is interpreted as a packet flooding defense system that comprises one or more routers.

IX. CLAIM REJECTIONS – 35 USC § 103 (OBVIOUSNESS)

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 7 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Maher (U.S. 7,058,974) in view of Savage ("Practical Network Support for IP Traceback").

Regarding **claim 7**, Maher discloses a method (FIG. 5) of providing packet flooding defense for a network (*see*, *e.g.*, FIGS. 1a and 1b) comprising a plurality of host computers (*i.e.*, webfarm 16 includes one or more network apparatuses, illustrated in FIGS. 2 and 4, performing host computing functions), routers (22), communication lines and transmitted data packets, said method comprising the steps of:

classifying data packets received at said host computer into wanted data packets and unwanted data packets by path (step 514; see also columns 7:54–8:3 – data packets received by a network apparatus (FIG. 2 or FIG. 4) are classified into valid ("wanted") and unverified ("unwanted") categories based on whether the packets are transmitted between known sources and destinations, *i.e.*, via a known path; the packets are considered "wanted" or "unwanted" to the extent that is it desirable or favorable for packets to flow between known sources and destinations, and it is undesirable or unfavorable for packets to flow from unverified sources);

associating a maximum acceptable processing rate with each class of data packet received at said host computer (*see* columns 7:54–8:3 and column 11:66–12:19 – the "wanted" class of

packets is given a high priority processing rate, i.e., "quality of service," whereas the "unwanted" class of packets is given a low priority processing rate); and

allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets (*see id.* – unwanted packets are given a lower processing rate than wanted packets).

Maher does not appear to expressly disclose the method includes:

"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," as claimed.

Savage discloses methods for combatting denial-of-service attacks that involve anonymous packet flooding (*see* Abstract). Savage teaches that is it conventional to employ "ingress filtering" in order to defend against anonymous attacks (*see* Section 2.1). Ingress filtering involves configuring routers to block packets that arrive with illegitimate source addresses (*see id.*). This is a similar prevention technique that is employed by Maher, which as explained above, teaches giving higher priority to traffic originating from verified sources, and giving lower priority to traffic from unverified sources.

Savage, however, identifies problems with ingress filtering. Notably, as traffic is aggregated from multiple ISPs into transmit networks, there is no longer enough information to unambiguously determine if an arriving packet originates from a valid, known source. Also, its effectiveness depends on widespread, if not universal, deployment, the overhead of ingress

filtering can become prohibitive on high-speed links, and even if universally deployed, attackers could still circumvent the filtering by forging addresses within a valid customer network. *See id.*

With these problems in mind, Savage proposes tracing flooding attacks by marking packets, either probabilistically or deterministically, with the addresses of the routers they traverse (*see* Section 3). For instance, a packet can be marked by appending the address of each node it traverses so that every received packet has a complete ordered list of the routers it traversed; this provides a complete path of the packet through a network and allows the receiver of the packet to trace the entire path back to its origin (*see* Section 4.1). Alternatively, probabilistic marking of only one node address can allow reconstruction of a complete traffic path from a given source when enough packets have been received (*see* Section 4.2).

It would have been obvious to those skilled in the art to modify Maher by Savage to achieve the claimed invention by determining a complete path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer, as claimed, since Savage teaches that providing a complete traceback of a received packet via marking at each traversed node is a more effective way to combat denial-of-service flooding attacks than the ingress filtering technique that is employed by Maher. Accordingly, Savage provides an express teaching and motivation to improve upon Maher's system by determining complete path information rather than simply filtering packets based on their source addresses.

X. CONFIRMED PATENTABLE CLAIM

Regarding **claim 10**, Maher discloses a method (FIG. 5) of providing packet flooding defense for a network (*see*, *e.g.*, FIGS. 1a and 1b) comprising a plurality of host computers (i.e., webfarm 16 includes webservers 30), routers (i.e., webfarm 16 includes one or more network apparatuses, illustrated in FIG. 4, performing host routing and computing functions), communication lines and transmitted data packets, said method comprising the steps of:

classifying data packets received at said router (step 514; see also columns 7:54–8:3 – data packets received by a network apparatus (FIG. 4) are classified into valid ("wanted") and unverified ("unwanted") categories based on whether the packets are transmitted between known sources and destinations, *i.e.*, via a known path; the packets are considered "wanted" or "unwanted" to the extent that is it desirable for packets to flow between known sources and destinations, and it is undesirable for packets to flow from unverified sources);

associating a maximum acceptable transmission rate with each class of data packet received at said router (*see* columns 7:54–8:3 and column 11:66–12:19 – the "wanted" class of packets is given a high priority processing rate, i.e., "quality of service," whereas the "unwanted" class of packets is given a low priority processing rate); and

allocating a transmission rate equal to or less than said maximum acceptable transmission rate for unwanted data packets (*see id.* – unwanted packets are given a lower processing rate than wanted packets).

Maher does not appear to expressly disclose the method includes:

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.

Also, Maher discloses classifying data packets received at said router but does not appear to disclose the classifying is done via packet marks provided by routers leading to said host computer by path, as claimed.

Savage discloses methods for combatting denial-of-service attacks that involve anonymous packet flooding (*see* Abstract). Savage teaches that is it conventional to employ "ingress filtering" in order to defend against anonymous attacks (*see* Section 2.1). Ingress filtering involves configuring routers to block packets that arrive with illegitimate source addresses (*see id.*). This is a similar prevention technique that is employed by Maher, which as explained above, teaches giving higher priority to traffic originating from verified sources, and giving lower priority to traffic from unverified sources.

Savage, however, identifies problems with ingress filtering. Notably, as traffic is aggregated from multiple ISPs into transmit networks, there is no longer enough information to unambiguously determine if an arriving packet originates from a valid, known source. Also, its effectiveness depends on widespread, if not universal, deployment, the overhead of ingress filtering can become prohibitive on high-speed links, and even if universally deployed, attackers could still circumvent the filtering by forging addresses within a valid customer network. *See id.*

With these problems in mind, Savage proposes tracing flooding attacks by marking packets probabilistically or deterministically, with the addresses of the routers they traverse (see Section 3). For instance, a packet can be marked by appending the address of each node it traverses so that every received packet has a complete ordered list of the routers it traversed; this provides a complete path of the packet through a network and allows the receiver of the packet to trace the entire path back to its origin (*see* Section 4.1). Alternatively, probabilistic marking of

only one node address can allow reconstruction of a complete traffic path from a given source when enough packets have been received (*see* Section 4.2).

It would have been obvious to those skilled in the art to modify Maher by Savage to determine a complete path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer, as claimed, since Savage teaches that providing a complete traceback of a received packet via marking at each traversed node is a more effective way to combat denial-of-service flooding attacks than the ingress filtering technique that is employed by Maher. Accordingly, Savage provides an express teaching and motivation to improve upon Maher's system by determining complete path information rather than simply filtering packets based on their source addresses.

However, neither Maher nor Savage appears to disclose or suggest the classifying of data packets is done "via packet marks provided by routers leading to said host computer by path," as claimed.

Maher is silent on the incorporation of router-provided packet marks, and therefore does not teach classifying the packets on such a basis.

Savage discloses utilizing router-provided packet marks in order to acquire complete traceback information for packets received by a victim. However, Savage does not appear to disclose using the router-provided packet marks for classifying the packets, as claimed. Rather, Savage only appears to be concerned with determining the path of received packets (the "traceback" problem) and does not seem to disclose any methods or algorithms for using the

router marking data to classify received packets in any manner, *e.g.* to distinguish between the packets from an attacker and the packets from a non-attacker.

For this reason, claim 10 is confirmed as patentable over the combination of Maher and Savage. Furthermore, Schuba does not appear to cure this deficiency in the teachings of Maher and Savage because Schuba's disclosure does not involve routers marking traversed packets, as claimed.

XI. CONCLUSION

In order to ensure full consideration of any amendments, affidavits or declarations, or other documents as evidence of patentability, such documents must be submitted in response to this Office action. Submissions after the next Office action, which is intended to be a final action, will be governed by the requirements of 37 CFR § 1.116, after final rejection and 37 CFR § 41.33 after appeal, which will be strictly enforced.

Extensions of time under 37 CFR § 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR § 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. § 305 requires that reexamination proceedings "will be conducted with special dispatch" (37 CFR § 1.550(a)). Extension of time in *ex parte* reexamination proceedings are provided for in 37 CFR § 1.550(c).

The patent owner is reminded of the continuing responsibility under 37 CFR § 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving Patent No. 7,523,497 throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Colin LaRose whose telephone number is 571-272-7423.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew J. Fischer can be reached at 571-272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-9900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

General inquiries may be directed to the Central Reexamination Unit customer service line at (571) 272-7705.

/COLIN M LAROSE/
Primary Examiner, Art Unit 3992

Conferees:

/NICK CORSARO/
Primary Examiner, Art Unit 3992

/ANDREW J. FISCHER/
Supervisory Patent Reexamination Specialist, Art Unit 3992

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,746	7523497
	Certificate Date	Certificate Number

Requester Correspondence Address: ☐ Patent Owner ☑ Third Party
HAYNES AND BOONE, LLP IP SECTION 2323 VICTORY AVENUE SUITE 700 DALLAS, TX 75219

LITIGATION REVIEW ☑	CML (examiner initials)	04 May 2021 (date)
Case Name		Director Initials
PacSec3, LLC v. NETSCOUT Systems, Inc, 6:20-cv-00914, W.D. TX.		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	**NUMBER**
n/a	

/COLIN M LAROSE/ Primary Examiner, Art Unit 3992	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,746	7523497
	Examiner	Art Unit
	Colin LaRose	3992

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
review prosecution history of U.S. 7,523,497	06/10/2021	CML

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/COLIN M LAROSE/ Primary Examiner, Art Unit 3992	

OPAP AKIMA-13
OCT 15 2021
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent of Donald N. Cohen	§	THIRD PARTY REQUESTER'S REPLY
U.S. Patent No. 7,523,497	§	
Filed: May 7, 2004	§	Attorney Docket No.: 50348.65
Issued: April 21, 2009	§	Customer No.: 27683
	§	Confirmation No. 9957
Title: PACKET FLOODING DEFENSE SYSTEM	§	Examiner: Colin M. Larose
Control No.: 90/014,746	§	

THIRD PARTY REQUESTER'S REPLY TO PATENT OWNER'S STATEMENT UNDER 37 C.F.R. § 1.535

Mail Stop *Ex Parte* Reexam
Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Third Party Requester, Unified Patents, LLC, respectfully submits this Reply under 37 C.F.R. § 1.535 to Patent Owner's Statement ("Statement") filed on August 17, 2021.

The Office issued an Order Granting Request for *Ex Parte* Reexamination ("Order") on June 17, 2021, finding that Third Party Requester's Request for *Ex*

Parte Reexamination ("Request") raised numerous substantial new questions ("SNQs") of patentability with respect to claims 1, 4, 7, 10, 13, and 16 ("challenged claims") of U.S. Patent No. 7,523,497 ("the '497 patent," EX1001). Patent Owner's Statement does not show that the challenged claims are patentable and does not show that the Office erred in finding that the Request raised numerous SNQs with respect to the challenged claims. Therefore, the Office should issue an Office Action rejecting the challenged claims in this reexamination proceeding.

TABLE OF CONTENTS

I. Introduction 4

II. *Savage* Raises an SNQ 5

III. Patent Owner's arguments against *Savage* Lack Merit 6

IV. Patent Owner's Arguments Against *Maher* and *Schuba* Lack Merit 11

V. Claim Construction 15

VI. Update in Parallel Litigation Involving '497 Patent 16

VII. List of Exhibits 17

VIII. Conclusion 20

IX. Certificate of Service 21

I. INTRODUCTION

None of Patent Owner's arguments in the Statement support termination of this reexamination. First, Patent Owner does not contest that *Savage* (EX1005), which was not considered during prosecution, teaches the allegedly allowable features of the challenged claims; this confirms that *Savage* raises an SNQ, as previously found. Instead, Patent Owner attempts to show nonobviousness by attacking the references individually, rather than analyzing the combination of references as set forth in the Request, but it is well-settled law that one cannot show nonobviousness by attacking references individually when the proposed rejections are based on a combination of references. Second, Patent Owner argues that *Savage* does not teach limitations of the challenged claims for which *Savage* was not cited in the Request. *See, e.g.*, Statement, 4-5 (arguing that *Savage* does not disclose limitations [1.1] and [1.2] when the Request shows that *Maher* (EX1006) teaches those limitations); 7-8 (arguing that *Savage* does not disclose limitations for which *Maher* and *Schuba* (EX1007) were cited). Finally, Patent Owner attempts to distinguish the claims from *Savage*, *Maher*, and *Schuba* by pointing to features not recited in the claims, which are irrelevant to the claims' obviousness. *See, e.g.*, Statement, 5 (arguing that *Savage* does not "resist packet flood attacks.") (capitalization removed).

Because none of the arguments in the Statement are persuasive, the Office

should issue an Office Action rejecting the challenged claims in this reexamination proceeding.

II. *SAVAGE* RAISES AN SNQ

The Request showed that *Savage* (EX1005) teaches the allegedly allowable features of challenged independent claims 1, 4, 7, 10, 13 and 16 of the '497 patent. Request, 24-28, 17-22 (identification of allowable subject matter during prosecution). In particular, the Request showed that *Savage* teaches limitations [1.3.1], [1.3.2], [4.3.1], [4.3.2], [7.1.1], [7.1.2], [10.1.1], [10.1.2], [13.1.1], [13.1.2], [16.1.1] and [16.1.2]. Request, 24-28, 51-57 (limitations [7.1.1]-[7.1.2]), 104-105 (limitations [13.1.1]-[13.1.2]), 112-115 (limitations [1.3.1]-[1.3.2]), 129-132 (limitations [10.1.1]-[10.1.2]), 143 (limitations [16.1.1]-[16.1.2]), and 149-153 (limitations [4.3.1]-[4.3.2]). Further, *Savage* was not considered during prosecution of the '497 patent. Request, 25.

The Office found that *Savage* raises an SNQ because "Savage appears to provide new technological teachings that were missing in the prior art during initial examination of the '497 patent and was not previously considered during the initial examination." Order, 4-5. Indeed, *Savage* expressly teaches the allegedly allowable feature of "said path comprising all routers in said network via which said packets are routed to said computer." Request, 25-28. Patent Owner acknowledges this teaching, admitting that *Savage* teaches that "every packet received by the victim

arrives with a complete ordered list of the routers it traversed—a built-in attack path." Statement, 4 (citing *Savage* (EX1005) at 299).

In the Statement, Patent Owner does not contest that *Savage* teaches the allegedly allowable features of claims 1, 4, 7, 10, 13 and 16; in fact, the Statement is completely silent on *Savage*'s teaching of the allegedly allowable features of the challenged claims. Patent Owner's silence is telling. *Savage* raises an SNQ, and Patent Owner has not refuted that fact.

III. PATENT OWNER'S ARGUMENTS AGAINST *SAVAGE* LACK MERIT

Rather than address the allegedly allowable features of the challenged claims, Patent Owner instead argues that "Savage does not teach how the packet marks and path denoted by the marks can be used **TO DEFEND AGAINST OR RESIST** packet flood attacks." Statement, 5 (emphasis original); *see also id.*, 7 (arguing that "There is counterpart in Savage that addresses defending the victim.") (emphasis removed), *id.* (arguing that *Savage* "does not disclose any method to detect when an attack may be taking place or how to defend against it."), 6 ("Savage does not disclose anything related to detection of or defenses against DDoS attacks."), 6-7 (arguing that *Savage* does not permit "an effective defense using the kind of packet marks advocated therein," and that *Savage* is concerned with "using the path information in the detected attack packets to TRACEBACK to the true source

address of the attack."). Patent Owner's arguments are incorrect for several reasons.

First, Patent Owner is improperly arguing against the references individually when the Request showed that the challenged claims are unpatentable over a combination of references: *Savage* (EX1005), *Maher* (EX1006), and *Schuba* (EX1007). Request, 35 (proposed rejection #1), 116 (proposed rejection #2). The preambles of claims 1, 4, 13, and 16 recite "[a] packet flooding defense system for a network," and the preambles of claims 7 and 10 recite "[a] method of providing packet flooding defense for a network." Third Party Requester showed that the preambles of claims 1, 4, 7, 10, 13 and 16, which are the only part of the claims that recite the word "defense," are obvious over *Savage* and *Maher*. *Maher* expressly discloses "[a] method and apparatus for **preventing denial of service type attacks** on data networks." *Maher* (EX1006), Abstract; *see also id.*, 1:8-10 ("method and device that **prevents denial of service type internet attacks**."), 2:52-53 ("method of **preventing DoS attacks**.") (emphases added); Request, 50. Likewise, *Schuba* teaches "a defense for denial of service attacks." *Schuba* (EX1007), 1:58-60; Request, 40. A person of ordinary skill in the art (POSITA) would have been motivated to modify *Savage* in view of *Maher* and *Schuba* for the reasons provided in Section III.A.4 of the Request (claims 1, 7, and 13), and would have been motivated to modify *Maher* in view of *Savage* and *Schbua* for the reasons provided in Section III.B.2 (claims 10, 14, and 16). Patent Owner has not rebutted any of

these reasons.

Patent Owner cannot show nonobviousness by attacking references individually when the proposed rejections are based on a combination of references. *See* MPEP § 2145(IV); *In re Keller*, 642 F.2d 413, 426 (Fed. Cir. 1981) ("one cannot show non-obviousness by attacking references individually where, as here, the rejections are based on combinations of references."). Thus, Patent Owner's arguments against *Savage* individually for allegedly not "teach[ing] how the packet marks and path denoted by the marks can be used to **DEFEND AGAINST OR RESIST** packet flood attacks" (Statement, 5 (emphasis original)) are without merit, when the Request showed that *Maher* expressly discloses "[a] method and apparatus for **preventing denial of service type attacks** on data networks." *Maher* (EX1006), Abstract; Request, 50. Likewise, Patent Owner argued that *Savage* individually does not disclose "defend[ing] against or resist[ing] packet flood attacks" (Statement, 5), "defending the victim" or "detect[ing] when an attack may be taking place or how to defend against it" (Statement, 7). However, as noted above, *Maher* expressly discloses defending against denial-of-service type attacks, and Requester explained that the combination of *Savage* and *Maher* renders obvious the preambles of claims 1, 4, 7, 10, 13 and 16, which are the only part of the claims that recite the word "defense." Request, 48-51 (limitation [7.0]), 101-104 (limitation [13.0]), 111 (limitation [1.0]), 127-129 (limitation [10.0]), 142 (limitation [16.0]), 148 (limitation

[4.0]).

Further, Patent Owner argues that *Savage* does not disclose the following limitations:

[1.1] means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;

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

[1.4] means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate.

Statement, 5-6.

But Patent Owner's arguments against *Savage* for limitations [1.1], [1.2], and [1.4] are without merit, because Patent Owner is again improperly attacking references individually when the proposed rejections are based on a combination of references. *See* MPEP § 2145(IV); *In re Keller*, 642 F.2d at 426 ("one cannot show non-obviousness by attacking references individually where, as here, the rejections are based on combinations of references."). Third Party Requester cited *Maher* and *Schuba* for teaching the limitations that Patent Owner argues are not taught by *Savage*. Request, 111-112 and 115-116 (analysis of limitations [1.1], [1.2] and [1.4], which refers to analysis of claim 7), 57-68 (analysis of limitation [7.2] citing *Maher*

and *Schuba*), 68-73 (analysis of limitation [7.3] citing *Maher*), and 73-76 (analysis of limitation [7.4] citing *Maher*). Third Party Requester cited *Savage*'s teaching for marking each packet with the router through which the packet traveled (the allegedly-allowable feature), so that "every packet received by the victim arrives with a complete ordered list of the routers it traversed—a built-in attack path." Request, 26 (quoting *Savage*, 299). The Request, supported by the declaration of Dr. Madisetti (EX1003), also showed why a POSITA would have been motivated to combine *Savage*, *Maher*, and *Schuba* to defend against packet flooding attacks. Request, 40-48, 118-127. But rather than address the obvious combination of references as set forth in the Request, Patent Owner improperly attacks the references individually, contrary to precedent. The Office should reject Patent Owner's erroneous attempt to show nonobviousness by attacking the references individually.

Second, Patent Owner is attempting to distinguish its claims by arguing features that are not recited in the claims. For example, Patent Owner argues that the '497 patent's disclosure of distributing a defense "among cooperating sites and routers," where "[t]he quality of defense is related to the size of the cooperating neighborhood," is not disclosed by *Savage*. Statement, 6. As yet another example, Patent Owner argues that "the cited elements of the '497 patent...are specific to detecting when an attack is ongoing and defending against it actively whether

attackers elect to cooperate with the victims or not." Statement, 8. As one more example, Patent Owner argues that the '497 patent "allocate[s] 'fair service' to every path through which traffic is being forwarded to the enterprise." Statement, 7. None of these features are recited in the claims. Patent Owner is improperly importing limitations from the specification that are not required by the challenged claims. *See* MPEP §§ 2111.01(II), 2145(VI) (*citing Constant v. Advanced Micro-Devices*, 848 F.2d 1560, 1571-72 (limitations not stated in the claims could not be used to establish patentability)); *see also SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) (citation omitted) ("[A] particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment."); *Hill-Rom Servs., Inc. v. Stryker Corp.*, 755 F.3d 1367, 1371 (Fed. Cir. 2014) ("While we read claims in view of the specification, of which they are a part, we do not read limitations from the embodiments in the specification into the claims."); *Comaper Corp. v. Antec, Inc.*, 596 F.3d 1343, 1348 (Fed. Cir. 2010) ("[T]his court has repeatedly cautioned against limiting claims to a preferred embodiment.").

IV. PATENT OWNER'S ARGUMENTS AGAINST *MAHER* AND *SCHUBA* LACK MERIT

Similar to its arguments against *Savage*, Patent Owner argues against *Maher* individually, without addressing the combination of *Savage* and *Maher*. For

instance, Patent Owner argues that "Maher does not disclose finding information regarding the path that the received packets traversed via packet-marking by routers along the path leading to the host computer (Order, at 6), not to mention 'said path comprising all routers in said network via which said packets are routed to said computer' as required by claims 4, 10, and 16 of the '497 patent." Statement, 9. Patent Owner's arguments about *Maher* are incorrect for at least two reasons.

First, the above-described features are taught by *Savage*. *See, e.g.*, Request, 51-56 (describing how *Savage* teaches the path-identification features of limitations [7.1.1] and [7.1.2]). Contrary to Patent Owner's argument above, Third Party Requester did not cite Maher to teach "finding information regarding the path that the received packets traversed via packet-marking by routers along the path leading to the host computer (Order, at 6), not to mention 'said path comprising all routers in said network via which said packets are routed to said computer' as required by claims 4, 10, and 16 of the '497 patent." Statement, 9.

Second, the Request relies on *Maher* and *Schuba* for teaching the feature of "classifying data packets received at said host computer into wanted data packets and unwanted data packets by path," as recited in limitation [7.3] (corresponding to limitations [4.1], [10.2], and [16.2]). For example, the Request showed how *Maher* and *Schuba* teach classifying data packets received at a host computer into wanted data packets and unwanted data packets. Request, 58; *see id.*, 58-61 (*Schuba* teaches

classifying data packets into wanted ("acceptable") or unwanted ("unacceptable") data packets by partial path information (source address)), and 61-65 (*Maher* teaches a quality of service processor that classified (qualifies) data based on the source and destination of packets (i.e., the path).) Yet the Statement merely attacks *Maher* individually without addressing how the combination of *Maher* and *Schuba*, with *Savage*, renders the claims obvious. Statement, 8-10 (attacking *Maher* individually).

Patent Owner repeats this error in Section D of the Statement, repeatedly arguing that individual limitations are not disclosed by individual references. Statement, 11-12. For instance, Patent Owner argues that the following limitations are not ***individually*** disclosed by *Savage*, *Maher*, or *Schuba* in a piecemeal fashion, despite the fact that Third Party Requester relied on the combination of *Savage*, *Maher*, and *Schuba* to show that these limitations are obvious.

In the Statement, Patent Owner argues that *Savage*, *Maher*, and *Schuba* individually do not disclose "classifying data packets received at a host computer into wanted data packets and unwanted data packets." Statement, 11-12. However, Third Party Requester showed that the combined teachings of *Maher* and *Schuba* render obvious the above-identified "classifying" limitation (i.e., limitation [7.2]).

Request, 57-68 (limitation [7.2]).[1]

Further, Patent Owner argued that *Savage* individually does not disclose "associating a maximum acceptable processing rate with each class of data packet received at said computer." Statement, 11. However, Third Party Requester showed that *Maher* teaches the above-identified "associating" limitation (i.e., limitation [7.3]). Request, 68-73 (limitation [7.3]).[2] Patent Owner has not contested that *Maher* teaches the "associating" limitation.

In addition, Patent Owner argued that *Savage* individually does not disclose "using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate." Statement, 11. However, Third Party Requester showed that *Maher* teaches the above-identified "allocat[ing]" limitation (i.e., limitation 7.4]). Request, 73-76

[1] For corresponding limitations [13.2], [1.1], [10.2], [16.2], and [4.1], *see* Request, 106 (limitation [13.2]), 111-112 (limitation [1.1]), 132 (limitation [10.2]), 143-145 (limitation [16.2]), and 148 (limitation [4.1]).

[2] For corresponding limitations [13.3], [1.2], [10.3], [16.3], and [4.2], *see* Request, 106-108 (limitation [13.3]), 112 (limitation [1.2]), 132-134 (limitation [10.3]), 145 (limitation [16.3]), and 149 (limitation [4.2]).

(limitation [7.4]).[3] Patent Owner has not contested that *Maher* teaches the "allocat[ing]" limitation.

Patent Owner's allegation that *Savage*, *Maher*, and *Schuba* in combination do not render obvious the challenged claims is thus based incorrectly on its flawed arguments that *Savage*, *Maher*, or *Schuba* **individually** do not teach the above limitations. For similar reasons as set forth in § III, *supra*, the Office should reject Patent Owner's erroneous attempt to show nonobviousness by attacking the references individually.

V. CLAIM CONSTRUCTION

After Patent Owner filed its Statement, the U.S. District Court for the Western District of Texas issued a Claim Construction Order (EX1046) in *PacSec3, LLC v. NETSCOUT Systems, Inc.*, No. 6:20-cv-00914. The district court found that several means-plus-function limitations in claims 1, 4, 13, and 16 are indefinite because the specification does not describe sufficient structure for performing the recited functions. *See* EX1046, 9-12.

Third Party Requester respectfully submits that the Office may still determine

[3] For corresponding limitations [13.4], [1.4], [10.4], [16.4], and [4.4], *see* Request, 108-109 (limitation [13.4]), 115-116 (limitation [1.4]), 134-135 (limitation [10.4]), 145-146 (limitation [16.4]), and 153 (limitation [4.4]).

whether the challenged claims are unpatentable over *Savage*, *Maher*, and *Schuba* independent of the district court's claim construction order. *See Samsung Elecs. Am., Inc. v. Prisua Eng'g Corp.*, 948 F.3d 1342, 1355 (Fed. Cir. 2020) (finding that even if the claims may be indefinite, "[i]t does not necessarily preclude the [Office] from addressing the patentability of the claims on section 102 and 103 grounds."). Likewise, the district court's claim construction order finding that claims 1, 4, 13, and 16 are indefinite because the specification does not describe sufficient structure for certain means-plus-function limitations does not preclude the Office from addressing the patentability of claims 1, 4, 13, and 16 on section 103 grounds.

VI. UPDATE IN PARALLEL LITIGATION INVOLVING '497 PATENT

After Patent Owner filed its Statement, the U.S. Court of Appeals for the Federal Circuit issued an Order (EX1047) instructing the District Court for the Western District of Texas in *PacSec3, LLC v. NETSCOUT Systems, Inc.*, No. 6:20-cv-00914, to transfer the case to the U.S. District Court for the Eastern District of Michigan. At the time of filing this Reply, the District Court for the Western District of Texas had not yet transferred the case to the U.S. District Court for the Eastern District of Michigan.

VII. LIST OF EXHIBITS

EX1001	U.S. Patent 7,523,497 by Donald N. Cohen ("'497 patent")
EX1002	Prosecution History of U.S. Patent 7,523,497 ("'497 FH")
EX1003	Declaration of Dr. Vijay Madisetti ("Madisetti")
EX1004	*Curriculum Vitae* of Dr. Vijay Madisetti
EX1005	Stefan Savage et al., "Practical Network Support for IP Traceback," ACM SIGCOMM 2000: Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2000, pp. 295-306 ("*Savage*")
EX1006	U.S. Patent 7,058,974 by Robert D. Maher, III ("Maher")
EX1007	U.S. Patent 6,725,378 by Christoph L. Schuba et al. ("Schuba")
EX1008	U.S. Patent 5,367,523 by Rong-Feng Chang et al. ("Chang")
EX1009	Declaration of Mr. Scott Delman
EX1010	U.S. Patent Application Publication 2002/0032871 by Gerald R. Malan et al. ("Malan")
EX1011	U.S. Patent 7,062,782 by Robert J. Stone et al. ("Stone")
EX1012	U.S. Patent 7,120,931 by David Cheriton ("Cheriton")
EX1013	U.S. Patent 6,502,135 by Edmund C. Munger et al. ("Munger")
EX1014	Plaintiff's Opening Claim Construction Brief, *PacSec3, LLC v. NetScout Systems, Inc.*, No. 6:20-cv-00914 (W.D. Tex.) (filed April 12, 2021) (Albright)
EX1015	Declaration of Dr. Stefan Savage
EX1016	*Curriculum Vitae* of Dr. Stefan Savage
EX1017	Program of ACM SIGCOMM 2000 Conference in Stockholm, Sweden, August 28, 2000 to September 1, 2000, available at http://conferences.sigcomm.org/sigcomm/2000/
EX1018	Internet Archive version (saved on August 20, 2000) of program of ACM SIGCOMM 2000 Conference in Stockholm, Sweden, August 28, 2000 to September 1, 2000, available at https://web.archive.org/web/20000820231540/ http://www.acm.org/sigcomm/sigcomm2000/conf/techprog.htm
EX1019	Reserved

EX1020	Stefan Savage et al., "Practical Network Support for IP Traceback," presentation slides presented at ACM SIGCOMM 2000 Conference on September 1, 2000
EX1021	Excerpt of *Computer Communication Review*, ACM SIGCOMM, Proceedings of ACM SIGCOMM 2000, Vol. 30, No. 4, Oct. 2000
EX1022	"About the ACM Organization," available at https://www.acm.org/about-acm/about-the-acm-organization
EX1023	"ACM SIGCOMM: Welcome," available at http://www.sigcomm.org/
EX1024	"SIGCOMM Conference," available at http://sigcomm.org/events/sigcomm-conference
EX1025	Declaration of Dr. Sylvia Hall-Ellis
EX1026	*Curriculum Vitae* of Dr. Sylvia Hall-Ellis
EX1027	U.S. Patent 6,789,190 by Donald N. Cohen
EX1028	Prosecution History of U.S. Patent 6,789,190
EX1029	Reserved
EX1030	Reserved
EX1031	Reserved
EX1032	Reserved
EX1033	Reserved
EX1034	Reserved
EX1035	Reserved
EX1036	K. Ramakrishnan et al., "A Proposal to add Explicit Congestion Notification (ECN) to IP," Network Working Group Request for Comments: 2481 (Jan. 1999), available at https://tools.ietf.org/html/rfc2481 ("RFC 2481")
EX1037	K. Nichols et al., "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," Networking Working Group Request for Comments: 2474 (Dec. 1998), available at https://tools.ietf.org/html/rfc2474 ("RFC 2474")
EX1038	S. Blake et al., "An Architecture for Differentiated Services," Network Working Group Request for Comments: 2475 (Dec. 1998), available at https://tools.ietf.org/html/rfc2475 ("RFC 2475")
EX1039	Ion Stoica et al., "Providing Guaranteed Services Without Per Flow Management," ACM SIGCOMM Computer Communication Review, Vol. 29,

	No. 4, Oct. 1999, pp. 81-94 ("Stoica")
EX1040	Excerpt of *ACM SIGCOMM 2000 Conference: Applications, Technologies, Architectures, and Protocols for Computer Communication*, Stockholm, Sweden, August 28, 2000 to September 1, 2000, obtained from University of Cincinnati Library
EX1041	K. Park et al., "A Proactive Approach to Distributed DoS Attack Prevention Using Route-Based Packet Filtering," Department of Computer Sciences, Purdue University, Dec. 3, 2000, available at https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/bibtex_archive/2001-40.pdf
EX1042	T. M. Gil, "Multops: a data structure for denial-of-service attack detection," Dissertation, Submitted to the Division of Mathematics and Computer Sciences of Vrije Universitei (Amsterdam, Netherlands), Dec. 27, 2000, available at https://thomer.com/mit/thesis.pdf
EX1043	P. Eronen, "Denial of service in public key protocols," Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, 2000, available at http://www.pasieronen.com/publications/netsec_2000.pdf
EX1044	"Internet Protocol – DARPA Internet Program Protocol Specification," IETF Network Working Group, Request for Comments: 791 (J. Postel ed., Sept. 1981), available at https://tools.ietf.org/html/rfc791 ("RFC 791")
EX1045	T. Socolofsky, "A TCP/IP Tutorial," Network Working Group Request for Comments 1180 (Jan. 1991), available at https://tools.ietf.org/html/rfc1180 ("RFC 1180")
EX1046 **(NEW)**	Claim Construction Order, *PacSec3, LLC v. NETSCOUT Systems, Inc.*, No. 6:20-cv-00914 (W.D. Tex. Sept. 9, 2021) (Albright)
EX1047 **(NEW)**	Order, *In re NetScout Systems, Inc.*, Appeal No. 21-173, Dkt. No. 18 (Fed. Cir. Oct. 13, 2021) (slip op.)

VIII. CONCLUSION

For the reasons set forth above and in the Request, the Office should issue an Office Action rejecting claims 1, 4, 7, 10, 13, and 16.

As identified in the attached Certificate of Service and in accordance with 37 C.F.R. §§ 1.33(c) and 1.510(b)(5), a copy of the present Reply, in its entirety, is being served to the address of the attorney or agent of record.

Please direct all correspondence in this matter to the undersigned.

Respectfully submitted,

October 15, 2021

/Raghav Bajaj/
Raghav Bajaj
Counsel for Third Party Requester
Registration No. 66,630

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence and any attachments are being deposited with the U.S. Postal Service on October 15, 2021 as Priority Mail Express bearing the label no. EE 258207684 US for submission with the U.S. Patent and Trademark on October 15, 2021.

/Lydia Epps-Hilliard/
Lydia Epps-Hilliard

IX. CERTIFICATE OF SERVICE

The undersigned certifies that copies of the following,

(1) Third Party Requester's Reply to Patent Owner's Statement Under 37 C.F.R. § 1.535; and

(2) Exhibits EX1046 and EX1047

in their entirety were served via First Class Mail on:

Belasco, Jacobs & Townsley, PC
6701 Center Drive West
14th Floor
Los Angeles, CA 90045

the attorney of record for the assignee of U.S. Patent No. 7,523,497, in accordance with 37 C.F.R. § 1.510(b)(5), on the 15th day of October 2021.

As a courtesy, the undersigned also certifies that copies of items (1) and (2) above were also served in their entirety on:

William P. Ramey III
Ramey & Schwaller, LLP
5020 Montrose Blvd., Ste. 800
Houston, TX 77006

the attorney who signed the Patent Owner Statement in this reexamination proceeding, on the 15th day of October 2021.

Dated: October 15, 2021

/Raghav Bajaj/
Raghav Bajaj
Counsel for Third Party Requester
Registration No. 57,456

EX1046

Claim Construction Order, PacSec3, LLC v. NETSCOUT Systems, Inc., No. 6:20-cv-00914 (W.D. Tex. Sept. 9, 2021) (Albright)

Customer No.: 27683

Haynes and Boone, LLP - Attorneys
IP Section, 2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651-5000
Fax [214] 200-0853

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

PACSEC3, LLC, *Plaintiff*	§	
	§	**NO. 6:20-CV-00914**
-v-	§	
NETSCOUT SYSTEMS, INC., *Defendants*	§	

CLAIM CONSTRUCTION ORDER

The Court held a *Markman* hearing on September 9, 2021. During that hearing, the Court provided its final constructions. The Court now enters those claim constructions.

SIGNED this 9th day of September, 2021.

ALAN D ALBRIGHT
UNITED STATES DISTRICT JUDGE

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Preliminary Construction
"means for classifying data packets received at said firewall" U.S. Patent No. 6,789,190, Claim 1 Jointly Proposed	§112, ¶6 does not apply, as a firewall is disclosed as the structure. If §112, ¶6 applies: **Function**: classifying data packets that are received at said firewall **Structure**: 1:57 to 2:4; 3:1 to 3:5; Fig 1: 4:54 to 4:59 and 5:37 to 5:51; Fig 4: 5:3 to 5:6 and 6:13 to 6:24; Fig 7: 5:18 to 5:22 and 6:55 to 7:3	§112, ¶6 applies. **Function**: classifying data packets received at said firewall **Structure**: The specification does not disclose sufficient structure. Indefinite.	§ 112, ¶ 6 applies **Function**: classifying data packets received at said firewall **Structure:** None. Indefinite due to lack of corresponding structure.

Cloudflare, Inc. Exhibit 1003 Page 210

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Preliminary Construction
"means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall" U.S. Patent No. 6,789,190, Claim 1 Jointly Proposed	§112, ¶6 does not apply, as a firewall is disclosed as the structure. If §112, ¶6 applies: **Function**: associating a maximum acceptable transmission rate received at said firewall said firewall **Structure**: 1:65 to 2:4; 3:6 to 3:12; Fig 1: 4:59 to 4:54 and 5:37 to 5:51; Fig 4: 5:3 to 5:6 and 6:13 to 6:24; Fig 7: 5:18 to 5:22 and 6:55 to 7:3	§112, ¶6 applies. **Function**: associating a maximum acceptable transmission rate with each class of data packet received at said firewall **Structure**: The specification does not disclose sufficient structure. Indefinite.	§ 112, ¶ 6 applies. **Function**: associating a maximum acceptable transmission rate with each class of data packet received at said firewall **Structure:** None. Indefinite due to lack of corresponding structure.

Cloudflare, Inc. Exhibit 1003 Page 211

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Preliminary Construction
"means for said firewall to find information for packets it receives regarding the path by which said packets came to said firewall" U.S. Patent No. 6,789,190, Claim 1 Jointly Proposed	§112, ¶6 does not apply, as a firewall is disclosed as the structure. If §112, ¶6 applies: **Function**: finding information for packets it receives regarding the path by which said packets came to said firewall **Structure**: 2:4 to 2:17; 3:6 to 3:12; 4:14 to 4:18; Fig 1: 4:59 to 4:54 and 5:37 to 5:51; Fig 4: 5:3 to 5:6 and 6:13 to 6:24; Fig 7: 5:18 to 5:22 and 6:55 to 7:3	§112, ¶6 applies. **Function**: finding information for packets it receives regarding the path by which said packets came to said firewall **Structure**: The specification does not disclose sufficient structure. Indefinite.	§ 112, ¶ 6 applies. **Function**: finding information for packets it receives regarding the path by which said packets came to said firewall **Structure**: None. Indefinite due to lack of corresponding structure.

Cloudflare, Inc. Exhibit 1003 Page 212

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Preliminary Construction
"means for classifying data packets received at said firewall related to the consumption of at least one resource" U.S. Patent No. 7,047,564, Claim 1 Jointly Proposed	§112, ¶6 does not apply, as a firewall is disclosed as the structure. If §112, ¶6 applies: **Function**: classifying data packets received at said firewall related to the consumption of at least one resource **Structure**: 3:18 to 3:20; 3:42 to 3:49; 4:46 to 4:50; 5:10 to 5:18; Figure 1 provides details	112, ¶6 applies. **Function**: classifying data packets received at said firewall related to the consumption of at least one resource **Structure**: The specification does not disclose sufficient structure. Indefinite.	§ 112, ¶ 6 applies. **Function**: classifying data packets received at said firewall related to the consumption of at least one resource **Structure**: The specification does not disclose sufficient structure. Indefinite.

Cloudflare, Inc. Exhibit 1003 Page 213

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Preliminary Construction
"means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall" U.S. Patent No. 7,047,564, Claim 1 Jointly Proposed	§112, ¶6 does not apply, as a firewall is disclosed as the structure. If §112, ¶6 applies: **Function**: associating a maximum acceptable transmission rate with each class of data packet received at said firewall **Structure**: 3:18 to 3:20; 3:42 to 3:49; 4:46 to 4:50; 5:10 to 5:31; Figure 1 provides details.	§112, ¶6 applies. **Function**: associating a maximum acceptable transmission rate with each class of data packet received at said firewall **Structure**: The specification does not disclose sufficient structure. Indefinite.	§ 112, ¶ 6 applies. **Function**: associating a maximum acceptable transmission rate with each class of data packet received at said firewall **Structure**: The specification does not disclose sufficient structure. Indefinite.

Cloudflare, Inc. Exhibit 1003 Page 214

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Preliminary Construction
"means for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet" U.S. Patent No. 7,047,564, Claim 1 Jointly Proposed	§112, ¶6 does not apply, as a firewall is disclosed as the structure. If §112, ¶6 applies: **Function**: limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet **Structure**: 3:18 to 3:20; 3:42 to 3:49; 4:46 to 4:50; 5:10 to 5:18; Figure 1 provides details	§112, ¶6 applies. **Function**: limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet **Structure**: The specification does not disclose sufficient structure. Indefinite.	§112, ¶ 6 applies. **Function**: limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet **Structure**: The specification does not disclose sufficient structure. Indefinite.
"means for said firewall to measure the amount of service requested by each packet" U.S. Patent No. 7,047,564, Claim 4 Jointly Proposed	§112, ¶6 does not apply as a firewall is disclosed as the structure. If §112, ¶6 applies: **Function**: measuring the amount of service requested by each packet **Structure**: 3:20 - 3:24; 4:17 - 4:23; 4:61 - 4:64; 5:62 - 5:64; Figure 4	§112, ¶6 applies. **Function**: measuring the amount of service requested by each packet **Structure**: The specification does not disclose sufficient structure. Indefinite.	§112, ¶ 6 applies. **Function**: measuring the amount of service requested by each packet **Structure**: The specification does not disclose sufficient structure. Indefinite

Cloudflare, Inc. Exhibit 1003 Page 215

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Preliminary Construction
"means for said firewall to measure the amount of service consumed in order to send each identified response data packet" U.S. Patent No. 7,047,564, Claim 5 Jointly Proposed	§112, ¶6 does not apply as a firewall is disclosed as the structure. If §112, ¶6 applies: **Function**: measuring, for the firewall, the amount of service of each type consumed to send each identified response data packet **Structure**: 3:24 - 3:27; 4:23 - 4:31; 4:65 - 5:03; 5:65 - 6:13; Figure 5	§112, ¶6 applies. **Function**: measuring the amount of service consumed in order to send each identified response data packet **Structure**: The specification does not disclose sufficient structure.	§112, ¶ 6 applies. **Function**: measuring the amount of service consumed in order to send each identified response data packet **Structure**: The specification does not disclose sufficient structure.

Cloudflare, Inc. Exhibit 1003 Page 216

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Preliminary Construction
"means for classifying data packets received at a/said host computer/router into wanted data packets and unwanted data packets/...by path" U.S. Patent No. 7,523,497, Claims 1, 4, 13, and 16 Jointly Proposed	§112, ¶6 does not apply, as a host computer/router is disclosed as the structure. If §112, ¶6 applies: **Function**: classifying data packets received at a host computer/router into wanted data packets and unwanted data packets/...by path **Structure**: 3:30 - 3:42; 5:29 - 5:33; 6:12 - 6:25; Figure 1; Figure 4; Figure 7	§112, ¶6 applies. **Function**: classifying data packets received at a/said host computer/router into wanted data packets and unwanted data packets/...by path **Structure**: The specification does not disclose sufficient structure. Indefinite.	§112, ¶ 6 applies. **Function**: classifying data packets received at a/said host computer/router into wanted data packets and unwanted data packets/...by path **Structure**: The specification does not disclose sufficient structure. Indefinite.
"means for associating a maximum acceptable [processing] / [transmission] rate with each class of data packet received at said [computer] / [router]" U.S. Patent No. 7,523,497, Claims 1, 4 Jointly Proposed	112, ¶6 does not apply, as a computer/router is disclosed as the structure. **Function**: associating a maximum acceptable processing/transmission rate with each class of data packet received at said computer/router **Structure**: 3:43-3:61; 5:33-5:39; 6:26-6:46; Figure 2; Figure 5; Figure 8	§112, ¶6 applies. **Function**: associating a maximum acceptable processing/transmission rate with each class of data packet received at said computer/router **Structure**: The specification does not disclose sufficient structure. Indefinite.	§ 112, ¶ 6 applies. **Function**: associating a maximum acceptable processing/transmission rate with each class of data packet received at said computer/router **Structure**: The specification does not disclose sufficient structure. Indefinite.

Cloudflare, Inc. Exhibit 1003 Page 217

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Preliminary Construction
"means for said [computer] / [router] to find information for packets it receives regarding the path by which said packets came to said [computer] / [router] via packet marks provided by routers leading to said host computer" U.S. Patent No. 7,523,497, Claims 1, 4 Jointly Proposed	§112, ¶ 6 applies. **Function**: finding information, for said computer/router, for packets received regarding the path by which said packets came to said router via packet marks provided by routers leading to said host computer **Structure**: 3:62 - 4:20; 5:40 - 5:44; 6:46 - 6:51; Figure 3; Figure 6; Figure 9	§112, ¶6 applies. **Function**: finding information for packets it receives regarding the path by which said packets came to said computer/router via packet marks provided by routers leading to said host computer **Structure**: The specification does not disclose sufficient structure. Indefinite.	§ 112, ¶6 applies. **Function**: finding information for packets it receives regarding the path by which said packets came to said computer/router via packet marks provided by routers leading to said host computer **Structure**: The specification does not disclose sufficient structure. Indefinite.
[means in said computer for using] / [means in said router for said router to use] said information to allocate the [processing] / [transmission] rate available for unwanted data packets to be less than or equal to said maximum acceptable [processing] / [transmission] rate U.S. Patent No. 7,523,497, Claims 1, 4 Jointly Proposed	§112, ¶6 applies. **Function**: allocating the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate **Structure**: 3:30 - 3:42; 5:29 - 5:33; 6:12 - 6:25; Figure 1; Figure 4; Figure 7	§112, ¶6 applies. **Function**: using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate **Structure**: The specification does not disclose sufficient structure. Indefinite.	§ 112, ¶ 6 applies. **Function**: using said information to allocate the [processing] / [transmission] rate available for unwanted data packets to be less than or equal to said maximum acceptable [processing] / [transmission] rate **Structure**: The specification does not disclose sufficient structure. Indefinite.

Cloudflare, Inc. Exhibit 1003 Page 218

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Preliminary Construction
means for [determining] / [a router to determine] a path by which data packets [arrive at a host computer] / [came to said router] via packet marks provided by routers leading to said [host computer] / [router] U.S. Patent No. 7,523,497, Claims 13, 16 [Jointly Proposed]	§112, ¶6 does not apply, as a router is disclosed as the structure. If §112, ¶6 applies: **Function**: determining a path by which data packets arrive at a host computer/router via packet marks provided by routers leading to said host computer **Structure**: 3:30-3:42; 5:29-5:33; 6:12- 6:25; Figure 1; Figure 4; Figure 7	§112, ¶6 applies. **Function**: determining a path by which data packets arrive at a host computer/router via packet marks provided by routers leading to said host computer **Structure**: The specification does not disclose sufficient structure. Indefinite.	§ 112, ¶ 6 applies. **Function**: determining a path by which data packets arrive at a host computer/router via packet marks provided by routers leading to said host computer/router **Structure**: The specification does not disclose sufficient structure. Indefinite.
means for [assigning] / [associating] a maximum acceptable [processing] / [transmission] rate to each class of data packet U.S. Patent No. 7,523,497, Claims 13, 16 Jointly Proposed	§112, ¶6 applies. **Function**: assigning/associating a maximum acceptable processing rate to each class of data packet **Structure**: 3:30 - 3:42; 5:29 - 5:33; 6:12 - 6:25; Figure 1; Figure 4; Figure 7	§112, ¶6 applies. **Function**: assigning a maximum acceptable processing rate to each class of data packet **Structure**: The specification does not disclose sufficient structure. Indefinite.	§ 112, ¶ 6 applies. **Function**: [assigning] / [associating] a maximum acceptable [processing] / [transmission] rate to each class of data packet **Structure**: The specification does not disclose sufficient structure. Indefinite.

Cloudflare, Inc. Exhibit 1003 Page 219

Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Preliminary Construction
means for [allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets] / [said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate] U.S. Patent No. 7,523,497, Claims 13, 16 Jointly Proposed	§112, ¶6 does not apply, as a router is disclosed as the structure. If §112, ¶6 applies: **Function**: allocating a processing rate that is equal to or less than said maximum acceptable processing rate to said unwanted data packets **Structure**: 3:30 - 3:42; 5:29 - 5:33; 6:12 - 6:25; Figure 1; Figure 4; Figure 7	§112, ¶6 applies. **Function**: allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets **Structure**: The specification does not disclose sufficient structure. Indefinite.	§ 112, ¶ 6 applies. **Function**: allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets **Structure**: The specification does not disclose sufficient structure. Indefinite.
"router" U.S. Patent No. 7,523,497, Claims 1, 4, 7, 10, 13, 16 Proposed by Defendant	Plain and ordinary meaning	"a device that determines the optimal path along which communications traffic should be forwarded and that is not a firewall"	Plain and ordinary meaning
"host computer" U.S. Patent No. 7,523,497, Claims 1, 4, 7, 10, 13, 16 Proposed by Defendant	Plain and ordinary meaning	"a computer that processes data through the application layer and that is not a firewall"	Plain and ordinary meaning

Cloudflare, Inc. Exhibit 1003 Page 220

EX1047

Order, In re NetScout Systems, Inc., Appeal No. 21-173, Dkt. No. 18 (Fed. Cir. Oct. 13, 2021) (slip op.)

Customer No.: 27683

Haynes and Boone, LLP - Attorneys
IP Section, 2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651-5000
Fax [214] 200-0853

NOTE: This order is nonprecedential.

United States Court of Appeals for the Federal Circuit

In re: NETSCOUT SYSTEMS, INC.,
Petitioner

2021-173

On Petition for Writ of Mandamus to the United States District Court for the Western District of Texas in No. 6:20-cv-00914-ADA, Judge Alan D. Albright.

ON PETITION AND MOTION

Before LOURIE, BRYSON, and TARANTO, *Circuit Judges*.

PER CURIAM.

ORDER

NetScout Systems, Inc., petitions for a writ of mandamus directing the United States District Court for the Western District of Texas to transfer this action to the United States District Court for the Eastern District of Michigan. PacSec3, LLC, opposes the petition and moves for leave to file its response out of time. NetScout replies. For the following reasons, we grant the petition.

I

On October 2, 2020, PacSec3 brought this patent infringement action in the Waco Division of the Western District of Texas. PacSec3 filed the action shortly after incorporating in Texas and acquiring the asserted patents, which concern network firewalls. App. 120. PacSec3 does not have an office or employee in the Western District of Texas. Its only employee is located in the Southern District of Texas, App. 112, 118.

In December 2020, NetScout moved to transfer this case to the Eastern District of Michigan pursuant to 28 U.S.C. § 1404(a). NetScout noted that the accused products were designed and developed by its security division in Ann Arbor, Michigan, where its core technical documents and source code are located. App. 40–42. NetScout noted that engineers knowledgeable about the design, development, and operation of the accused products, including NetScout's Vice President of Engineering, Scott Dawson, work from Ann Arbor, Michigan. App. 41. NetScout also identified two of its employees from its headquarters in Massachusetts who are knowledgeable about NetScout's relevant financial and marketing information. *Id.* NetScout stated that none of the design or development work on the accused products was conducted in its sole Texas facility, which is located in the Eastern District of Texas. *Id.* at 42.

In its response opposing the transfer motion, PacSec3 argued that judicial economy favored denying the motion. In support of that argument, PacSec3 argued that it had filed additional related lawsuits in the Western District of Texas after the transfer motion was filed in this case. Those cases alleged that different defendants had infringed the same patents that are asserted in this case. *See PacSec3, LLC v. Juniper Networks, Inc.*, No. 6:21-cv-00387-ADA (filed Apr. 21, 2021); *PacSec3, LLC v. Cisco Sys., Inc.*, No. 6:21-cv-00388-ADA (filed Apr. 21, 2021); *PacSec3, LLC*

v. Watchguard Techs., Inc., No. 6:21-cv-00633-ADA (filed June 18, 2021).*

The district court denied NetScout's motion to transfer the case. At the outset, the court found that this action could have been brought in the Eastern District of Michigan. The district court then analyzed NetScout's transfer motion by applying the set of private-interest and public-interest factors that the Fifth Circuit has directed courts to use in making transfer decisions under section 1404(a). *See In re Volkswagen of Am., Inc.*, 545 F.3d 304 (5th Cir. 2008) (en banc) ("*Volkswagen II*").

The district court took particular note of five of the factors that the Fifth Circuit has identified as bearing on transfer: (1) the relative ease of access to sources of proof between the forums; (2) the relative convenience of the two forums for potential witnesses; (3) practical issues that may make trial of a case easier, more expeditious, and less expensive in one of the forums; (4) the administrative difficulties flowing from court congestion; and (5) the local interest in having disputes regarding activities occurring principally within a particular district decided by a court within that district.

As for the sources of proof, the district court recognized that NetScout had attested to the fact that the great bulk of its documentary evidence was located in the Eastern District of Michigan. However, the court found that NetScout had failed to "specifically identify what documents are in physical form and what documents are in clcctronic form," and had failed to explain why documents in physical form could not be made available electronically from NetScout's offices in the Eastern District of Texas. App. 115. For that

---

* The *Cisco* case was voluntarily dismissed with prejudice on June 23, 2021. App. 132.

reason, the district court found that the sources-of-proof factor favored neither venue.

With regard to the relative convenience of the two forums for potential witnesses, the court recognized that at least one NetScout witness, Scott Dawson, resides in the Eastern District of Michigan while no party identified any prospective witnesses located in the Western District of Texas. Nonetheless, the court concluded that the convenience of the witnesses did not weigh in favor of either venue. In particular, the court explained that in its view "the convenience of party witnesses" is generally entitled to "little weight." *Id.* at 117 (internal quotation marks and citation omitted). The court found that the non-party witnesses who are in California would find either venue equally convenient. *Id.* at 118.

With regard to the practical issues that bear on the convenience and cost of a trial, the district court took note of the infringement cases that PacSec3 had filed in the Western District of Texas asserting the same patents against other defendants. Those cases were filed after NetScout filed its motion to transfer. *Id.* at 119. Based on the fact that the cases shared overlapping patents, the court presumed that all the cases would involve overlapping claim construction, invalidity, prior art, conception, and reduction to practice issues. *Id.* Because keeping the case against NetScout in the Western District of Texas would allow one trial judge to oversee those issues in all of PacSec3's filed cases, the district court found that the interests of judicial economy weighed strongly against transferring the case. *Id.*

The court recognized that the Eastern District of Michigan had a greater local interest in this dispute because the accused products resulted from research and development that took place in that district. Moreover, the court noted that PacSec3 was only recently formed and associated with

Texas. *Id.* at 120. The district court concluded, however, that the court congestion factor weighed strongly against transfer because the court in the Western District of Texas would be likely to reach trial more quickly than would a court in the Eastern District of Michigan. *Id.* at 119–20.

The district court found that the remaining factors were neutral. Taking into account the weight it assigned to each of the factors, the district court concluded that NetScout had failed to show that the Eastern District of Michigan was a clearly more convenient forum for this litigation. Accordingly, the district court denied the transfer motion.

II

Our review of transfer rulings is governed by the law of the regional circuit, which in this case is the Fifth Circuit. *See In re TS Tech USA Corp.*, 551 F.3d 1315, 1319 (Fed. Cir. 2008). Under Fifth Circuit law, the governing principles are well settled. Section 1404(a) authorizes a court to transfer a civil action "[f]or the convenience of parties and witnesses, in the interest of justice[.]" Fifth Circuit law provides that a motion to transfer should be granted if "the movant demonstrates that the transferee venue is clearly more convenient." *In re Radmax, Ltd.*, 720 F.3d 285, 288 (5th Cir. 2013) (quoting *Volkswagen II*, 545 F.3d at 315) (internal quotation marks omitted).

A district court enjoys broad discretion in making a transfer determination. *See In re Vistaprint Ltd.*, 628 F.3d 1342, 1344 (Fed. Cir. 2010). We have explained, however, that our deference does not exempt transfer determinations from scrutiny on mandamus. *In re Samsung Elecs. Co.*, 2 F.4th 1371, 1379 (Fed. Cir. 2021). When a court's denial of a motion to transfer under section 1404(a) contravenes governing legal standards, we have issued mandamus to overturn the denial of transfer. *See, e.g.*, *In re Apple Inc.*, 979 F.3d 1332 (Fed. Cir. 2020). Based on a close study of the record in this case, we conclude that the court clearly

abused its discretion in finding that NetScout failed to make the requisite showing to call for transfer of this case to the Eastern District of Michigan.

A

The district court's determination that the Eastern District of Michigan had a greater local interest in this case than the Western District of Texas is amply supported. It is undisputed that the events that form the basis for PacSec3's infringement contentions occurred in the Eastern District of Michigan where the accused products were developed. *See Apple*, 979 F.3d at 1345 (noting that this factor "most notably regards . . . the 'significant connections between a particular venue and *the events that gave rise to a suit*.'" (quoting *In re Acer Am. Corp.*, 626 F.3d 1252, 1256 (Fed. Cir. 2010)) (emphasis in *Apple*).

The district court also correctly determined that PacSec3's connections to Texas were recent and insubstantial. The record shows that PacSec3 was formed just a week before its acquisition of the asserted patents and less than two months before filing this lawsuit. Moreover, PacSec3 is based in the Southern District of Texas, not the Western District of Texas. Its connections to the forum plainly do not give the Western District of Texas any significant local interest in resolving this litigation. *See In re Juniper Networks, Inc.*, No. 2021-160, 2021 WL 4343309, at *5 (Fed. Cir. Sept. 24, 2021); *In re Samsung Elecs. Co.*, 2 F.4th 1371, 1365 (Fed. Cir. 2021); *In re Zimmer Holdings, Inc.*, 609 F.3d 1378, 1381 (Fed. Cir. 2010) (party's presence in Texas "appears to be recent, ephemeral, and an artifact of litigation.").

B

The district court clearly erred in its assessment that the convenience of the witnesses was a neutral factor in the transfer analysis. The Fifth Circuit has stated that the convenience of the witnesses is best served if the court can

"minimize the time when [witnesses] are removed from their regular work or home responsibilities." *In re Volkswagen AG*, 371 F.3d 201, 205 (5th Cir. 2004). That task "gets increasingly difficult and complicated when the travel time from [the witnesses'] home or work site to the court facility is five or six hours one-way as opposed to 30 minutes or an hour." *Id.*; *see also In re Google LLC*, No. 2021-170, 2021 WL 4427899, at *4 (Fed. Cir. Sept. 27, 2021) ("In light of the purpose underlying the rule, the inquiry should focus on the cost and inconvenience imposed on the witnesses by requiring them to travel to a distant forum and to be away from their homes and work for an extended period of time.").

Those principles are not, as the district court viewed them, applicable only to non-party witnesses. As we have held, the fact that witnesses are affiliated with a party "does not negate the inconvenience and cost to those individuals to travel a significant distance to testify." *Google*, 2021 WL 4427899, at *4; *see also Samsung*, 2 F.4th at 1379 (holding that a district court's section 1404(a) analysis "must consider" the convenience of "possible party witnesses"); *In re Hulu, LLC*, No. 2021-142, 2021 WL 3278194, at *5 (Fed. Cir. Aug. 2, 2021); *In re Apple Inc.*, 818 F. App'x 1001, 1003 (Fed. Cir. 2020) (rejecting the view that the convenience of party witnesses is given "little weight"). We have likewise rejected the categorical assumption, made by the district court in this case, that defendants are likely to call few, if any, of the proposed party witnesses who are identified in support of a transfer motion. *Juniper Networks*, 2021 WL 4343309, at *4.

PacSec3 argues that its sole employee would be more inconvenienced by having to travel to the Eastern District of Michigan rather than to Waco, Texas. That witness, however, does not live in the Western District of Texas and would have to travel close to three hours to reach either forum. App. 97. The district court did not attach weight to the convenience of that witness. *Id.* at 118.

The district court also rejected PacSec3's argument that the Western District of Texas would be more convenient for three non-party witnesses in California, who are roughly equidistant from both the transferor and transferee forums. And with regard to PacSec3's contention that a number of NetScout's customers are located in Texas, the court ruled that PacSec3 had not established that any specific employees of those companies would be trial witnesses. *Id.* at 117. Those determinations have not been shown to be incorrect.

By contrast, NetScout explained that its engineers who designed and worked on the accused products are located in the Eastern District of Michigan. NetScout identified at least one engineer by name, Mr. Dawson, who resides there and who would likely be called as a witness. NetScout also identified two employees who work from NetScout's headquarters in Massachusetts and who have knowledge pertinent to the case. Those witnesses undisputedly would find trial in the Eastern District of Michigan more convenient. While PacSec3 contends that there are employees of NetScout in Texas that are knowledgeable about the accused products, it does not identify those individuals, and the district court did not find they have relevant information.

Accordingly, NetScout has shown that the Eastern District of Michigan is clearly the more convenient venue for the identified witnesses, and PacSec 3 has not shown that the Western District of Texas is the more convenient venue for any witnesses. The district court therefore erred in not finding that the convenience of the witnesses favors transfer. *See Samsung*, 2 F.4th at 1379.

C

The district court also erred in its assessment of the sources of proof. That inquiry focuses on "the relative access to sources of evidence in the two competing forums," *Juniper Networks*, 2021 WL 4343309, at *6. Yet here, no

sources of proof are in located in the Western District of Texas. By contrast, there is no dispute that significant documents and source code were created and are maintained in the Eastern District of Michigan. While electronic storage makes documents more widely accessible than was true in the past, the fact that documents can often be accessed remotely does not render the sources-of-proof factor irrelevant. *See Volkswagen II*, 545 F.3d at 316 ("That access to some sources of proof presents a lesser inconvenience now than it might have absent recent developments does not render this factor superfluous."). The district court thus erred in not weighing this factor at least slightly in favor of transfer.

D

The district court also erred in weighing the practical problems factor significantly against transfer. At the time of the complaint and even at the time of NetScout's transfer motion in December 2020, there was no judicial economy benefit to keeping this case in the Western District of Texas. PacSec3 did not file the first of the other Texas actions relied on by the district court until April 2021. In previous cases, we have rejected a district court's reliance on considerations of judicial economy arising after the filing of the lawsuit or the transfer motion as irrelevant to the analysis. *In re HP Inc.*, 826 F. App'x 899, 903 n.2 (Fed. Cir. 2020); *In re EMC Corp.*, 501 F. App'x 973, 976 (Fed. Cir. 2013).

PacSec3 asks us to reject those cases as non-binding and contends that giving significant weight to post-motion events furthers the purposes of section 1404(a). We are not persuaded. To the extent that post-motion events may ever be considered in a section 1404(a) analysis, we must guard against manipulative measures designed to defeat transfer to a more convenient venue. *See Van Dusen v. Barrack*, 376 U.S. 612, 624 (1964); *Samsung*, 2 F.4th at 1378 ("We have similarly rejected parties' attempts to manipulate

venue."). PacSec3's infringement action against NetScout lacks any legitimate mooring to the Western District of Texas. To allow PacSec3 to defeat transfer to a more convenient forum by assigning significant weight to PacSec3's other actions, filed after the transfer motion was filed in this case, would invite venue manipulation.

Beyond that, while we recognize that judicial economy can serve important ends in a transfer analysis, we have rejected as a general proposition that the mere co-pendency of infringement suits in a particular district automatically tips the balance in the non-movant's favor. *See In re Google Inc.*, No. 2017-107, 2017 WL 977038, at *2 (Fed. Cir. Feb. 23, 2017); *see also Samsung*, 2 F.4th at 1379–80 (concluding that the district court erred in allowing judicial economy concerns to outweigh convenience); *EMC*, 501 F. App'x at 976. Here, PacSec3's other actions in the Western District of Texas involve different defendants and different accused products. They are therefore likely to involve significantly different discovery and evidence. Any judicial economy considerations would be insufficient to outweigh the clear benefits of transfer in light of the imbalance in the parties' respective presentations on the other private-interest and public-interest factors.

E

Finally, we disagree with the district court that court congestion analysis provides a basis for denying transfer. The district court did not find an appreciable difference in the degree of docket congestion between the two forums. *See Juniper Networks*, 2021 WL 4343309, at *6. Nor did the court point to any reason that a more rapid disposition of this case that might be available in Texas is worthy of important weight. *Id.* Instead, the court based its finding as to the court congestion factor solely on the median time to trial between the districts. We reject that rationale for denying transfer.

We have held that when other relevant factors weigh in favor of transfer or are neutral, "then the speed of the transferee district court should not alone outweigh all of those other factors." *In re Genentech, Inc.*, 566 F.3d 1338, 1347 (Fed. Cir. 2009). And where, as here, the court has relied only on median time-to-trial statistics to support its conclusion, we have characterized this factor as the "most speculative" of the factors bearing on the transfer decision. *Id.* Speculation about what might happen with regard to the speed of adjudication in a particular case is insufficient to warrant denying transfer to a more convenient forum.

F

In sum, the center of gravity of this action lies in the transferee district, and decidedly not in the Western District of Texas. Several of the most important factors bearing on the transfer decision favor transferring the case, and no factor favors retaining the case in the Western District of Texas. In fact, there is nothing at all that ties this case to the Western District of Texas: no witnesses reside there; no evidence is present there; and none of the conduct giving rise to this action took place there. The only apparent connection between this case and the Western District of Texas is that it appears that PacSec3 prefers to file its suits there. That is not enough to overcome a transfer motion directed to a district which is the home of evidence, witnesses and the conduct giving rise to the action. We therefore grant NetScout's petition seeking transfer of the case to the Eastern District of Michigan.

Accordingly,

IT IS ORDERED THAT:

(1) PacSec3's unopposed motion to file its corrected response brief out of time is granted. ECF Nos. 14 and 15 are accepted for filing.

(2) The petition for mandamus is granted. The district court's July 27, 2021, order is vacated, and it is directed to

transfer this matter to the United States District Court for the Eastern District of Michigan.

FOR THE COURT

October 13, 2021
Date

/s/ Peter R. Marksteiner
Peter R. Marksteiner
Clerk of Court

s28

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Donald N. Cohen	Group Art Unit: 3992
Appl. No.: 10/841,064	Examiner: Larose, Colin M
Filed: May 7, 2004	Confirmation No: 9957
U.S. Patent No. 7,523,497 Issue Date: April 21, 2009 Reexamination Control No. 90/014,746	Atty. Dkt. No.: 20227.0009.REEX00
Title: PACKET FLOODING DEFENSE SYSTEM	

Mail Stop "Ex Parte Reexam"
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted today via the Office electronic filing system (EFS-Web) in accordance with 37 CFR §1.8.

Date: August 17, 2021 Signature: /Theresa M. Evenbly/
Printed Name: Theresa M. Evenbly

PATENT OWNER STATEMENT PURSUANT TO 37 C.F.R.§ 1.530

Enclosed herewith is PacSec3 LLC's Patent Owner Statement pursuant to 37 C.F.R § 1.530 with respect to the challenge of claims 1, 4, 7, 10, 13, and 16 of U.S. Patent No. 7,523,497 filed by Third Party Requester, Unified Patents, LLC.

TABLE OF CONTENTS

I. INTRODUCTION 1

II. CLAIM CONSTRUCTION 2

III. CLAIMS 1, 4, 7, 10, 13, AND 16 ARE PATENTABLE OVER THE REFERENCES INCLUDED IN THE REQUEST 3

A. Challenged Claims 1, 4, 7, 10, 13 and 16 are Patentable Over Savage (SNQ A) 3
B. Challenged Claims 4, 10, and 16 are Patentable over Maher and Savage (SNQ B) 8
C. Challenged Claims 1, 4, 7, 10, 13 and 16 are Patentable over Maher and Schuba (SNQ C) 10
D. Challenged Claims 1, 4, 7, 10, 13 and 16 are Patentable Over Savage, Maher, and Schuba (SNQ D) 11

IV. LIST OF EXHIBITS 13

V. CONCLUSION 13

TABLE OF AUTHORITIES

Cases

In re Yamamoto, 740 F.2d 1569, 222 USPQ934 (Fed. Cir. 1984) 2

Statutes

35 U.S.C. 304..... 2

I. INTRODUCTION

U.S. Patent No. 7,523,497 ("the '497 Patent") is directed to a system to defend against and resist packet flooding Distributed Denial of Service (DDoS) attacks for a network having a plurality of host computers, routers, communication lines and transmitted data packets, the system includes means for 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; means for classifying data packets received at said host computer into wanted data packets and unwanted data packets by path; means for assigning a maximum acceptable processing rate to each class of data packet; and means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets.

Requester challenges the patentability of Claims 1, 4, 7, 10, 13 and 16 of the '497 Patent based on three (3) different alleged prior art references as follows.

1. Stefan Savage et al., "Practical Network Support for IP Traceback," ACM SIGCOMM 2000: Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2000, pp. 295-306 ("Savage");

2. U.S. Patent 6,725,378 ("Schuba"); and

3. U.S. Patent 7,058,974 ("Maher").

The Request alleges four (4) different combinations of the prior art references raise a substantial new question of patentability. In the Order Granting Request for *Ex Parte* Reexamination mailed on June 17, 2021, the Examiner concluded that only three (3) alleged grounds raise a substantial new question of patentability, as shown below:

Item	References	Claims	SNQ
A	Savage	1, 4, 7, 10, 13 and 16	Yes
B	Maher and Savage	4, 10 and 16	Yes
C	Maher and Schuba	1, 4, 7, 10, 13 and 16	No
D	Savage, Maher, and Schuba	1, 4, 7, 10, 13 and 16	Yes

II. Claim Construction

During reexamination ordered under 35 U.S.C. 304, claims are given the broadest reasonable interpretation consistent with the specification and limitations in the specification are not read into the claims *(In re Yamamoto,* 740 F.2d 1569, 222 USPQ934 (Fed. Cir. 1984)). (Ex. 2001 at ¶17).

Requester considered the plain and ordinary meaning of each term of the '497 Patent as it would have been understood by one skilled in the art (Req, at 20). Patent Owner reserves all rights to raise claim construction arguments in district court and in this proceeding. (Ex. 2001 at ¶18).

III. CLAIMS 1, 4, 7, 10, 13, AND 16 ARE PATENTABLE OVER THE REFERENCES INCLUDED IN THE REQUEST

A. Challenged Claims 1, 4, 7, 10, 13 and 16 are Patentable Over Savage (SNQ A)

Savage describes a technique for tracing anonymous packet flooding attacks on the Internet back towards their source. (Ex. 1005 at Abstract). (Ex. 2001 at ¶19).

Fig. 1 of Savage is shown below.

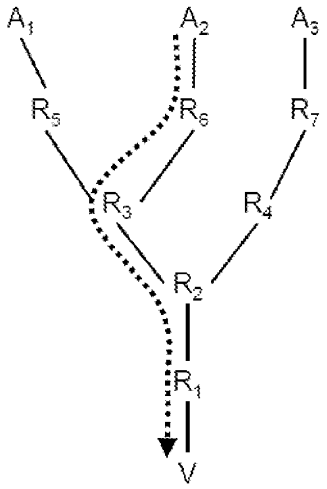


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

Ex. 1005 at Figure 1.

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** (Ex. 1005 at 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. 1005 at 299).

Edge sampling algorithm is to explicitly encode edges in the attack path rather than simply individual nodes. To do this, it is needed to reserve two static address-sized fields, start and end, in each packet to represent the routers at each end of a link, as well as an additional small field to represent the distance of an edge sample from the victim. (Ex. 1005 at 299). The victim uses the edges sampled in these

packets to create a graph (much as in Figure 1) leading back to the source, or sources, of attack. (Ex. 1005 at 300).

Savage teaches inserting a mark in each packet as it traverses each router in transit. The collection of marks represents the "path" taken by the packet to the end point. If the packet is part of an attack, the path becomes the "attack path". Savage does not describe how one would distinguish attack packets from non-attack packets, which the '497 Patent does teach. However, Savage does teach that the packet mark made by routers be used for the purpose of identifying the path **FOR TRACEBACK after** a packet flood attack is detected by some means not addressed in Savage. (Ex. 1005 at 297) Most important, Savage does not teach how the packet marks and path denoted by the marks can be used **TO DEFEND AGAINST OR RESIST** packet flood attacks. It must be noted that packet marking by routers is older than Savage. (Ex. 1005 at 297). (Ex. 2001 at ¶20).

Unlike Savage, the '497 Patent discloses how packet flood attacks can be detected. Claim 1 discloses "means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;". In addition, the '497 Patent also discloses how marks denoting path can be used to defend actively against packet flood attacks. Claim 1 discloses "means for associating a maximum acceptable processing rate with each class of data packet received at said computer;" and "means in said computer for using said information to allocate the processing

rate available for unwanted data packets to be less than or equal to said maximum accept able processing rate." Savage does not disclose anything related to detection of or defenses against DDoS Attacks. (Ex. 2001 at ¶21).

The '497 Patent states "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**." (Ex. 1001 at col. 2, lines 30-36). These are not disclosed by Savage. (Ex. 2001 at ¶22).

Savage describes a traceback technique using packet marks to encode path. Savage teaches "PROBABILISTIC" packet marking whereby the routers attack packet marks *TO A SELECT SAMPLE* of the packets traversing the router. Therefore, the packets that are used in a flood attack MAY NOT HAVE THE DESIRED PATH DATA when they arrive at the victim site. Savage teaches no way to handle this problem. the '497 Patent teaches packet marks that are supplied by cooperating routers unconditionally, with no probabilistic variation. As a result, ALL attack packets will invariably have the PATH DATA if they traversed the cooperating routers that mark the packets. (Ex. 2001 at ¶23).

In addition, the probabilistic variability of Savage makes it impossible to implement an effective defense using the kind of packet marks advocated therein.

Cloudflare, Inc. Exhibit 1003 Page 242

Savage is concerned with using the path information in the detected attack packets to TRACEBACK to the true source address of the attack. This is useful for forensics after an attack, but Savage does not propose the method as a defense, nor can the method disclosed in Savage be used for defense because of its probabilistic nature. (Ex. 2001 at ¶24).

The '497 Patent teaches how path information can be utilized by the host computer endpoint to classify packets, and to allocate "fair service" to every path through which traffic is being forwarded to the enterprise. This part of the invention **DEFENDS** the enterprise network against packet flood DDoS attacks. In Savage, it is not known which packets are unwanted and wanted. Therefore, the processing rate cannot be allocated to be less for unwanted packets. **There is no counterpart in Savage that addresses defending the victim**. (Ex. 2001 at ¶25).

Further, since Savage is exclusively a traceback method, it does not disclose any method to detect when an attack may be taking place or how to defend against it. Savage does not disclose the limitation "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path" as required by claims 7, 10, 13, and 16 of the '497 Patent. Savage does not disclose "associating a maximum acceptable processing rate with each class of data packet received at said compute" as required by claims 1 and 7 of the '497 Patent. Savage does not disclose "using said information to allocate the processing rate available

for unwanted data packets to be less than or equal to said maximum acceptable processing rate" as required by claims 1, 4, 7, 10, 13, and 16. of the '497 Patent. Requester admits that Savage does not expressly disclose what preventive measures are performed in the network on unwanted packets when a packet flooding attack has occurred. Req. at 44. Savage is directed to the hope of stopping a packet flooding attack simply by "tracing attacks back towards their origin-ideally stopping an attacker at the source." (Req. 44-45). At most, Savage stops an attacker basing on the **source** of the attacker, not on the **path**. If the attack originates in jurisdictions where attackers do not care about being detected, Savage provides no defense. The cited elements of the '497 Patent (classification of packets into wanted / unwanted, classification by path, assigning rate limits by class, and enforcing the rate limits) are specific to detecting when an attack is ongoing and defending against it actively whether attackers elect to cooperate with the victims or not. (Ex. 2001 at ¶26).

Therefore, as a traceback method (and not an active defense method) for packet flood attacks, Savage does not disclose, anticipate, or render claims 1, 4, 7, 10, 13 and 16 of the '497 Patent obvious. (Ex. 2001 at ¶27).

B. Challenged Claims 4, 10, and 16 are Patentable over Maher and Savage(SNQ B)

As set forth above, Savage does not disclose the limitation "classifying data packets received at a host computer into wanted data packets and unwanted data

packets by path", "associating a maximum acceptable processing rate with each class of data packet received at said compute", and "using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate" as required by claims 4, 10, and 16 of the '497 Patent. (Ex. 2001 at ¶28).

Maher is directed to "a method and apparatus for preventing denial of service type attacks on data networks" (Ex. 1006 at Abstract), the apparatus includes a traffic flow scanning engine 140 and a quality of service processor (Ex. 1006 at 3:6-9, 6:11-21, 7:27-41). Maher does not disclose finding information regarding the path that the received packets traversed via packet-marking by routers along the path leading to the host computer (Order at 6), not to mention "said path comprising all routers in said network via which said packets are routed to said computer" as required by claims 4, 10, and 16 of the '497 Patent. (Ex. 2001 at ¶29).

Further, Maher does not classify data packets received at a host computer into wanted data packets and unwanted data packets by path. (Ex. 2001 at ¶30). Maher states "Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the contents contain valid network traffic between known **sources** and destinations. Traffic flows that have **not been verified because they are from unknown sources** or because they are new unclassified flows **can be assigned to a low quality of service queue until the sources are**

verified or the traffic flow classified as valid traffic. Since most DoS attacks send new session information, **data from spoofed sources**, or meaningless data, network apparatus 100 would assign those traffic flows to low quality traffic queues." (Ex. 1006 at 7: 56-67).

Requester states that "the scanning and analysis of the source and destination addresses in packets constitutes an analysis of the path between the source and destination of the packets (Ex, 1003at ¶96) (Req. 39). This statement is groundless as the contents of the packets do not include information about the path in spite of the contents of the packets comprising the information about sources and destinations. Otherwise, Savage will not find the path of the packets at great cost. Maher does not classify data packets based on path. Thus, Maher does not disclose "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path" as required by claims 4, 10, and 16 of the '497 Patent. (Ex. 2001 at ¶30).

Therefore, Maher and Savage alone or in combination do not render claims 4, 10, and 16 of the '497 Patent obvious. (Ex. 2001 at ¶31).

C. Challenged Claims 1, 4, 7, 10, 13 and 16 are Patentable over Maher and Schuba (SNQ C)

Patent Owner agrees with the Order that the Request for Reexamination does not establish that the combination of the Maher and Schuba raise a bona fide substantial new question of patentability for claims 1, 4, 7, 10, 13, and 16, because neither Maher nor Schuba are packet flood detection and mitigation solutions. (Order, at 5-6). As such, Maher and Schuba do not disclose finding information regarding the path received packets traversed via packet-marking by routers along the path leading to the host computer, in which the path comprises all routers in the network (Order, at 5-6). (Ex. 2001 at ¶32).

D. Challenged Claims 1, 4, 7, 10, 13 and 16 are Patentable Over Savage, Maher, and Schuba (SNQ D).

As depicted above, Savage does not disclose the limitation "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path" as required by claims 7, 10, 13, and 16 of the '497 Patent. Savage does not disclose "associating a maximum acceptable processing rate with each class of data packet received at said compute" as required by claims 1 and 7 of the '497 Patent. Savage does not disclose "using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate" as required by claims 1, 4, 7, 10, 13, and 16. of the '497 Patent. (Ex. 2001 at ¶33).

Cloudflare, Inc. Exhibit 1003 Page 247

As also depicted above, Maher does not disclose "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path". (Ex. 2001 at ¶34).

Schuba classifies data packets received at a host computer into wanted data packets and unwanted data packets by **source of the packets not by path**. Requester states "Schuba discloses that messages transmitted to a network are classified as being acceptable, unacceptable, or suspect type, based on the source address of the packets. Ex. 1007 at, Abstract, 2:1-5, 2: 22-26, 3: 8-13. Schuba thus teaches that incoming packets are classified into one of three states (acceptable, unacceptable, or suspect) based on the incoming packets' source address." (Req. at 40). (Ex. 2001 at ¶35).

Savage, Maher, and Schuba, alone or in combination, do not teach at least "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path". (Ex. 2001 at ¶36).

Therefore, Savage, Maher and Schuba do not render claims 1, 4, 7, 10, 13, and 16 of the '497 Patent obvious. (Ex. 2001 at ¶37).

IV. LIST OF EXHIBITS

Exhibit No.	Document
2001	Declaration of Swamy Narayanaswamy with Ex. A Curriculum Vitae

V. CONCLUSION

Therefore, the Examiner should find all Challenged Claims are patentable over the prior art cited in the Request for Reexamination and conclude this Reexamination proceeding.

Ramey & Schwaller, LLP
5020 Montrose Blvd., Ste. 800
Houston, Texas 77006
(713) 426-3923 (telephone)

Respectfully submitted,
/William P. Ramey III/
William P. Ramey, III
Reg. No.: 44,295
Attorney for Applicant

CERTIFICATE OF SERVICE

The undersigned certifies that copies of the following,

1) Patent Owner Statement Pursuant to 37 C.F.R.§ 1.530;
2) Exhibit 2001- Declaration of Swamy Narayanaswamy with Ex. A Curriculum Vitae

in their entirety were served on:

Raghav Bajaj
Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, TX 75219
raghav.bajaj@haynesboone.com

the attorney of record, in accordance with 37 C.F.R. § 1.510(b)(5), on the 17th day of August 2021.

Dated: August 17, 2021

William P. Ramey, III
Registration No.: 44,295

Cloudflare, Inc. Exhibit 1003 Page 250

Curriculum Vitae

(323) 336-3006 **Dr. Swamy Narayanaswamy** swamy@calqlogic.com

LinkedIn: https://www.linkedin.com/in/knarayanaswamy

Software Development Skill Suite:

- *Modeling and Methods:* UML, Rapid Application Development, Agile development, DevOps
- *Cloud, Micro-services and Containers:* Docker, Kubernetes, and scalable cloud delivery of solutions
- *Machine/Deep Learning, Data Science:* Scikit-Learn, PyTorch, TensorFlow, Keras, Anaconda, Jupyter;
- *Application Languages:* Python, R, Java, C++, C#, Common Lisp;
- *Platforms:* Jupyter, Eclipse, NetBeans IDE, Web2Py, and .NET framework

Professional Interests:

- ✓ **Applying machine / deep learning** & data science to build technologies that improve business outcomes;
- ✓ Experienced in the practical pitfalls/problems of **deploying data-driven solutions into real businesses**;
- ✓ **Master developer in the platforms listed,** with wide experience from soup to nuts in software creation;
- ✓ **Proven architect and leader**, with experience managing technical teams to deliver results effectively;
- ✓ **Teaching courses / mentoring developers** in my areas of expertise (machine learning, data science, AI)

Professional Experience:

2017- Present Chief Technology Officer and co-founder, CalQLogic. ,

- Spear-heading the company's emergence in the real-time analytics marketplace. The platform leverages advanced methods to support D-I-Y analytics over disparate data sources over the Internet and Intranet. The product targets pharma, IOT, supply chain, and other markets.
- Developing / Managing Data Analytics / Machine Learning Consulting projects for clients:
- ✓ Prototyped machine learning solutions for a healthcare startup focused on special needs children. Used Python and Scikit-Learn to build a solution with automatic document OCR, content classification, and extraction of critical data.
- ✓ Working with a medical device startup (using Python / TensorFlow) on its backend deep learning strategy to improve automated diagnostics using machine learning algorithms and models as needed by their executives.
- ✓ Assisting a literature monitoring company in leveraging machine learning to detect deep structure within technical papers in different domains. Leveraging various supervised learning models; and Deep Learning neural networks. Utilized Python/Scitkit Learn

1995 – 2017 Chief Technology Officer and co-founder, Cs3 Inc. ,

Spear-heading the company's technology direction and development of product suite.

Principal Investigator for several R&D projects leading to new products:

"Detection and Containment of Computer Epidemics through Correlation of Communication Anomalies" Department of Homeland Security (2004 – present)

"Attack Attribution Techniques for Heterogeneous, Non-Cooperative Infrastructure" Advanced Research and Development Activity (2003 - present)

"An Event Monitoring Framework for Automatic Network Diagnosis for Defense" Defense Advanced Research Projects Agency (1999-2002)

"Software Evolution Through Automatic Monitoring" DARPA (1996-1999)

"Automatic Monitoring of Software Requirements" NSF, (1996-1997)

- Led Product development for Sonario (a HR Talent management solution) for a client Iscomp Systems / Levinson Institute, that is now in production at corporations;
- Spearheaded Cs3's flagship DDoS defense products under the brand name ManaNet. Conceptualized the products and managed the development of these breakthrough technologies. Presented the technology at multiple venues. Guided the acquisition of 4 US Patents in cybersecurity / DDoS defense;

1985 - 1995	Computer Scientist, USC/Information Sciences Institute, Co-developer/maintainer of domain modeling environment to apply AI methods to software Development in developing rapid prototypes of software using formal specifications; Providing automated support for evolution of software using Artificial Intelligence methods; Author of about 20 research publications in conferences and journals
2004 – Present	Adjunct Professor at Loyola Marymount University / USC / UCLA Extension Developed and taught AI / Machine Learning courses for grads/undergrads. Taught the capstone AI course offerings for over 5 years at USC. Developed several advanced curricula in OO programming,

Education:

1980 - 1985	University of Southern California, Los Angeles, CA. PhD, Computer Science. (May 1985);
1978 - 1980	University of Nebraska-Lincoln, NE Master of Science, Computer Science.
1973 - 1978	Indian Institute of Technology, Madras, India Bachelor of Technology, Electronics.

Professional Activities:

Speaker and Panelist:

- Multiple appearances in various industry panels and workshops particularly as it relates to cybersecurity, data analytics and business applications of machine learning, IOT, etc. (e.g., Digital Growth Summit). I have contributed to multiple books on my areas within my core competencies.

Program Committees:

- International Symp. on Object Technologies for Advanced Software, Kanazawa, Japan, January, 1996.
- 9th International Software Process Workshop, Airlie, Virginia, October, 1994.
- 1st Int'l Workshop on Process-Centered Software Environments, Boulder, Colorado, October 1993.

Organizer:

- OOPSLA Workshop on Are CASE Frameworks ready for Prime-Time? Austin, Texas, October 1995.

Reviewer:

Reviewed several technical articles for

- International Conference on Software Engineering.
- International Conference on the Software Process.
- IEEE Transactions on Software Engineering.
- IEEE Transactions on Software Engineering and Methodology.
- Journal of Systems and Software, IEEE Transactions on Knowledge Engineering

Awards and Honors:

- Co-author of 8 US Patents in cooperation with the rest of my technology team;
- Led Cs3 to several key R&D contracts in national competitions against much larger corporate juggernauts;
- Governor's Gold Medal, Graduating Class of 1978. Indian Institute of Technology, Madras (One of the 5 elite technology schools in India)

Professional Affiliations:

- Member of ACM and IEEE.

Ex. 2001A-2

Publications:

1. *Using First Order Logic to Query Heterogeneous Internet Data Sources*, Soft Computing and Software Engineering Conference, March 2015, Berkeley, CA. (Selected Best Paper at the Conference), https://www.sciencedirect.com/science/article/pii/S1877050915025661
2. *Key Concepts to Support Creation of Powerful IOT Apps*, Invited Paper, CIO Review Magazine, December 2014, http://magazine.cioreview.com/December-2014/IoT/
3. *Attack Attribution in Non-Cooperative Networks*, IEEE Conference on Information Assurance, August, 2004
4. *Defending Government Networks Against Distributed Denial of Service Attacks,* with Donald Cohen, Cs3 Inc White Paper, http://www.cs3-inc.com/government-ddos-threat-and-solutions.pdf.
5. *Changes to IP to Eliminate Source Forgery, with Donald Cohen*, Cs3 White Paper, http://www.cs3-inc.com/sf.PDF.
6. *A Fair Service Approach to Defending Against Packet Flooding Attacks on the Internet*, with Donald Cohen, Cs3 White Paper, http://www.cs3-inc.com/ddos.PDF.
7. *Relations as Abstraction for C ++ Programming*, with Neil Goldman and Donald Cohen Object-Oriented Programming Systems & Languages (OOPSLA 95).
8. CSCW 94 Workshop to Explore Relationships between Research in Computer Supported Cooperative Work & Software Process — Workshop Report, with Balachander Krishnamurthy, ACM Software Engineering Notes, April 1995.
9. *Process Formalism/Tools/Architecture — Implications for Humans*, (Session Summary), Proceedings of the International Software Process Workshop (ISPW 9), October 1994.
10. *Adding Performance Information to ADT Interfaces*: *Why and How*, with Neil Goldman and Donald Cohen, SIGPLAN Workshop on Interface Definition Languages, Portland, Oregon, January 1994.
11. *Interactive Elaborations of Generic Designs*, with Lewis Johnson and Robert Balzer, Proceedings of the Knowledge-Based Software Engineering, December, 1993.
12. *Mechanism for Generic Process Support*, with Robert Balzer, Proceedings of the First ACM Symposium on the Foundations of Software Engineering, December, 1993.
13. *PSEE Architectures: ISPW8 Session Summary*, with Maria Penedo, Proceedings of the 8th International Software Process Workshop, March, 1993.
14. *Just What is a Process-Sensitive Software Engineering Environment?,* Proceedings of the Workshop on Process-Sensitive Software Engineering Environments, September, 1992.
15. *Lazy Consistency: A Basis for Cooperative Software Development*, with Neil Goldman, Proceedings of the Computer Supported Cooperative Work Conference, November, 1992.
16. *Software Evolution Based on Iterative Prototyping*, with Neil Goldman, Proceedings of the 14th International Conference on Software Engineering, May, 1992.
17. *Team Coordination: Information Sharing + Policies*, with Neil Goldman, Proceedings of the 7th International Software Process Workshop, 1991.
18. *A Flexible Framework to Support Cooperative Distributed Software Development*, with Neil Goldman, Journal of Systems and Software, October, 1991.
19. *A Logical Framework to Support Cooperative Software Development,* with Donald Cohen, Proceedings of the 6th International Software Process Workshop, 1990.
20. *A Text-Based Representation for Program Variants*, Proceedings of the Second International Workshop on Software Configuration Management, 1989.
21. *Static-Analysis Based Program Evolution Support in the Common Lisp Framework*, Proceedings of the 10th International Conference on Software Engineering, April, 1988.
22. *An Incremental Mechanism for Schema Evolution in Engineering Domains*, with K.V. Bapa Rao, Proceedings of the International Conference on Data Engineering, February 1988.
23. *Version Control in the Common Lisp Framework*, Proceedings of First International Workshop on Software Version and Configuration Control, 1988.
24. *Static Analysis: An Aid to Program Maintenance and Development*, Hawaii International Conference on System Sciences, January, 1988.
25. *Maintaining Configurations of Evolving Systems*, with Walt Scacchi, IEEE Transactions on Software Engineering, SE-13, No. 3, 1987.
26. *A Database Foundation to Support Software System Evolution*, With Walt Scacchi, Journal of Systems and Software, May, 1987.
27. *An Environment for the Development and Maintenance of Large Software Systems*, SOFTFAIR II, Second Conference on Software Development Tools, Techniques, and Alternatives, December, 1985.
28. *An Approach to Information Management for CAD/VLSI Applications*, with Dennis Mcleod and K.V. Bapa Rao, Proceedings of the ACM SIGMOD, 1983.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Donald N. Cohen	Group Art Unit: 3992
Appl. No.: 10/841,064	Examiner: Larose, Colin M
Filed: May 7, 2004	Confirmation No: 9957
U.S. Patent No. 7,523,497 Issue Date: April 21, 2009 Reexamination Control No. 90/014,746	Atty. Dkt. No.: 20227.0009.REEX00
Title: PACKET FLOODING DEFENSE SYSTEM	

Mail Stop "Ex Parte Reexam"
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted today via the Office electronic filing system (EFS-Web) in accordance with 37 CFR §1.8.

Date: August 17, 2021 Signature: /Theresa M. Evenbly/

DECLARATION OF SWAMY NARAYANASWAMY

I, Swamy Narayanaswamy, do hereby declare as follows:

I. INTRODUCTION

1. I have been retained as an expert on behalf of PacSec 3 LLC ("Patent Owner" or "PacSec3") in this reexamination proceeding of U.S. Patent No.

7,523,497 ("the '497 Patent"). I understand this proceeding was initiated by Requester Unified Patents, LLC ("Requester" or "Unified Patents").

2. I have set forth my professional qualifications and relevant experience in Section II of this Declaration, and a copy of my curriculum vitae is available at Attachment A.

3. I have been asked to provide my expert opinions regarding the validity or invalidity of claims 1, 4, 7, 10, 13, and 16 of the '497 Patent.

4. I understand that Requester has asserted invalidity based on the following references: (Request for Ex Parte Reexamination at 20-21).

Reference	Exhibit
Savage et al., "Practical Network Support for IP Traceback," SIGCOMM '00: Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2000, pp. 295-306 ("Savage")	1005
U.S. Patent No. 7,058,974 to Maher *et al.* ("Maher")	1006
U.S. Patent No. 6,725,378 to Schuba *et al.* (Schuba)	1007

5. In particular, I understand that Requester has asserted the following Substantial New Questions of Patentability (SNQs) based on these references: (Order at 4).

Ground	Challenged Patent Claims	Reference(s)/Basis	Request Granted
A	1, 4, 7, 10, 13, and 16	Savage	Yes
B	4, 10, and 16	Maher and Savage	Yes
C	1, 4, 7, 10, 13, and 16	Maher and Schuba	No
D	1, 4, 7, 10, 13, and 16	Savage, Maher, and Schuba	Yes

6. As set forth in this Declaration, I do not agree that the identified references or combinations of references anticipate or render unpatentable the challenged claims of the '497 Patent.

7. In forming the opinions I express in this Declaration, I have considered, among other things, the materials cited or discussed in this Declaration, the '497 Patent, the corresponding file history, Unified Patent's Request for Reexamination, Madisetti's Declaration, the references and exhibits on which Requester and Madisetti rely, and the Order Granting Reexamination of U.S. Patent 7,523,497. Additionally, I have relied on my own knowledge, training, and more than 53 years of experience in analyzing electronics and software. I am a co-author of 8 U.S. Patents.

8. I am being compensated for my time in connection with this Request at my standard consulting rate, and my compensation is not affected by the outcome of this matter.

A. Background and Qualifications

9. I am currently the Chief Technology Officer and co-founder of CalQLogic.

10. I received a Ph.D. in Computer Science from the University of Southern California in 1985; a Master of Science in Computer Science from the University of Nebraska-Lincoln in 1980, and a Bachelor of Technology in Electronics from the Indian Institute of Technology in 1978.

11. From 2017-Present, I served as the Chief Technology Officer and co-founder of CalQLogic. From 2004-Present, I have served as an adjunct professor at Loyola Marymount University, USC, and UCLA Extension. From 1995-2017, I serve as the Chief Technology Officer and co-founder of Cs3 Inc. From 1985-1995, I serve as a computer scientist at the USC/Information Sciences Institute.

12. I have more than 53 years of experience in analyzing electronics and software.

13. I have been a speaker and panelist at various industry panels and workshops, particularly as it relates to cybersecurity and data analytics.

14. I am a co-author of 8 U.S. Patents.

15. Additional details regarding my background and qualifications are set forth in my curriculum vitae in Attachment A.

16. U.S. Patent No. 7,523,497 ("the '497 Patent") is directed to a system to defend against and resist packet flooding Distributed Denial of Service (DDoS) attacks for a network having a plurality of host computers, routers, communication

lines and transmitted data packets, the system includes means for 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; means for classifying data packets received at said host computer into wanted data packets and unwanted data packets by path; means for assigning a maximum acceptable processing rate to each class of data packet; and means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets.

II. Claim Construction

17. During reexamination ordered under 35 U.S.C. 304, claims are given the broadest reasonable interpretation consistent with the specification and limitations in the specification are not read into the claims *(In re Yamamoto,* 740 F.2d 1569, 222 USPQ934 (Fed. Cir. 1984)).

18. Requester considered the plain and ordinary meaning of each term of the '497 Patent as it would have been understood by one skilled in the art (Req, at 20). Patent Owner reserves all rights to raise claim construction arguments in district court and in this proceeding.

III. CLAIMS 1, 4, 7, 10, 13, AND 16 ARE PATENTABLE OVER THE REFERENCES INCLUDED IN THE REQUEST

B. Challenged Claims 1, 4, 7, 10, 13 and 16 are Patentable Over Savage (SNQ A)

19. Savage describes a technique for tracing anonymous packet flooding attacks on the Internet back towards their source. (Ex. 1005 at Abstract). Fig. 1 of Savage is shown below.

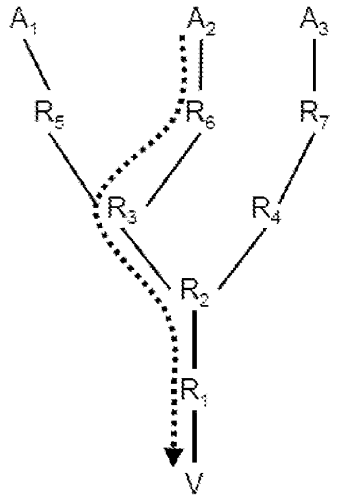


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

Ex. 1005 at Figure 1.

20. Savage teaches inserting a mark in each packet as it traverses each router in transit. The collection of marks represents the "path" taken by the packet to the end point. If the packet is part of an attack, the path becomes the "attack path". Savage does not describe how one would distinguish attack packets from non-

attack packets, which the '497 Patent does teach. However, Savage does teach that the packet mark made by routers be used for the purpose of identifying the path FOR TRACEBACK after a packet flood attack is detected by some means not addressed in Savage. (Ex. 1005 at 297) Most important, Savage does not teach how the packet marks and path denoted by the marks can be used TO DEFEND AGAINST OR RESIST packet flood attacks. It must be noted that packet marking by routers is older than Savage. (Ex. 1005 at 297).

21. Unlike Savage, the '497 Patent discloses how packet flood attacks can be detected. Claim 1 discloses "means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;". In addition, the '497 Patent also discloses how marks denoting path can be used to defend actively against packet flood attacks. Claim 1 discloses "means for associating a maximum acceptable processing rate with each class of data packet received at said computer;" and "means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum accept able processing rate." Savage does not disclose anything related to detection of or defenses against DDoS Attacks.

22. The '497 Patent states "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." (Ex. 1001 at col. 2, lines 30-36). These are not disclosed by Savage.

23. Savage describes a traceback technique using packet marks to encode path. Savage teaches "PROBABILISTIC" packet marking whereby the routers attack packet marks TO A SELECT SAMPLE of the packets traversing the router. Therefore, the packets that are used in a flood attack MAY NOT HAVE THE DESIRED PATH DATA when they arrive at the victim site. Savage teaches no way to handle this problem. the '497 Patent teaches packet marks that are supplied by cooperating routers unconditionally, with no probabilistic variation. As a result, ALL attack packets will invariably have the PATH DATA if they traversed the cooperating routers that mark the packets.

24. In addition, the probabilistic variability of Savage makes it impossible to implement an effective defense using the kind of packet marks advocated therein. Savage is concerned with using the path information in the detected attack packets to TRACEBACK to the true source address of the attack. This is useful for forensics after an attack, but Savage does not propose the method as a defense, nor can the method disclosed in Savage be used for defense because of its probabilistic nature.

25. The '497 Patent teaches how path information can be utilized by the host computer endpoint to classify packets, and to allocate "fair service" to every path through which traffic is being forwarded to the enterprise. This part of the invention DEFENDS the enterprise network against packet flood DDoS attacks. In Savage, it is not known which packets are unwanted and wanted. Therefore, the processing rate cannot be allocated to be less for unwanted packets. There is no counterpart in Savage that addresses defending the victim.

26. Further, since Savage is exclusively a traceback method, it does not disclose any method to detect when an attack may be taking place or how to defend against it. Savage does not disclose the limitation "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path" as required by claims 7, 10, 13, and 16 of the '497 Patent. Savage does not disclose "associating a maximum acceptable processing rate with each class of data packet received at said compute" as required by claims 1 and 7 of the '497 Patent. Savage does not disclose "using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate" as required by claims 1, 4, 7, 10, 13, and 16. of the '497 Patent. Requester admits that Savage does not expressly disclose what preventive measures are performed in the network on unwanted packets when a packet flooding attack has occurred. Req. at 44. Savage is directed to the hope of stopping

a packet flooding attack simply by "tracing attacks back towards their origin-ideally stopping an attacker at the source." (Req. 44-45). At most, Savage stops an attacker basing on the source of the attacker, not on the path. If the attack originates in jurisdictions where attackers do not care about being detected, Savage provides no defense. The cited elements of the '497 Patent (classification of packets into wanted / unwanted, classification by path, assigning rate limits by class, and enforcing the rate limits) are specific to detecting when an attack is ongoing and defending against it actively whether attackers elect to cooperate with the victims or not.

27. Therefore, as a traceback method (and not an active defense method) for packet flood attacks, Savage does not disclose, anticipate, or render claims 1, 4, 7, 10, 13 and 16 of the '497 Patent obvious.

C. Challenged Claims 4, 10, and 16 are Patentable over Maher and Savage (SNQ B)

28. As set forth above, Savage does not disclose the limitation "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path", "associating a maximum acceptable processing rate with each class of data packet received at said compute", and "using said information to allocate the processing rate available for unwanted data packets to be less than or

equal to said maximum acceptable processing rate" as required by claims 4, 10, and 16 of the '497 Patent.

29. Maher is directed to "a method and apparatus for preventing denial of service type attacks on data networks" (Ex. 1006 at Abstract), the apparatus includes a traffic flow scanning engine 140 and a quality of service processor (Ex. 1006 at 3:6-9, 6:11-21, 7:27-41). Maher does not disclose finding information regarding the path that the received packets traversed via packet-marking by routers along the path leading to the host computer (Order at 6), not to mention "said path comprising all routers in said network via which said packets are routed to said computer" as required by claims 4, 10, and 16 of the '497 Patent.

30. Further, Maher does not classify data packets received at a host computer into wanted data packets and unwanted data packets by path. Requester states that "the scanning and analysis of the source and destination addresses in packets constitutes an analysis of the path between the source and destination of the packets (Ex, 1003at ¶96) (Req. 39). This statement is groundless as the contents of the packets do not include information about the path in spite of the contents of the packets comprising the information about sources and destinations. Otherwise, Savage will not find the path of the packets at great cost. Maher does not classify data packets based on path. Thus, Maher does not disclose "classifying data

packets received at a host computer into wanted data packets and unwanted data packets by path" as required by claims 4, 10, and 16 of the '497 Patent.

31. Therefore, Maher and Savage alone or in combination do not render claims 4, 10, and 16 of the '497 Patent obvious.

D. Challenged Claims 1, 4, 7, 10, 13 and 16 are Patentable over Maher and Schuba (SNQ C)

32. The Order states that the Request for Reexamination does not establish that the combination of the Maher and Schuba raise a bona fide substantial new question of patentability for claims 1, 4, 7, 10, 13, and 16, because neither Maher nor Schuba are packet flood detection and mitigation solutions. (Order, at 5-6). As such, Maher and Schuba do not disclose finding information regarding the path received packets traversed via packet-marking by routers along the path leading to the host computer, in which the path comprises all routers in the network (Order, at 5-6).

D. Challenged Claims 1, 4, 7, 10, 13 and 16 are Patentable Over Savage, Maher, and Schuba(SNQ D).

33. As depicted above, Savage does not disclose the limitation "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path" as required by claims 7, 10, 13, and 16 of the '497 Patent. Savage does not disclose "associating a maximum acceptable processing rate with each

class of data packet received at said compute" as required by claims 1 and 7 of the '497 Patent. Savage does not disclose "using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate" as required by claims 1, 4, 7, 10, 13, and 16. of the '497 Patent.

34. As also depicted above, Maher does not disclose "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path".

35. Schuba classifies data packets received at a host computer into wanted data packets and unwanted data packets by source of the packets not by path. Requester states "Schuba discloses that messages transmitted to a network are classified as being acceptable, unacceptable, or suspect type, based on the source address of the packets. Ex. 1007 at, Abstract, 2:1-5, 2: 22-26, 3: 8-13. Schuba thus teaches that incoming packets are classified into one of three states (acceptable, unacceptable, or suspect) based on the incoming packets' source address." (Req. at 40).

36. Savage, Maher, and Schuba, alone or in combination, do not teach at least "classifying data packets received at a host computer into wanted data packets and unwanted data packets by path".

37. Therefore, Savage, Maher and Schuba do not render claims 1, 4, 7, 10, 13, and 16 of the '497 Patent obvious.

IV. CONCLUSION

38. All Challenged Claims are patentable over the prior art cited in the Request for Reexamination.

Date: 8/16/2021

Respectfully submitted,



Swamy Narayanaswamy

Electronic Acknowledgement Receipt

EFS ID:	43534652
Application Number:	90014746
International Application Number:	
Confirmation Number:	9957
Title of Invention:	PACKET FLOODING DEFENSE SYSTEM
First Named Inventor/Applicant Name:	7523497
Customer Number:	31718
Filer:	William Peterson Ramey/Theresa Evenbly
Filer Authorized By:	William Peterson Ramey
Attorney Docket Number:	50348.65
Receipt Date:	17-AUG-2021
Filing Date:	03-MAY-2021
Time Stamp:	18:32:59
Application Type:	Reexam (Patent Owner)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2021-08-16_497-PatentOwnerStatement.pdf	368133 dcd1ada4333093800a699d5e13e5dd8babef43fc	yes	17

	Multipart Description/PDF files in .zip description				
	Document Description	**Start**	**End**		
	Reexam Timely Patent Owner's Stmnt in Resp to Order	1	16		
	Reexam Certificate of Service	17	17		
Warnings:					
Information:					
2	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	2021-08-16_ExANarayanaswamy-CV.pdf	856022 268e7257d23c733357486406d955081a491dd124	no	3
Warnings:					
Information:					
3	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	2021-08-16_Ex2001-DeclarationNarayanaswamy2.pdf	325649 9f5af464c54a337a5d232850744547772c27bc667	no	14
Warnings:					
Information:					
		Total Files Size (in bytes):	1549804		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/014,746	05/03/2021	7523497	50348.65	9957

31718 7590 06/17/2021

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

EXAMINER	
LAROSE, COLIN M	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
06/17/2021	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

HAYNES AND BOONE, LLP
IP SECTION
2323 VICTORY AVENUE
SUITE 700
DALLAS, TX 75219

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/014,746* .

PATENT UNDER REEXAMINATION *7523497* .

ART UNIT *3992* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

PTOL-465 (Rev.07-04)

Order Granting Request For Ex Parte Reexamination	Control No. 90/014,746	Patent Under Reexamination 7523497	
	Examiner Colin LaRose	Art Unit 3992	AIA (FITF) Status No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The request for *ex parte* reexamination filed 05/03/2021 has been considered and a determination has been made. An identification of the claims, the references relied upon, and the rationale supporting the determination are attached.

Attachments: a)☐ PTO-892, b)☐ PTO/SB/08, c)☑ Other: annotated IDS

1. ☑ The request for *ex parte* reexamination is GRANTED.

RESPONSE TIMES ARE SET AS FOLLOWS:

For Patent Owner's Statement (Optional): TWO MONTHS from the mailing date of this communication (37 CFR 1.530 (b)). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).**

For Requester's Reply (optional): TWO MONTHS from the **date of service** of any timely filed Patent Owner's Statement (37 CFR 1.535). **NO EXTENSION OF THIS TIME PERIOD IS PERMITTED.** If Patent Owner does not file a timely statement under 37 CFR 1.530(b), then no reply by requester is permitted.

/COLIN M LAROSE/ Primary Examiner, Art Unit 3992		

cc:Requester (if third party requester)

ORDER GRANTING REEXAMINATION OF U.S. PATENT 7,523,497

TABLE OF CONTENTS

I. Acknowledgement of Request for Reexamination 2
II. Prosecution History of the '497 Patent 3
III. Substantial New Question of Patentability 4
IV. Only Claims 1, 4, 7, 10, 13, and 16 Are Subject to Reexamination 6
V. Patent Owner Statement (Optional) 7
VI. Waiver of Right to File Patent Owner Statement 8
VII. Notice of Other Proceedings 8
VIII. Notice Regarding Patent Owner's Correspondence Address 9
IX. Conclusion 10

I. ACKNOWLEDGEMENT OF REQUEST FOR REEXAMINATION

An *ex parte* request for reexamination (hereinafter "Request") of claims 1, 4, 7, 10, 13, and 16 of U.S. Patent 7,523,497 (hereinafter "'497 Patent") was received on May 3, 2021, based on the following prior art patents and/or publications:

Stefan Savage et al., "Practical Network Support for IP Traceback," ACM SIGCOMM 2000: Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2000, pp. 295-306 ("Savage");

U.S. Patent 6,725,378 ("Schuba"); and

U.S. Patent 7,058,974 ("Maher").

II. PROSECUTION HISTORY OF THE '497 PATENT

The Request's summary of the prosecution history of the '497 patent appears to be accurate (see Request, pp. 13-20). Notably, during prosecution of the '497 patent, the Applicant amended claim 1 in response to a rejection under § 102 to include limitations specifying the path comprises all routers in the network via which the packets are routed to the computer:

> 1. (currently amended): A packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system comprising:
>
> means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;
>
> means for associating a maximum acceptable processing rate with each class of data packet received at said computer;
>
> means for said computer to find information for packets it receives regarding the path by which said packets came to said 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; and
>
> means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate.

See Application Control No. 10/841,064, Amendment dated June 13, 2008.

Claims 4, 7, 10, 13, and 16 were amended in substantially the same manner. In response to the Applicant's claim amendments, the Examiner allowed all pending claims and remarked

that the prior art does not teach "path forwarding along the entire path [from the attacker] to the victim, said path information encompassing the entire path through the associated routers." [1]

III. SUBSTANTIAL NEW QUESTION OF PATENTABILITY

The Request alleges the following substantial new questions of patentability (SNQs) based on the above-identified prior art:

SNQ A—Savage for claims 1, 4, 7, 10, 13, and 16 (see Request at pp. 24-28);

SNQ B—Maher and Savage for claims 4, 10, and 16 (see Request at pp. 28-31);

SNQ C—Maher and Schuba for claims 1, 4, 7, 10, 13, and 16 (see Request at pp. 31-33);

SNQ D—Savage, Maher, and Schuba for claims 1, 4, 7, 10, 13, and 16 (see Request at p. 33).

SNQ A—Savage for claims 1, 4, 7, 10, 13, and 16

The Request (pp. 24-28) alleges that Savage, which is directed to a technique for tracing anonymous packet-flooding attacks, raises a substantial new question of patentability for claims 1, 4, 7, 10, 13, and 16. The Request identifies Savage as teaching the limitations that previously distinguished the claims from the prior art during the initial examination, viz., finding information regarding the path received packets traversed via packet-marking by routers along the path leading to the host computer, in which the path comprises all routers in the network.

Specifically, the Request alleges Savage discloses such a limitation with the "Node append algorithm" of FIG. 2 on p. 299, which is described at Section 4.1 as providing "a

[1] *See* Application Control No. 10/841,064, Notice of Allowance and Fees Due dated December 23, 2008.

complete ordered list" of all the routers a received packet traversed upon arrival at the host computer.

Since Savage appears to provide new technological teachings that were missing in the prior art during the initial examination of the '497 patent and was not previously considered during the initial examination, Savage is considered important in determining the patentability of the claims and therefore does raise a substantial new question of patentability for claims 1, 4, 7, 10, 13, and 16.

SNQ B—Maher and Savage for claims 4, 10, and 16

The Request (pp. 28-31) alleges that the combination of Maher, which is directed to preventing denial of service attacks, and Savage, which is directed to a technique for tracing anonymous packet-flooding attacks, raises a substantial new question of patentability for claims 4, 10, and 16.

Since Savage alone is determined to raise a bona fide SNQ for claims 4, 10, and 16 according to SNQ A, the combination of Maher and Savage likewise raises a substantial new question of patentability for claims 4, 10, and 16.

SNQ C—Maher and Schuba for claims 1, 4, 7, 10, 13, and 16

The Request (pp. 31-33) alleges that the combination of Maher, which is directed to preventing denial of service attacks, and Schuba, which is directed to network protection for denial of service attacks, raises a substantial new question of patentability for claims 1, 4, 7, 10, 13, and 16. The Request does not appear to allege on p. 31-33 that either Maher or Schuba comprise teachings related to the limitations that previously distinguished the claims from the

prior art during the initial examination, viz., finding information regarding the path received packets traversed via packet-marking by routers along the path leading to the host computer, in which the path comprises all routers in the network. Although Maher and Schuba are considered relevant prior art, the Request does not establish that the combination of the two references raises a bona fide substantial new question of patentability for claims 1, 4, 7, 10, 13, and 16.

SNQ D—Savage, Maher, and Schuba for claims 1, 4, 7, 10, 13, and 16

The Request (p. 33) alleges that the combination of Savage, Maher, and Schuba raises a substantial new question of patentability for claims 1, 4, 7, 10, 13, and 16.

Since Savage alone is determined to raise a bona fide SNQ for these claims according to SNQ A, the combination of Savage, Maher, and Schuba likewise raises a substantial new question of patentability for claims 1, 4, 7, 10, 13, and 16.

The Request to reexamine claims 1, 4, 7, 10, 13, and 16 is **GRANTED** on the basis of SNQs A, B, and D.

IV. ONLY CLAIMS 1, 4, 7, 10, 13, AND 16 ARE SUBJECT TO REEXAMINATION

Since Requester did not request reexamination of claims 2, 3, 5, 6, 8, 9, 11, 12, 14, 15, 17, and 18, and did not assert the existence of a substantial new question of patentability (SNQ) for such claims (See 35 U.S.C. §31 l(b)(2); See also 37 CFR 1.915b and 1.923), such claims will not be reexamined. This matter was squarely addressed in *Sony Computer Entertainment*

America Inc., et al. v. Jon W. Dudas, Civil Action No. 1:05CV1447 (E.D.Va. May 22, 2006), Slip Copy, 2006 WL 1472462. The District Court upheld the Office's discretion to not reexamine claims in an *inter partes* reexamination proceeding other than those claims for which reexamination had specifically been requested. The Court stated:

> "To be sure, a party may seek, and the PTO may grant, *inter partes* review of each and every claim of a patent. Moreover, while the PTO in its discretion may review claims for which *inter partes* review was not requested, nothing in the statute compels it to do so. To ensure that the PTO considers a claim for *inter partes* review, 35 U.S.C. § 31 l(b)(2) requires that the party seeking reexamination demonstrate why the PTO should reexamine each and every claim for which it seeks review. Here, it is undisputed that Sony did not seek review of every claim under the '213 and '333 patents. Accordingly, Sony cannot now claim that the PTO wrongly failed to reexamine claims for which Sony never requested review, and its argument that AIPA compels a contrary result is unpersuasive."

V. PATENT OWNER STATEMENT (OPTIONAL)

In response to this Order for Reexamination, the Patent Owner is given a **two (2) month** period to file an optional Patent Owner Statement in accordance with 37 C.F.R. 1.530(b) and (c). The Patent Owner Statement must clearly point out why the patent claims are believed to be patentable, considering the cited prior art patents or printed publications alone or in any reasonable combination. In addition, the Patent Owner may utilize the Patent Owner Statement to introduce amendments. A copy of the Patent Owner Statement must be served on the Third Party Requester. See MPEP § 2249.

If a Patent Owner Statement is timely filed and served on the Third Party Requester, the Third Party is given the opportunity to reply within two (2) months from the date of service in

accordance with 37 C.F.R. 1.535. The reply need not be limited to the issues raised in the Patent Owner Statement and may include additional prior art patents and printed publications as well as any issue appropriate for reexamination. A copy of the reply must be served on the Patent Owner. If no Patent Owner Statement is filed, no reply is permitted from the Third Party Requester. See MPEP § 2251.

VI. WAIVER OF RIGHT TO FILE PATENT OWNER STATEMENT

In a reexamination proceeding, Patent Owner may waive the right under 37 C.F.R. 1.530 to file a Patent Owner Statement for the purposes of expediting prosecution; see MPEP § 2249. The document should contain a statement that Patent Owner waives the right under 37 C.F.R. 1.530 to file a Patent Owner Statement and proof of service in the manner provided by 37 C.F.R. 1.248, if the request for reexamination was made by a third party requester; see 37 C.F.R. 1.550(f). The Patent Owner may consider using the following statement in a document waiving the right to file a Patent Owner Statement:

WAIVER OF RIGHT TO FILE PATENT OWNER STATEMENT

Patent Owner hereby waives the right under 37 C.F.R. 1.530 to file a Patent Owner Statement.

VII. NOTICE OF OTHER PROCEEDINGS

The Patent Owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving Patent No. 7,523,497 throughout the course of this reexamination proceeding. The third party

Requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

VIII. NOTICE REGARDING PATENT OWNER'S CORRESPONDENCE ADDRESS

37 C.F.R. § 1.33(c) states:

> (c) All notices, official letters, and other communications for the patent owner or owners in a reexamination or supplemental examination proceeding will be directed to the correspondence address in the patent file.

The correspondence address for any pending reexamination proceeding not having the same correspondence address as that of the patent is, by way of this revision to 37 CFR 1.33(c), automatically changed to that of the patent file as of the effective date.

This change is effective for any reexamination proceeding which is pending before the Office as of May 16, 2007, including the present reexamination proceeding, and to any reexamination proceeding which is filed after that date.

Parties are to take this change into account when filing papers, and direct communications accordingly.

In the event the patent owner's correspondence address listed in the papers (record) for the present proceeding is different from the correspondence address of the patent, it is strongly encouraged that the patent owner affirmatively file a Notification of Change of Correspondence Address in the reexamination proceeding and/or the patent (depending on which address patent owner desires), to conform the address of the proceeding with that of the patent and to clarify the record as to which address should be used for correspondence.

Telephone Numbers for reexamination inquiries:

Reexamination	(571) 272-7703
Central Reexam Unit (CRU)	(571) 272-7705

IX. CONCLUSION

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.550(a)). Extensions of time in *ex parte* reexamination proceedings are provided for in 37 CFR 1.550(c). See MPEP § 2265.

All correspondence relating to this *ex parte* reexamination proceeding should be directed:

By Mail to: Mail Stop *Ex Parte* Reexam
Attn: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

By EFS: Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

For EFS-Web transmissions, 37 CFR 1.8(a)(1)(i) (C) and (ii) state that correspondence (except for a request for reexamination and a corrected replacement request for reexamination) will be considered timely if (a) it is transmitted via the Office's electronic filing system in accordance with 37 CFR 1.6(a)(4), and (b) it includes a certificate of transmission for each piece of correspondence stating the date of transmission, which is prior to the expiration of the set period of time in the Office action.

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Colin LaRose whose telephone number is 571-272-7423.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew J. Fischer can be reached at 571-272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-9900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you

would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/COLIN M LAROSE/
Primary Examiner, Art Unit 3992

Conferees:

/NICK CORSARO/
Primary Examiner, Art Unit 3992

/M.F/
Supervisory Patent Examiner, Art Unit 3992

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,746	7523497
	Examiner	Art Unit
	Colin LaRose	3992

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
review prosecution history of U.S. 7,523,497	06/10/2021	CML

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/COLIN M LAROSE/ Primary Examiner, Art Unit 3992	

Reexamination	Application/Control No.	Applicant(s)/Patent Under Reexamination
	90/014,746	7523497
	Certificate Date	Certificate Number

Requester Correspondence Address: ☐ Patent Owner ☑ Third Party
HAYNES AND BOONE, LLP IP SECTION 2323 VICTORY AVENUE SUITE 700 DALLAS, TX 75219

LITIGATION REVIEW ☑	CML (examiner initials)	04 May 2021 (date)
Case Name		Director Initials
n/a		

COPENDING OFFICE PROCEEDINGS	
TYPE OF PROCEEDING	NUMBER
n/a	

/COLIN M LAROSE/ Primary Examiner, Art Unit 3992	

In place of PTO-1449 Form	U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE			*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Application Number	In Ex Parte Reexamination of 7,523,497
				Filing Date	Herewith
				First Inventor Name	Donald N. Cohen
				Art Unit	TBD
				Examiner Name	TBD
SHEET	1	OF	1	Attorney Docket Number	50348.65

U. S. PATENTS				
Examiner's Initials	**Cite No.**	**Document Number**	**Issue Date MM-DD-YYYY**	**Name of Patentee or Applicant of Cited Document**
	Ex. 1006	7,058,974	2006-06-06	Maher et al.
	Ex. 1007	6,725,378	2004-04-20	Schuba et al.

U. S. PATENT APPLICATION PUBLICATIONS				
Examiner's Initials	**Cite No.**	**Document Number**	**Publication Date MM-DD-YYYY**	**Name of Patentee or Applicant of Cited Document**

FOREIGN PATENT DOCUMENTS					
Examiner's Initials	**Cite No.**	**Foreign Patent Document (Country Code – Number – Kind)**	**Publication Date MM-DD-YYYY**	**Patentee or Applicant of Cited Document**	**Translation Y/N**

NON-PATENT LITERATURE DOCUMENTS		
Examiner's Initials	**Cite No.**	**Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published**
	Ex. 1005	Savage et al., "Practical Network Support for IP Traceback," SIGCOMM'00: Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2000, pp. 295-306 ("*Savage*")

Examiner Signature	/COLIN M LAROSE/	Date Considered	06/11/2021

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

Customer No. 27683

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /C.M.L/

Bibliographic Data

Application No: 90/014,746

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /COLIN M LAROSE/ (Examiner's Signature) | (Initials)

Title: PACKET FLOODING DEFENSE SYSTEM

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
05/03/2021	726	3992	50348.65
RULE			

APPLICANTS

INVENTORS

7523497,

PACSEC3, LLC, HOUSTON, TX, UNITED STATES

RAGHAV BAJAJ (3RD PTY REQ.), DALLAS, TX, UNITED STATES

CONTINUING DATA

This application is a REX of 10841064 05/07/2004 PAT 7523497

10841064 is a CON of 09715813 11/16/2000 PAT 6789190

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

STATE OR COUNTRY

ADDRESS

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

FILING FEE RECEIVED

$225

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/014,746	05/03/2021	7523497	50348.65	9957

31718 7590 05/26/2021

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

EXAMINER	
LAROSE, COLIN M	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
05/26/2021	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

HAYNES AND BOONE
IP SECTION
2323 VICTORY AVENUE
SUITE 700
DALLAS, TX 75219

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/014,746* .

PATENT UNDER REEXAMINATION *7523497* .

ART UNIT *OCRU* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

PTOL-465 (Rev.07-04)

Ex Parte Reexamination Interview Summary – Pilot Program for Waiver of Patent Owner's Statement	**Control No.** 90/014,746	**Patent Under Reexamination is Requested** 7523497	
	Examiner COLIN LAROSE	**Art Unit** 3992	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

All participants (USPTO official and patent owner):

(1) SHANETTE BROWN (3) _____

(2) _____ (4) _____

Date of Telephonic Interview: 18 May 2021.

A. The USPTO official requested waiver of the patent owner's statement pursuant to the pilot program for waiver of patent owner's statement in *ex parte* reexamination proceedings.*

☐ The patent owner **agreed** to waive its right to file a patent owner's statement under 35 U.S.C. 304 in the event reexamination is ordered for the above-identified patent.

☐ The patent owner **did not agree** to waive its right to file a patent owner's statement under 35 U.S.C. 304 at this time.

☑ USPTO personnel were unable to reach the patent owner.**

B. The Patent Owner of record telephoned the Office and indicated they would like to participate in the pilot program for waiver of patent owner's statement in *ex parte* reexamination proceedings.*

☐ The Patent owner of record telephoned the Office and **agreed** to waive its right to file a patent owner's statement under 35 U.S.C. 304 in the event reexamination is ordered for the above-identified patent.

The patent owner is not required to file a written statement of this telephone communication under 37 CFR 1.560(b) or otherwise. However, any disagreement as to this interview summary must be brought to the immediate attention of the USPTO, and no later than one month from the mailing date of this interview summary. Extensions of time are governed by 37 CFR 1.550(c).

*For more information regarding this pilot program, see *Pilot Program for Waiver of Patent Owner's Statement in Ex Parte Reexamination Proceedings, 75 Fed. Reg.* 47269 (August 5, 2010), available on the USPTO Web site at http://www.uspto.gov/patents/law/notices/2010.jsp.

**The patent owner may contact the USPTO personnel at (571) 272-7705 or at the telephone number provided below if the patent owner decides to waive the right to file a patent owner's statement under 35 U.S.C. 304.

/SHANETTE BROWN/ (571)272-6632
Signature and telephone number of the USPTO official, who contacted, was contacted by, or attempted to contact the patent owner.

cc: Requester (if third party requester)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
90/014,746	05/03/2021	7523497

CONFIRMATION NO. 9957

REEXAM ASSIGNMENT NOTICE

31718
BELASCO JACOBS & TOWNSLEY, PC
6701 Center Drive West
14th Floor
Los Angeles, CA 90045

OC000000125520098

Date Mailed: 05/12/2021

NOTICE OF ASSIGNMENT OF REEXAMINATION REQUEST

The above-identified request for reexamination has been assigned to Art Unit 3992. All future correspondence to the proceeding should be identified by the control number listed above and directed to the assigned Art Unit.

A copy of this Notice is being sent to the latest attorney or agent of record in the patent file or to all owners of record. (See 37 CFR 1.33(c)). If the addressee is not, or does not represent, the current owner, he or she is required to forward all communications regarding this proceeding to the current owner(s). An attorney or agent receiving this communication who does not represent the current owner(s) may wish to seek to withdraw pursuant to 37 CFR 1.36 in order to avoid receiving future communications. If the address of the current owner(s) is unknown, this communication should be returned within the request to withdraw pursuant to Section 1.36.

NOTICE OF USPTO EX PARTE REEXAMINATION PATENT OWNER STATEMENT WAIVER PROGRAM

The USPTO has implemented a pilot program where, after a reexamination proceeding has been granted a filing date and before the examiner begins his or her review, the patent owner may orally waive the right to file a patent owner's statement. See *"Pilot Program for Waiver of Patent Owner's Statement in Ex Parte Reexamination Proceedings,"* 75 FR 47269 (August 5, 2010). One goal of the pilot program is to reduce the pendency of reexamination proceedings and improve the efficiency of the reexamination process.

Ordinarily when ex parte reexamination is ordered, the USPTO must wait until after the receipt of the patent owner's statement and the third party requester's reply, or after the expiration of the time period for filing the statement and reply (a period that can be as long as 5 to 6 months), before mailing a first determination of patentability. The USPTO's first determination of patentability is usually a first Office action on the merits or a Notice of Intent to Issue Reexamination Certificate (NIRC).

Under the pilot program, the patent owner's oral waiver allows the USPTO to act on the first determination of patentability immediately after determining that reexamination will be ordered, and in a suitable case issue the reexamination order and the first determination of patentability (which could be a NIRC if the claims under reexamination are confirmed) at the same time.

Benefits to the Patent Owner for participating in this pilot program include reduction in pendency.

To participate in this pilot program, Patent Owners may contact the USPTO's Central Reexamination Unit (CRU) at 571-272-7705. The USPTO will make the oral waiver of record in the reexamination file in an interview summary and a copy will be mailed to the patent owner and any third party requester.

cc: Third Party Requester(if any)
HAYNES AND BOONE, LLP
2323 VICTORY AVEUENE
SUITE 700
DALLAS, TX 75219

/tplovelace/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
90/014,746	05/03/2021	7523497

CONFIRMATION NO. 9957

HAYNES AND BOONE, LLP
2323 VICTORY AVEUENE
SUITE 700
DALLAS, TX 75219

REEXAMINATION REQUEST NOTICE

OC000000125520096

Date Mailed: 05/12/2021

NOTICE OF REEXAMINATION REQUEST FILING DATE

(Third Party Requester)

Requester is hereby notified that the filing date of the request for reexamination is 05/03/2021, the date that the filing requirements of 37 CFR § 1.510 were received.

A decision on the request for reexamination will be mailed within three months from the filing date of the request for reexamination. (See 37 CFR 1.515(a)).

A copy of the Notice is being sent to the person identified by the requester as the patent owner. Further patent owner correspondence will be the latest attorney or agent of record in the patent file. (See 37 CFR 1.33). Any paper filed should include a reference to the present request for reexamination (by Reexamination Control Number).

cc: Patent Owner
31718
BELASCO JACOBS & TOWNSLEY, PC
6701 Center Drive West
14th Floor
Los Angeles, CA 90045

/tplovelace/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9957

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
90/014,746	05/03/2021 RULE	726	3992	50348.65

APPLICANTS

INVENTORS

7523497, Residence Not Provided;
PACSEC3, LLC, HOUSTON, TX;
RAGHAV BAJAJ (3RD PTY REQ.), DALLAS, TX;
HAYNES AND BOONE, LLP, DALLAS, TX

**** CONTINUING DATA ***************************

This application is a REX of 10/841,064 05/07/2004 PAT 7523497
which is a CON of 09/715,813 11/16/2000 PAT 6789190

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

Foreign Priority claimed ❑ Yes ❑ No 35 USC 119(a-d) conditions met ❑ Yes ❑ No Verified and Acknowledged _____ Examiner's Signature	❑ Met after Allowance _____ Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
				18	12

ADDRESS

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

TITLE

PACKET FLOODING DEFENSE SYSTEM

FILING FEE RECEIVED		
12600	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

BIB (Rev. 05/07).

Patent Assignment Abstract of Title

Total Assignments: 2

Application #: 10841064 **Filing Dt:** 05/07/2004 **Patent #:** 7523492 **Issue Dt:** 04/21/2009
PCT #: NONE **Intl Reg #:** **Publication #:** US20040230839 **Pub Dt:** 11/18/2004
Inventor: Donald N. Cohen
Title: PACKET FLOODING DEFENSE SYSTEM

Assignment: 1

Reel/Frame: 030220 / 0075 **Received:** 04/15/2013 **Recorded:** 04/15/2013 **Mailed:** 04/17/2013 **Pages:** 2
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).
Assignor: COHEN, DONALD N. **Exec Dt:** 03/20/2013
Assignee: COMPUTING SERVICES SUPPORT SOLUTIONS, INC.
5777 WEST CENTURY BOULEVARD
SUITE 1185
LOS ANGELES, CALIFORNIA 90045
Correspondent: DAVID A. BELASCO
BELASCO JACOBS & TOWNSLEY, LLP
14TH FLOOR
6701 CENTER DRIVE WEST
LOS ANGELES, CA 90045

Assignment: 2

Reel/Frame: 053526 / 0117 **Received:** 08/18/2020 **Recorded:** 08/18/2020 **Mailed:** 08/19/2020 **Pages:** 2
Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).
Assignor: COMPUTING SERVICES SUPPORT SOLUTIONS, INC. **Exec Dt:** 08/12/2020
Assignee: PACSEC3 LLC
5218 CHANDLER STREET
HOUSTON, TEXAS 77007
Correspondent: CARLOS GORRICHATEGUI
5218 CHANDLER STREET
HOUSTON, TX 77007

Search Results as of: 05/05/2021 02:24 PM

If you have any comments or questions concerning the data displayed, contact PRD / Assignments at 571-272-3350. v.2.6
Web interface last modified: Jun 26, 2017 v.2.6

Litigation Search Report CRU 3999

Reexamination Control No. 90/014,746

To: EXAMINER	From: Shanette Brown
Location: CRU	Location: CRU 3999 / REM 4C75
Art Unit: 3999	Phone: (571) 272-6632
Date: 05/04/2021	E-mail: Shanett.brown@uspto.gov

Search Notes

U.S. Patent No. 7,523,497

1. Performed a KeyCite Search in Westlaw, which retrieves all history on the patent including any litigation.
2. Performed a search on the patent in Lexis CourtLink for any open dockets or closed cases.
3. Performed a search in Lexis in the Federal Courts and Administrative Materials databases for any cases found.
4. Performed a search in Lexis in the IP Journal and Periodicals database for any articles on the patent.
5. Performed a search in Lexis in the news databases for any articles about the patent or any articles about litigation on this patent.

Litigation: No Cases Found

Paper No.

Citing References (20)

Treatment	Title	Date	Type	Depth	Headnote(s)
Mentioned by	**1. Packet flooding defense system** LitAlert P2021-17-51 ... Date: 04/21/2021 Subsequent Action: 04/21/2021 Action Taken: CAUSE - 35 USC 145 - COMPLAINT FOR PATENT INFRINGEMENT Notes: none Other Patents: US 7047564 US 7523497 Other Trademarks: none See LitAlert No: none ...	Apr. 21, 2021	Lit Alert		—
Mentioned by	**2. Packet flooding defense system** LitAlert P2021-17-52 ... Date: 04/21/2021 Subsequent Action: 04/21/2021 Action Taken: CAUSE - 35 USC 145 - COMPLAINT FOR PATENT INFRINGEMENT Notes: none Other Patents: US 7047564 US 7523497 Other Trademarks: none See LitAlert No: none ...	Apr. 21, 2021	Lit Alert		—
Mentioned by	**3. Packet flooding defense system** LitAlert P2021-17-54 ... Date: 04/21/2021 Subsequent Action: 04/21/2021 Action Taken: CAUSE - 15 USC 1126 - COMPLAINT FOR PATENT INFRINGEMENT Notes: none Other Patents: US 7047564 US 7523497 Other Trademarks: none See LitAlert No: none ...	Apr. 21, 2021	Lit Alert		—
Mentioned by	**4. Packet flooding defense system** LitAlert P2021-17-55 ... Date: 04/21/2021 Subsequent Action: 04/21/2021 Action Taken: CAUSE - 28 USC 1338 - COMPLAINT FOR PATENT INFRINGEMENT Notes: none Other Patents: US 7047564 US 7523497 Other Trademarks: none See LitAlert No: none ...	Apr. 21, 2021	Lit Alert		—
Mentioned by	**5. Packet flooding defense system** LitAlert P2020-52-32 ... Date: 12/14/2020 Subsequent Action: 12/14/2020 Action Taken: CAUSE - 28 USC 1338 - COMPLAINT FOR PATENT INFRINGEMENT Notes: none Other Patents: US 7047564 US 7523497 Other Trademarks: none See LitAlert No: none ...	Dec. 14, 2020	Lit Alert		—
Mentioned by	**6. Packet flooding defense system** LitAlert P2020-41-11 ... Date: 10/02/2020 Subsequent Action: 10/02/2020 Action Taken: CAUSE - 28 USC 1338 - COMPLAINT FOR PATENT INFRINGEMENT Notes: none Other Patents: US 7047564 US 7523497 Other Trademarks: none See LitAlert No: none ...	Oct. 02, 2020	Lit Alert		—

© Copyright 2021 Thomson Reuters/West. No Claim to Orig. US Gov. Works

Treatment	Title	Date	Type	Depth	Headnote(s)
Mentioned by	**7. Packet flooding defense system** LitAlert P2020-41-16 ... Date: 10/02/2020 Subsequent Action: 10/02/2020 Action Taken: CAUSE - 15 USC 1126 - COMPLAINT FOR PATENT INFRINGEMENT Notes: none Other Patents: US 7047564 US 7523497 Other Trademarks: none See LitAlert No: none ...	Oct. 02, 2020	Lit Alert		—
—	**8. PACKET FLOODING DEFENSE SYSTEM THAT IS DISTRIBUTED AMONG COOPERATING SITES AND ROUTERS AND ACTS TO IDENTIFY ROUTERS FORWARDING UNWANTED DATA AND THEN TO REDUCE THE RATE AT WHICH THE DATA IS FORWARDED** Out Of Plan DWPI 2003-168090 ... said information to allocate the processing rate available for packets of each class in a desired way.First Derwent Appearance:2004.77 Publication No. (Derwent): US 7523497 B2 Original Title (English):PACKET FLOODING DEFENSE SYSTEM Publication Date:2009-04-21 Application No.:US 841064 Application Date:2004-05-07 Inventor(s ...	Nov. 16, 2000	DWPI	—	—
—	**9. RF 053526/0117** Out Of Plan ... App. 20030084317 Published Application Date 2003-05-01 Application Number 10/001349 Application Date 2001-10-31 Title PACKET FLOODING DEFENSE SYSTEM Granted Patent Number US Pat. 7523497 Granted Patent Date 2009-04-21 Published Application Number US Pat. App. 20040230839 Published Application Date 2004-11-18 Application Number 10/841064 ...	Aug. 18, 2020	Assignments	—	—
—	**10. RF 030220/0075** Out Of Plan ... DRIVE WEST LOS ANGELES, CA 90045 Number of Pages 2 Last Modified 2013-04-17 PATENTS AFFECTED Title PACKET FLOODING DEFENSE SYSTEM Granted Patent Number US Pat. 7523497 Granted Patent Date 2009-04-21 Published Application Number US Pat. App. 20040230839 Published Application Date 2004-11-18 Application Number 10/841064 ...	Apr. 15, 2013	Assignments	—	—
—	**11. PacSec3, LLC v. Palo Alto Networks, Inc.**	Apr. 21, 2021	Docket Summaries	—	—
—	**12. PacSec3, LLC v. Cisco Systems, Inc.**	Apr. 21, 2021	Docket Summaries	—	—
—	**13. PacSec3, LLC v. Juniper Networks, Inc.**	Apr. 21, 2021	Docket Summaries	—	—
—	**14. PacSec3, LLC v. McAfee, LLC**	Apr. 21, 2021	Docket Summaries	—	—
—	**15. PacSec3, LLC v. F5 Networks, Inc.**	Dec. 14, 2020	Docket Summaries	—	—
—	**16. PacSec3, LLC v. NetScout, Inc.**	Oct. 02, 2020	Docket Summaries	—	—
—	**17. PacSec3, LLC v. F5 Networks, Inc.**	Oct. 02, 2020	Docket Summaries	—	—

© Copyright 2021 Thomson Reuters/West. No Claim to Orig. US Gov. Works

Treatment	Title	Date	Type	Depth	Headnote(s)
—	**18. DETERMINING THE LIKELIHOOD OF TRAFFIC BEING LEGITIMATELY RECEIVED AT A PROXY SERVER IN A CLOUD-BASED PROXY SERVICE** Out Of Plan US PAT 10581904 , U.S. PTO Utility Message(s) are received from each one of multiple proxy servers, which are anycasted to the same IP address, that indicate source IP addresses of packets that are received that are... ... 2008/04 Ramachandran et al.cited by applicant US United States US 7444404 B2 2008/10 Wetherall et al.cited by applicant US United States US 7523497 B2 2009/04 Cohen cited by applicant US United States US 7539191 B1 2009/05 Jacobson 370/392 H04L 63/1441 cited by examiner ...	Mar. 03, 2020	Patents	—	—
—	**19. MITIGATING A DENIAL-OF-SERVICE ATTACK IN A CLOUD-BASED PROXY SERVICE** Out Of Plan US PAT 10511624 , U.S. PTO Utility A proxy server in a cloud-based proxy service receives a message that indicates that a domain, whose traffic passes through the proxy server, may be under a denial-of-service (DoS)... ... 2008/04 Ramachandran et al.cited by applicant US United States US 7444404 B2 2008/10 Wetherall et al.cited by applicant US United States US 7523497 B2 2009/04 Cohen cited by applicant US United States US 7539191 B1 2009/05 Jacobson et al.cited by applicant US United States ...	Dec. 17, 2019	Patents	—	—
—	**20. MITIGATING A DENIAL-OF-SERVICE ATTACK IN A CLOUD-BASED PROXY SERVICE** Out Of Plan US PAT 10129296 , U.S. PTO Utility A proxy server in a cloud-based proxy service receives a message that indicates that a domain, whose traffic passes through the proxy server, may be under a denial-of-service (DoS)... ... 2008/04 Ramachandran et al.cited by applicant US United States US 7444404 B2 2008/10 Wetherall et al.cited by applicant US United States US 7523497 B2 2009/04 Cohen cited by applicant US United States US 7539191 B1 2009/05 Jacobson et al.cited by applicant US United States ...	Nov. 13, 2018	Patents	—	—

© Copyright 2021 Thomson Reuters/West. No Claim to Orig. US Gov. Works

CourtLink Client: -None- History Help More

Results for: US PAT=7523497 | Actions Edit Search

Dockets 0

Narrow By

Open or Unknown or Closed

Clear

Filter Results

Dockets (0)

No documents found in **Dockets** filtered by **Open or Unknown or Closed** .

Try the following:

- Remove one or more filters: **Open or Unknown or Closed**
- Modify your search (edit or remove some search terms or add synonyms).
- Check for spelling errors.
- Use the options available from the **Actions** menu above to modify your search.
- Note: Some content may not be visible based on the restrictions of your subscription.

LexisNexis About Privacy Policy Cookie Policy Terms & Conditions RELX™

Copyright © 2021 LexisNexis.

US7523497B2 - Packet flooding defense system

Original

Bibliographic information & Images

Publication number and date
US7523497B2
2009-04-21

Granted

Application number and date
US10841064 (/api/control?query=AN:("US10841064")&autosearch=true)
2004-05-07

Priority number and date
US10841064 (/api/control?query=PRN:("US10841064")&autosearch=true)
2004-05-07

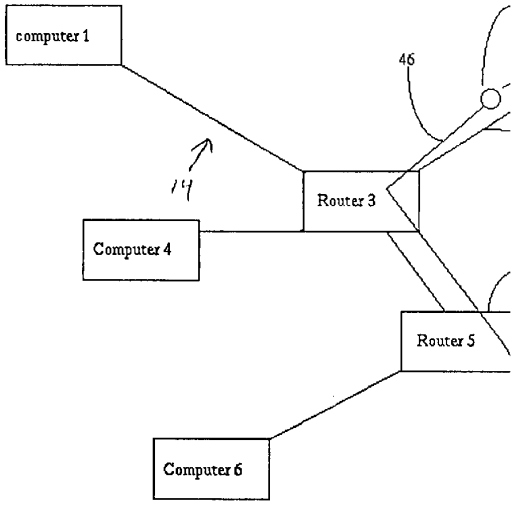
Original assignee
COHEN DONALD N (/api/control?query=pa:("COHEN%20DONALD%20N")&autosearch=true)

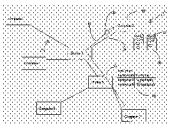
Current assignee
PACSEC3 LLC (/api/control?query=pacu:("PACSEC3%20LLC")&autosearch=true)

Inventor
Donald N. Cohen (/api/control?query=in:("Donald%20N.%20Cohen")&autosearch=true)

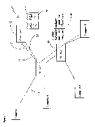
Legal representative
David A. Belasco (/api/control?query=ag:("David%20A.%20Belasco")&autosearch=true)

1/10 Clipped image









Abstract

The invention prevents “packet flooding”, where an attacker uses up all available bandwidth to a victim witl attacks. The defense is distributed among cooperating sites and routers. The sites identify data they don't v then ask these routers to reduce the rate at which such data is forwarded. Variations of the defense protect use up some service offered by a site.

Original

Claims

1. A packet flooding defense system for a network comprising a plurality of host computers, routers, comm classifying data packets received at a host computer into wanted data packets and unwanted data packets; data packet received at said computer; means for said computer to find information for packets it receives provided by routers leading to said host computer; said path comprising all routers in said network via whi said information to allocate the processing rate available for unwanted data packets to be less than or equ

2. A packet flooding defense system for a network comprising a plurality of host computers, routers, comm classifying data packets received at a host computer into wanted data packets and unwanted data packets; which said data packets are routed to said computer; means for associating a maximum acceptable proces computer to determine the rate at which data packets of each class are transmitted from a router to said c acceptable transmission rate for data packets being transmitted to said computer; means for said router to and means in said computer for keeping the rate of data packet transmissions received at said computer b control of the rate of transmission of data packets from said router, and freeing a portion of the network pr

3. A packet flooding defense system as described in claim 2 , wherein: said router receives information rega transmitted to said computer; and said router controls the rate of transmission of each class of data packet

4. A packet flooding defense system for a network comprising a plurality of host computers, routers, comm classifying data packets received at a router into wanted data packets and unwanted data packets; means f packet received at said router; means for said router to find information for packets it receives regarding th routers leading to said host computer; said path comprising all routers in said network via which said packe said information to allocate the transmission rate for unwanted data packets to be less than equal to said n

5. A packet flooding defense system for a network comprising a plurality of host computers, routers, comm classifying data packets received at a first router into wanted data packets and unwanted data packets; saic said data packets are routed to said computer; means for associating a maximum acceptable transmission router to determine the rate at which data packets of each class are transmitted from a second router to sa maximum acceptable transmission rate for data packets being transmitted to said first router; means for sa second router to said first router; and means in said first router for keeping the rate of data packet transmi rate for unwanted data packets by said control of the rate of transmission of data packets from said second said first router.

6. A packet flooding defense system as described in claim 5 , wherein: said second router receives informati being transmitted to said first router; and said second router controls the rate of transmission of each class

7. A method of providing packet flooding defense for a network comprising a plurality of host computers, r the steps of: determining a path by which data packets arrive at a host computer via packet marks provided network via which said packets are routed to said computer; classifying data packets received at said host c a maximum acceptable processing rate with each class of data packet received at said host computer; and processing rate for unwanted data packets.

8. A method of providing packet flooding defense for a network comprising a plurality of host computers, r the steps of: classifying data packets received at a host computer into wanted data packets and unwanted d network via which said data packets are routed to said computer; associating a maximum acceptable proce the rate at which data packets of each class are transmitted from a router to said computer; receiving a ma computer in said router; and controlling the rate of transmission of data packets from said router to said cc are kept below the maximum acceptable processing rate for each data packet class; and freeing a portion c

9. A method as described in claim 8 , in which: said router receives information regarding maximum accept computer; and said router controls the rate of transmission of each class of data packet to said computer.

10. A method of providing packet flooding defense for a network comprising a plurality of host computers, comprising the steps of: determining a path by which data packets arrive at said router via packet marks pr in said network via which said packets are routed to said computer; classifying data packets received at saic path; associating a maximum acceptable transmission rate with each class of data packet received at said r acceptable transmission rate for unwanted data packets.

11. A method of providing packet flooding defense for a network comprising a plurality of host computers, comprising the steps of: classifying data packets received at a first router into wanted data packets and unv said network via which said data packets are routed to said computer; associating a maximum acceptable t determining by said first router of the rate at which data packets of each class are transmitted from a secor regarding maximum acceptable transmission rate for data packets being transmitted to said first router; ar from said second router to said first router so that said rate of transmission is below the maximum accepta network providing data packet transmission to said first router.

12. A method as described in claim 11 , in which: said second router receives information regarding maximu said first router; and said second router controls the rate of transmission of each class of data packets to sa

13. A packet flooding defense system for a network comprising a plurality of host computers, routers, comr determining a path by which data packets arrive at a host computer via packet marks provided by routers le which said packets are routed to said computer; means for classifying data packets received at said host co

Cloudflare, Inc. Exhibit 1003 Page 302

assigning a maximum acceptable processing rate to each class of data packet; and means for allocating a p said unwanted data packets.

14. A packet flooding defense system for a network comprising a plurality of host computers, routers, comr classifying data packets received at a host computer into wanted data packets and unwanted data packets; which said data packets are routed to said computer; means for associating a maximum acceptable proces computer to determine the rate at which data packets of each class are transmitted from a router to said cc acceptable transmission rate for data packets being transmitted to said computer; and means for said rout computer so that the rate of data packet transmissions received at said computer is kept below the maximu the network providing data packet transmission to said computer.

15. A packet flooding defense system as described in claim 14 , in which: said router receives information re transmitted to said computer; and said router controls the rate of transmission of each class of data packet

16. A packet flooding defense system for a network comprising a plurality of host computers, routers, comr router to determine a path by which said packets came to said router via packet marks provided by routers said packets are routed to said computer; means for classifying data packets received at said router into wa maximum acceptable transmission rate with each class of data packet received at said router; and means fc than equal to said maximum acceptable processing rate.

17. A packet flooding defense system for a network comprising a plurality of host computers, routers, comr classifying data packets received at a first router into wanted data packets and unwanted data packets; saic said data packets are routed to said computer; means for associating a maximum acceptable transmission router to determine the rate at which data packets of each class are transmitted from a second router to sa maximum acceptable transmission rate for data packets being transmitted to said first router; and means f second router to said first router so that the rate of data packet transmission received at said first router is and freeing a portion of the network providing data packet transmission to said first router.

18. A packet flooding defense system as described in claim 17 , wherein: said second router receives inform packet being transmitted to said first router; and said second router controls the rate of transmission of ea

Original

Families

INPADOC

This section contains all family relations of this particular document. For more information about the differe

Extended (5)	Complete (2)	Main (2)	Domestic (2)	Application number
2000-11-16 Priority claims US09715813 US10841064	2004-05-07 Priority claims US09715813 US10841064	2004-05-07 Priority claims US09715813 US10841064	2004-05-07	10841064 US10841064
				10841064 US10841064
	2000-11-16 Priority claims US09715813	2000-11-16 Priority claims US09715813	2000-11-16	US01045304 WOUS01045304
				US01045304 WOUS01045304
			2000-11-16	09715813 US09715813

Description

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This Application is a continuation of U.S. patent application Ser. No. 09/715,813, filed 11/16/2000 now

FIELD OF INVENTION

[0002] The invention pertains to network data transmission controls. More particularly, the invention relate computers or routers connected to a network.

BACKGROUND OF THE INVENTION

[0003] Various types of systems have been developed for handling unwanted network data transmission in Crayford et al. discloses a method that verifies the integrity of data transmitted over a network by comparir network repeaters. Where the destination address fails to match the stored end station addresses, the data

[0004] U.S. Pat. No. 6,044,402 issued to Jacobson et al., describes a system in which the only data packets th that satisfy the blocking policies stored by the blocking data structure. Thus only, "pre-approved" data can discloses a system that relies upon a stored list of acceptable packet identifiers at each node in the network the acceptability of data packets based upon a destination address/source address match and will disrupt a discloses a system that uses source and destination address matching to determine if packets should be tra network. It also employs a system where an end station can be disabled by a program that determines that variations exist, the above-described designs for handling unwanted network data transmissions are typica

[0005] U.S. Pat. No. 5,367,523 to Chang et al. discloses an end-to-end, closed loop flow and congestion contı rate response messages between data senders and receivers to allow the sender to adjust the data rate to backed on data packets and result in changes in the input data rate in a direction to optimize data throughp reduce data input and reduce data input drastically, respectively. Incremental changes in data input are alte operating point than when closer to the optimum operating point. Chang, et al, is intended for end-to-end receiver in solving the problem. In a packet flooding defense, the sender, who is the attacker, will never coc source/destination address pairs in the packet. Chang, et al, assume this information is accurate. In an atta to confound the defense if it uses information the attacker controls, such as the source address.

[0006] The primary objective of the present invention is to defend against "packet flooding attacks" in whic or no value (at least to the victim), thereby making more valuable communication with the victim slow or ur which the attacker tries to use up some other resource by sending more requests of some particular type t

[0007] One way to view all these attacks is that a resource is being allocated in an unfair way. Well-behaved amounts. The most straight-forward allocation mechanism, which might be called "first come first served", allocation would reduce the impact of an attacker to that of a normal user.

[0008] There are two obvious impediments to the "fair service" goal above. One is lack of a reliable way to a fairly allocated. The other is lack of control over what packets arrive. The solution described here to both of

[0009] The defense is distributed among cooperating sites and routers. A set of transitively connected coop defense is related to the size of the cooperating neighborhood, a larger neighborhood providing better def packets. The association of packets with the "users" is approximated by associating packets with "places" ir service will be allocated in a fair (or otherwise reasonable) manner among these places. A "place" in this se router.

Cloudflare, Inc. Exhibit 1003 Page 304

[0010] One such place is likely to be shared by many actual users. An attack will deny service to those users each place is shared by fewer users, so an attack will deny service to fewer users. It is advantageous to a us neighborhood of that machine, since no attacker from another machine can deny him service. Conversely, a entry point into the cooperating neighborhood with as many users as possible.

[0011] Routers will supply data about the forwarding path of the packets that arrive at a site. The site can us This would solve the problem of unfair service if the packets that arrived were a fair sample of those that w forward all the packets they receive. To some extent fair service is limited by network topology, i.e., too mar relative to users of uncrowded paths. However another potential cause for this problem is a flooding attack a similar way to that described above for sites. That is, they allocate the limited resource of forwarding ban the cooperating neighborhood.

[0012] The final step in the defense is that cooperating routers will limit the rate at which they forward pack but it is useful for limiting the bandwidth used by "unwanted" packets. The rate-limiting request is to be ma This helps the site because it no longer has to process as many unwanted packets. It helps the network by f

[0013] Even if the traffic is not reduced, the distinction between "wanted" and "unwanted" packets plays ar packets (in fact, the great majority) that are expected in a very strong sense. It is reasonable to process the site is willing to process them at only a limited rate. A reasonable approach is to schedule these as describe regard as "unwanted" those that end up being significantly delayed (or discarded).

SUMMARY OF THE INVENTION

[0014] The present invention addresses many of the deficiencies of prior network defense systems and sati

[0015] A packet flooding defense system for a network providing the desired features may be constructed f routers, communication lines and transmitted data packets. Means are provided for classifying data packet processing rate with each class of data packet received at the computer. Means are also provided for the cc packets came to the computer. Thus, the computer can use the information to allocate the processing rate

[0016] In another variant, a packet flooding defense system for a network including a plurality of host comp for classifying data packets received at a host computer and means for associating a maximum acceptable provided for the computer to determine the rate at which data packets of each class are transmitted from a regarding maximum acceptable transmission rate for data packets being transmitted to the computer. Mea from the router to the computer. Thus, the rate of data packet transmissions received at the computer is ke the control of the rate of transmission of data packets from the router, thereby freeing a portion of the net

[0017] In this invention a path (which is not controlled by the attacker) is used to determine the actual direc (which is done via packet marks provided by routers leading up to the victim). In other words this invention forwarding bandwidth in a router. The part that makes this invention completely different from Chang, et a in order to work as a defense.

[0018] In yet another variant, the router is capable of receiving information regarding maximum acceptable and the router is capable of controlling the rate of transmission of each class of data packets to the comput

[0019] In still another variant, a packet flooding defense system for a network including a plurality of host c means for classifying data packets received at a router and means for associating a maximum acceptable tı provided for the router to find information for packets it receives regarding the path by which the packets c transmission rate for each class in a desired way.

[0020] In a further variant of the invention, a packet flooding defense system for a network including a plur includes means for classifying data packets received at a first router and means for associating a maximum router. Means are provided for the first router to determine the rate at which data packets of each class are router to receive information regarding maximum acceptable transmission rate for data packets being trar

Cloudflare, Inc. Exhibit 1003 Page 305

rate of transmission of data packets from the second router to the first router. Thus, the rate of data packet transmission rate for each data packet class by the control of the rate of transmission of data packets from transmission to the first router.

[0021] In yet a further variant, the second router is capable of receiving information regarding maximum ac first router and the second router is capable of controlling the rate of transmission of each class of data pac

[0022] In another variant, a packet flooding defense system for a network including a plurality of host comp one firewall. The firewall includes hardware and software serving to control packet transmission between th provided for classifying data packets received at the firewall as are means for associating a maximum accep Means are provided for the firewall to find information for packets it receives regarding the path by which t allocate the transmission rate for each class in a desired way.

[0023] In still another variant of the invention, a packet flooding defense system for a network including a p packets includes at least one firewall. The firewall includes hardware and software serving to control packet network and means for classifying data packets received at the firewall. Means are provided for associating at the firewall as are means for the firewall to determine the rate at which data packets of each class are tra information regarding maximum acceptable transmission rate for data packets being transmitted to the fir packets from the router to the firewall. Thus, the rate of data packet transmissions received at the firewall is by the control of the rate of transmission of data packets from the router, thereby freeing a portion of the r

[0024] In a final variant of the invention, the router is capable of receiving information regarding maximum firewall and the router is capable of controlling the rate of transmission of each class of data packets to the

[0025] An appreciation of the other aims and objectives of the present invention and an understanding of it description of a preferred embodiment.

DESCRIPTION OF THE DRAWINGS

[0026] FIG. 1 is a schematic view of a first embodiment of the invention illustrating the association of maxim and a path by which the packets came to the computer;

[0027] FIG. 2 is a schematic view of a second embodiment illustrating the association of maximum acceptab the packets came to the computer and illustrating information received at a router regarding maximum ac

[0028] FIG. 3 is a schematic view of a third embodiment illustrating information received at a router regardi transmitted to the computer;

[0029] FIG. 4 is a schematic view of a fourth embodiment illustrating association of maximum acceptable tr the packets came to the router;

[0030] FIG. 5 is a schematic view of a fifth embodiment illustrating the association of maximum acceptable t the packets came to the first router and illustrating information received at a second router regarding maxi router;

[0031] FIG. 6 is a schematic view of a sixth embodiment illustrating information received at the second rout being transmitted to the first router;

[0032] FIG. 7 is a schematic view of a seventh embodiment of the invention illustrating the association of m and a path by which the packets came to the firewall;

[0033] FIG. 8 is a schematic view of an eighth embodiment illustrating the association of maximum accepta which the packets came to the firewall and illustrating information received at a router regarding maximum and

[0034] FIG. 9 is a schematic view of a ninth embodiment illustrating information received at a router regard transmitted to the firewall.

Cloudflare, Inc. Exhibit 1003 Page 306

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0035] FIG. 1 illustrates a packet flooding defense system **10** for a network **14** providing the desired features a plurality of host computers **18**, routers **22**, communication lines **26** and transmitted data packets **30**. Mear means for associating a maximum acceptable processing rate **34** with each class **38** of data packet **30** receiv information for packets **30** it receives regarding the path **46** by which the packets **30** came to the computer for each class **38** in a desired way among the places from which packets **30** are transmitted.

[0036] In another variant, as illustrated in FIG. 2, a packet flooding defense system **10** for a network **14** inclu transmitted data packets **30** includes means for classifying data packets **30** received at a host computer **18** class **38** of data packet **30** received at the computer **18**. Means are provided for the computer **18** to determi **22** to the computer **18** as are means for the router **22** to receive information regarding maximum acceptabl Means are provided for the router **22** to control the rate of transmission of data packets **30** from the router computer **18** is kept below the maximum acceptable processing rate **34** for each data packet class **38** by the freeing a portion of the network **14** providing data packet transmission to the computer **18**.

[0037] In yet another variant, as illustrated in FIG. 3, the router **22** is capable of receiving information regarc being transmitted to the computer **18** and the router **22** is capable of controlling the rate of transmission of

[0038] In still another variant, as illustrated in FIG. 4, a packet flooding defense system **10** for a network **14** i transmitted data packets **30**, includes means for classifying data packets **30** received at a router **22** and mea of data packet **30** received at the router **22**. Means are provided for the router **22** to find information for pac router **22**. Thus, the router **22** can use the information to allocate the transmission rate for each class **38** in

[0039] In a further variant of the invention, as illustrated in FIG. 5, a packet flooding defense system **10** for a lines **26** and transmitted data packets **30** includes means for classifying data packets **30** received at a first rc with each class **38** of data packet **30** received at the first router **54**. Means are provided for the first router **5** from a second router **58** to the first router **54** as are means for the second router **58** to receive information transmitted to the first router **54**. Means are provided for the second router **58** to control the rate of transm rate of data packet transmissions received at the first router **54** is kept below the maximum acceptable tran transmission of data packets **30** from the second router **58**, thereby freeing a portion of the network **14** pro

[0040] In yet a further variant, as illustrated in FIG. 6, the second router **58** is capable of receiving informatic packet **30** being transmitted to the first router **54** and the second router **58** is capable of controlling the rate

[0041] In another variant, as illustrated in FIG. 7, a packet flooding defense system **10** for a network **14** inclu transmitted data packets **30** includes at least one firewall **86**. The firewall **86** includes hardware and softwar computer **18** connected to an internal network **90**. Means are provided for classifying data packets **30** receiv transmission rate **94** with each class **38** of data packet **30** received at the firewall **86**. Means are provided for by which the packets **30** came to the firewall **86**. Thus, the firewall **86** can use the information to allocate the

[0042] In still another variant of the invention, as illustrated in FIG. 8, a packet flooding defense system **10** f communication lines **26** and transmitted data packets **30** includes at least one firewall **86**. The firewall **86** inc network **14** and a host computer **18** connected to an internal network **90** and means for classifying data pac acceptable transmission rate **94** with each class **38** of data packet **30** received at the firewall **86** as are mean are transmitted from a router **22** to the firewall **86**. Means are provided for the router **22** to receive informa transmitted to the firewall **86** as are means for the router **22** to control the rate of transmission of data pack transmissions received at the firewall **86** is kept below the maximum acceptable transmission rate **94** for ea from the router **22**, thereby freeing a portion of the network **14** providing data packet transmission to the fi

[0043] In a final variant of the invention, as illustrated in FIG. 9, the router **22** is capable of receiving informa packet **30** being transmitted to the firewall **86** and the router **22** is capable of controlling the rate of transmi

[0044] The packet flooding defense system **10** has been described with reference to particular embodiment spirit and scope of the claims that follow.

Original

Classifications

IPC	CPC	US Class	ECLA	ICO
G06F11/30	H04L47/10	726/22	H04L47/10	T04L63:14D2
H04L12/56	H04L47/2441	370/229	H04L47/24D	
H04L29/06	H04L47/32	370/231	H04L47/32	
	H04L63/1458	370/235	H04L63/14D2	
		370/237		
		709/235		
		709/238		
		709/239		
		709/240		
		726/25		

Persons

Original Assignees

Original		Standardized	
COHEN DONALD N	(/api/control?query=pa:("COHEN%20DONALD%20N")&autosearch=true)	COHEN DONALD N	(/api/control?query=pas:(" D%20N")&autosearch=tru

Current Assignees

Original		Standardized	
PACSEC3 LLC	(/api/control?query=pacu:("PACSEC3%20LLC")&autosearch=true)	PACSEC3	(/api/control?query=pacus:("F ch=true)

5218 CHANDLER STREET, 77007, HOUSTON, TEXAS, UNITED STATES OF AMERICA

Inventor(s)

Original
Donald N. Cohen (/api/control?query=in:("Donald%20N.%20Cohen")&autosearch=true)

90064, 2815 Haddington Dr., Los Angeles, California, United States of America, US

Legal representative(s)

Original		Standardized
David A. Belasco	(/api/control?query=ag:("David%20A.%20Belasco")&autosearch=true)	

Belasco Jacobs & Townsley, LLP	(/api/control?query=ag:("Belasco%20Jacobs%20%26%20Townsley%2C%20LLP")&autosearch=true)

Legal information

Legal status

Event	Date	Description
Granted	2009-04-21	GRANTED
Filed	2004-05-07	FILED

Designated states

Date	Event code	Description

Ownership



Payment status

Date	Status	Event code	Description
2021-04-15	Fee paid	M2553	PAYMENT OF MAINTENANCE FEE, 12TH YR, SMALL ENTITY.
2017-04-14	Fee paid	M2552	PAYMENT OF MAINTENANCE FEE, 8TH YR, SMALL ENTITY.
2013-04-15	Fee paid	M2551	PAYMENT OF MAINTENANCE FEE, 4TH YR, SMALL ENTITY.

Litigation/Opposition

Pharmaceuticals

Product	Type	Active Ingredient	Applicant	Application No.	Application Type	Approval Date	Patent Expiry Date	Patent usage code	Exclusivity Code

No pharmaceuticals data

Citations

Show in a list ()

Citation type	Publication number	Citation relevance	Citation origin	Publication date	Title
backward	US5007052A		Cited by the examiner	1991-04-09	Method for routing pac
backward	US5353353A		Cited by the examiner	1994-10-04	Repeater security syste
backward	US5367523A		Cited by the examiner	1994-11-22	Adaptive rate-based co communications netwc
backward	US5434860A		Cited by the examiner	1995-07-18	Flow control for real-tir
backward	US5455865A		Cited by the examiner	1995-10-03	Robust packet routing failures
backward	US5581559A		Cited by the examiner	1996-12-03	Inverse packet disrupt

☐	backward	US5850515A	Cited by the examiner	1998-12-15	Intrusion control in rep
☐	backward	US6044402A	Cited by the examiner	2000-03-28	Network connection bl for monitoring connect unwanted connections
☐	backward	US6088804A	Cited by the examiner	2000-07-11	Adaptive system and m security attacks
☐	backward	US6412000B1	Cited by the examiner	2002-06-25	Method for automatica network
☐	backward	US20020032871A1	Cited by the examiner	2002-03-14	Method and system fo service attacks over a c
☐	forward	US7805759B2		2010-09-28	Systems and methods
☐	forward	US20090110000A1		2009-04-30	Apparatus and a meth
☐	forward	US8411566B2		2013-04-02	Apparatus and a meth
☐	forward	US9432331B1		2016-08-30	Mechanism for distribu
☐	forward	US9628509B2		2017-04-18	Identifying a denial-of-
☐	forward	US9641549B2		2017-05-02	Determining the likelih proxy server in a cloud
☐	forward	US9661020B2		2017-05-23	Mitigating a denial-of-s
☐	forward	US20140157416A1		2014-06-05	Determining the Likelih Proxy Server in a Cloud
☐	forward	US10129296B2		2018-11-13	Mitigating a denial-of-s

1 - 20 of 24

Non-patent literature

Yaar, A., et al, 'StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense entire document, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01705617.

Similar documents

The similarity check is done by matching this document to all documents in the database. Only the title and

Cloudflare, Inc. Exhibit 1003 Page 312

Lexis®

Results for: 7523497 OR 7,523,497

News (9) Sort by: Relevance

1.

Patent No. 7,523,497 Issued on April 21, for Packet Flooding Defense System (California Inventor)

US Fed News | Apr 22, 2009 | 175 words

... Patent No. **7,523,497** Issued on April 21, for Packet Flooding Defense System (California ...
... packet flooding defense system. The inventor was issued U.S. Patent No. **7,523,497** on April 21. According to the abstract released by the U.S. ...

2.

Page 20

Diarios Oficiais - Brazil | Feb 18, 2021 | EDITAIS; Pg. 20 | 1741 words

... 151°07'41" e distância15.920m chega-se ao vértice 2 com coordenadasX=417192.4048 e Y= **7523497** .2537. Deste comazimute de 158°52'47" e distância 37.595m chega-seao vértice 3 ...

3.

NAPLAN 2018: SCHOOL-BY-SCHOOL RESULTS

The Gold Coast Bulletin | Aug 29, 2018 | NEWS; Pg. 5 | 575 words

... 9 600 555 591 591 593 586 Merrimac State School Year **7 523 497** 544 538 537 527.8 551.9 Year 9 580 528 594 579 ...

4.

Las Vegas Sands (NYSE:LVS) Rating Increased to Hold at Cfra

American Banking and Market News | Apr 24, 2020 | 802 words

... LVS traded down $2.31 during trading hours on Friday, hitting $43.65. **7,523,497** shares of the company's stock traded hands, compared to its average ...

5.

Page 19

Diarios Oficiais - Brazil | Sep 29, 2020 | EDITAIS; Pg. 19 | 1781 words

... sob o nº 5000299-
88.2019.8.13.0097, requerida por MARIAAPARECIDA FREITAS RIBEIRO, inscrita no CPFsob o nº 813.884.206-
78. A ação tem por objeto umterreno com área de 10.5282 ha (dez hectares,cinquenta e dois ares e oitenta e dois centiares),situado no Bairro Quilombo, zona rural de
Conceição dos Ouros, MG, dentro das seguintesconfrontações: "Partindo-
se do vértice 1 comcoordenadas X=417184.7177 e Y=7523511.1950,seguindo com azimute 151°07'41" e distância15.920m chega-se ao vértice 2 com coordenadasX=417192.4048 e Y= **7523497** .2537. Deste comazimute de 158°52'47" e distância 37.595m chega-
seao vértice 3 com coordenadas X=417205.9512 eY=7523462.1844. Deste com azimute de 164°42'29"e distância 11.642m chega-
se ao vértice 4 comcoordenadas X=417209.0215 e Y=7523450.9550.Deste com azimute de 172°46'57" e distância31.233m chega-
se ao vértice 5 com coordenadasX=417212.9455 e Y=7523419.9695. Deste comazimute de 156°21'22" e distância 39.101m chega-
seao vértice 6 com coordenadas X=417228.6269 eY=7523384.1512. Deste com azimute de 154°22'44"e distância 28.296m chega-
se ao vértice 7 comcoordenadas X=417240.8627 e Y=7523358.6373.Deste com azimute de 142°45'27" e dist

ancia24.682m chega-
se ao vértice 8 com coordenadasX=417255.8002 e Y=7523338.9882. Deste comazimute de 133°07'47" e dist ância 25.651m chega-
seao vértice 9 com coordenadas X=417274.5206 eY=7523321.4516. Deste com azimute de 129°44'26"e dist ância 57.517m chega-
se ao vértice 10 comcoordenadas X=417318.7479 e Y=7523284.6806.Deste com azimute de 132°31'58" e dis tância59.512m chega-
se ao vértice 11 com coordenadasX=417362.6013 e Y=7523244.4501. Deste comazimute de 140°00'47" e dis tância 28.158m chega-
seao vértice 12 com coordenadas X=417380.6960 eY=7523222.8757. Deste com azimute de 144°29'46"e dis tância 10.616m chega-
se ao vértice 13 comcoordenadas X=417386.8615 e Y=7523214.2332.Deste com azimute de 155°45'07" e dis tância10.230m chega-
se ao vértice 14 com coordenadasX=417391.0630 e Y=7523204.9053. Deste comazimute de 165°59'34" e dis tância 24.075m chega-
seao vértice 15 com coordenadas X=417396.8902 eY=7523181.5462. Deste com azimute de 163°04'42"e dis tância 26.395m chega-
se ao vértice 16 comcoordenadas X=417404.5729 e Y=7523156.2942.Deste com azimute de 162°57'02" e dis tância39.861m chega-
se ao vértice 17 com coordenadasX=417416.2600 e Y=7523118.1850. Deste comazimute de 170°48'37" e dis tância 22.693m chega-
seao vértice 18 com coordenadas X=417419.8842 eY=7523095.7830, perfazendo um total de 493.177mconf rontando com Estrada Municipal de Conceiçãodos Ouros. Deste com azimute de 265°57'24" edistância 154.52 5m chega-
se ao vértice 19 comcoordenadas X=417265.7434 e Y=7523084.8876,confrontando com Benedito Inácio Rib eiro. Destecom azimute de 277°54'58" e distância 9.609mchega-se ao vértice 20 com coordenadas X=417256.2263 e Y=7523086.2110. Deste comazimute de 342°38'22" e distância 4.127m chega-
seao vértice 21 com coordenadas X=417254.9949 eY=7523090.1500, perfazendo um total de 13.736mconfro ntando com José Raimundo Gonçalves. Destecom azimute de 342°38'22" e distância 19.655mchega-se ao vértice 22 com ...

6.

Cooperative-routing mechanism based on node classification and task allocation for opportunistic social networks

IET Communications | Feb 01, 2020 | Pg. 420 - 429; 1751-8628; Vol. 14; No. 3 | 8788 words | WenyuZhengZhigangChenczg@csu.edu.cnJiaWuKanghuaiLiu

... Mobile and Multimedia Networks (WoWMoM), Coimbra, 2016, pp. 1–9, doi: 10.1109/WoWMoM.2016. **7523497** 31 Gao Y., Xiao Y., Wu M., : 'Dynamic social-aware peer ...

7.

Handball in Zahlen

Nürnberger Zeitung | Feb 25, 2014 | SPORT | 1180 words

... 17 10 0 7 542:503 20:14 6.HSG Konstanz 17 9 1 7 **523:497** 19:15 7.JSG Balingen-Weilst. 17 8 2 7 472:471 18:16 8.TuS Schutterwald ...

8.

Epigenetic targets for reversing immune defects caused by alcohol exposure.(ALCOHOL RESEARCH: Current Reviews)(Report)

ASAPII Database | Mar 22, 2013 | Pg. 97; ISSN: 2168-3492; Vol. 35; No. 1 | 14019 words | Curtis, Brenda J.Zahs, AnitaKovacs, Elizabeth J.

... of the IFN-gamma gene. Journal of Immunology 153(8): 3603-3610, 1994. PMID: **7523497** ZHANG, P.; BAGBYC, G.J.; HAPPEL, K.I.; ET AL. Alcohol abuse, immunosuppression, ...

9.

MICROCONTROLLERS: THE ENABLING TECHNOLOGY BEH

GlobalAdSource (English) | Mar 05, 2010 | 21 words

Cloudflare, Inc. Exhibit 1003 Page 314

... MICROCONTROLLERS: THE ENABLING TECHNOLOGY BEH ID **7523497** Description TEXT Price $23.0 USD Media Type Internet Country United States ...

Content type: News

Terms: 7523497 OR 7,523,497

Search Type: Boolean - Fewer Results

Narrow By: Sources: News

Date and Time: May 04, 2021 09:33:14 a.m. EDT



Print

Cookie Policy

Terms & Conditions

PTO/SB/57 (01-18)
Approved for use through 11/30/2021. OMB 0651-0064
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

(Also referred to as FORM PTO-1465)

REQUEST FOR *EX PARTE* REEXAMINATION TRANSMITTAL FORM

Address to:
Mail Stop *Ex Parte* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attorney Docket No.: 50348.65

Date: May 3, 2021

1. ■ This is a request for *ex parte* reexamination pursuant to 37 CFR 1.510 of patent number 7,523,497 issued April 21, 2009. The request is made by:
   ☐ patent owner. ■ third party requester.

2. ■ The name and address of the person requesting reexamination is:
   Raghav Bajaj, HAYNES AND BOONE, LLP
   2323 Victory Avenue, Suite 700
   Dallas, Texas 75219

3. Requester ☐ asserts small entity status (37 CFR 1.27) or ☐ certifies micro entity status (37 CFR 1.29). Only a patent owner requester can certify micro entity status. Form PTO/SB/15A or B must be attached to certify micro entity status.

4. This request is accompanied by payment of the reexamination fee as set forth in:
   ■ 37 CFR 1.20(c)(2); **or**
   ☐ 37 CFR 1.20(c)(1). **In checking this box for payment of the fee set forth in 37 CFR 1.20(c)(1), requester asserts that this request has forty (40) or fewer pages and complies with all other requirements of 37 CFR 1.20(c)(1).**

   Payment of the reexamination fee is made by the method set forth below.
   a. ☐ A check in the amount of $_____ is enclosed to cover the reexamination fee;
   b. ☐ The Director is hereby authorized to charge the reexamination fee to Deposit Account No. _____;
   c. ☐ Payment by credit card. Form PTO-2038 is attached; **or**
   d. ■ Payment made via EFS-Web.

   ■ In addition, the Director is hereby authorized to charge any fee deficiencies to Deposit Account No. 50-6990.

5. ■ Any refund should be made by ☐ check or ■ credit to Deposit Account No. 50-6990. 37 CFR 1.26(c). If payment is made by credit card, refund must be to credit card account.

6. ■ A copy of the patent to be reexamined having a double column format on one side of a separate paper is enclosed. 37 CFR 1.510(b)(4).

7. ☐ CD-ROM or CD-R in duplicate, Computer Program (Appendix) or large table
   ☐ Landscape Table on CD

This collection of information is required by 37 CFR 1.510. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) a request for reexamination. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 18 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop *Ex Parte* Reexam, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

8. ☐ Nucleotide and/or Amino Acid Sequence Submission
If applicable, items a. – c. are required.
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM (2 copies) or CD-R (2 copies) **or**
      ii. ☐ paper
   c. ☐ Statements verifying identity of above copies.

9. ■ A copy of any disclaimer, certificate of correction or reexamination certificate issued in the patent is included.

10. ■ Reexamination of claim(s) 1, 4, 7, 10, 13, and 16 is requested.

11. ■ A copy of every patent or printed publication relied upon is submitted herewith including a listing thereof on Form PTO/SB/08, PTO-1449, or equivalent.

12. ☐ An English language translation of all necessary and pertinent non-English language patents and/or printed publications is attached.

13. ■ The attached detailed request includes at least the following items:
   a. A statement identifying each substantial new question of patentability based on prior patents and printed publications. 37 CFR 1.510(b)(1).
   b. An identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited art to every claim for which reexamination is requested. 37 CFR1.510(b)(2).

14. ☐ A proposed amendment is included (only where the patent owner is the requester). 37 CFR 1.510(e).

15. ■ It is certified that the statutory estoppel provisions of 35 U.S.C. 315(e)(1) or 35 U.S.C. 325(e)(1) do not prohibit requester from filing this *ex parte* reexamination request. 37 CFR 1.510(b)(6).

16. Service
   a. ■ It is certified that a copy of this request (if filed by other than the patent owner) has been served in its entirety on the patent owner as provided in 37 CFR 1.33(c).

      The name and address of the party served are:

      Belasco, Jacobs & Townsley, PC

      6701 Center Drive West, 14th Floor

      Los Angeles, CA 90045

      Date of Service: May 3, 2021

   OR

   b. ☐ A duplicate copy is enclosed since service on patent owner was not possible. An explanation of the efforts made to serve patent owner **is attached**. See MPEP 2220.

17. Correspondence Address: Direct all communication about the reexamination to:

☒ The address associated with Customer Number: 27683

OR

☐ Firm or Individual Name _____
(at the address identified below)

Address

City	State	Zip

Country

Telephone	Email
214-651-5000	IPDOCKETING@HAYNESBOONE.COM

18. ☒ The patent is currently the subject of the following concurrent proceeding(s):

a. ☐ Copending reissue Application No. _____

b. ☐ Copending reexamination Control No. _____

c. ☐ Copending Interference No. _____

d. ☒ Copending litigation styled:

PacSec3, LLC v. NETSCOUT Systems, Inc., No. 6:20-cv-00914 (W.D. Tex.) (filed Oct. 10, 2020); PacSec3, LLC v. McAfee, LLC, No. 2:21-cv-00140 (E.D. Tex.) (filed Apr. 21, 2021);

PacSec3, LLC v. Palo Alto Networks, Inc., No. 2:21-cv-00141 (E.D. Tex.) (filed Apr. 21, 2021); PacSec3, LLC v. Juniper Networks, Inc., No. 6:21-cv-00387 (W.D. Tex.) (filed Apr. 21, 2021);

PacSec3, LLC v. Cisco Systems, Inc., No. 6:21-cv-00388 (W.D. Tex.) (filed Apr. 21, 2021)

WARNING : Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

/Raghav Bajaj/	May 3, 2021
Authorized Signature	Date
Raghav Bajaj	66,630
Typed/Printed Name	Registration No.

☐ For Patent Owner Requester ☒ For Third Party Requester

In place of PTO-1449 Form	U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE			*Complete if Known*	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*				Application Number	In Ex Parte Reexamination of 7,523,497
				Filing Date	Herewith
				First Inventor Name	Donald N. Cohen
				Art Unit	TBD
				Examiner Name	TBD
SHEET	1	OF	1	Attorney Docket Number	50348.65

U. S. PATENTS				
Examiner's Initials	**Cite No.**	**Document Number**	**Issue Date MM-DD-YYYY**	**Name of Patentee or Applicant of Cited Document**
	Ex. 1006	7,058,974	2006-06-06	Maher et al.
	Ex. 1007	6,725,378	2004-04-20	Schuba et al.

U. S. PATENT APPLICATION PUBLICATIONS				
Examiner's Initials	**Cite No.**	**Document Number**	**Publication Date MM-DD-YYYY**	**Name of Patentee or Applicant of Cited Document**

FOREIGN PATENT DOCUMENTS					
Examiner's Initials	**Cite No.**	**Foreign Patent Document (Country Code – Number – Kind)**	**Publication Date MM-DD-YYYY**	**Patentee or Applicant of Cited Document**	**Translation Y/N**

NON-PATENT LITERATURE DOCUMENTS		
Examiner's Initials	**Cite No.**	**Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published**
	Ex. 1005	Savage et al., "Practical Network Support for IP Traceback," SIGCOMM'00: Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2000, pp. 295-306 ("*Savage*")

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

Customer No. 27683

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent of: Donald N. Cohen	§	REQUEST FOR *Ex Parte* REEXAMINATION
	§	
U.S. Patent No. 7,523,497	§	
	§	Attorney Docket No.: 50348.65
Filed: May 7, 2004	§	
	§	Customer No.: 27683
Issued: April 21, 2009	§	
	§	
Title: PACKET FLOODING DEFENSE SYSTEM	§	Real Party in Interest: Unified Patents, LLC
	§	

REQUESTER'S POWER OF ATTORNEY
PURSUANT TO 37 CFR 1.510(f)

Pursuant to 37 CFR 1.510(f) Requester, **Unified Patents, LLC**, hereby appoints the Practitioner(s) associated with **Customer Number 27683**, as its attorney(s) to prosecute and to transact all business in the United States Patent and Trademark Office in connection with the above-identified request for *Ex Parte* Reexamination. Please recognize the correspondence address (including any electronic mail address) associated with **Customer Number 27683** for the above-identified *Ex Parte* Reexamination proceeding number to be the address associated with the appointed counsel(s).

The undersigned is authorized to sign this Power of Attorney on behalf of the Requester.

Executed on 5/3/2021.

Unified Patents, LLC

By: Jonathan Stroud

Printed Name: Jonathan Stroud

Title: Chief IP Counsel

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent of Donald N. Cohen	§	REQUEST FOR *EX PARTE*
	§	REEXAMINATION
U.S. Patent No. 7,523,497	§	
	§	Attorney Docket No.: 050348.065
Filed: May 7, 2004	§	
	§	Customer No.: 27683
Issued: April 21, 2009	§	
	§	
Title: PACKET FLOODING DEFENSE SYSTEM	§	
	§	
	§	
	§	

REQUEST FOR *EX PARTE* REEXAMINATION UNDER 35 U.S.C. §§ 302-306

Mail Stop *Ex Parte* Reexam
Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to the provisions of 35 U.S.C. §§ 302-306, Unified Patents, LLC ("Requester") hereby requests an *ex parte* reexamination of claims 1, 4, 7, 10, 13, and 16 ("Challenged Claims") of United States Patent No. 7,523,497 ("the '497 patent," EX1001) that issued on April 21, 2009, to Donald N. Cohen, resulting from U.S. Patent Application No. 09/715,813 filed on May 7, 2004.

Requester hereby asserts that claims 1, 4, 7, 10, 13, and 16 of the '497 patent are invalid over prior art references that were not previously before the Patent Office,

that are non-cumulative of, and better than, the prior art that was before the examiner during the original prosecution of the '497 patent, and that raise substantial new questions of patentability. Requester therefore requests that an order for reexamination be issued, and that the Office reject and cancel all challenged claims.

The '497 patent is the subject of five pending district court litigation cases identified below. The '497 patent was the subject of two terminated district court litigation cases identified below. No final judgment has been entered in any of the following seven cases.

Pending Cases
PacSec3, LLC v. NETSCOUT Systems, Inc., No. 6:20-cv-00914 (W.D. Tex.) (filed Oct. 10, 2020)
PacSec3, LLC v. McAfee, LLC, No. 2:21-cv-00140 (E.D. Tex.) (filed Apr. 21, 2021)
PacSec3, LLC v. Palo Alto Networks, Inc., No. 2:21-cv-00141 (E.D. Tex.) (filed Apr. 21, 2021)
PacSec3, LLC v. Juniper Networks, Inc., No. 6:21-cv-00387 (W.D. Tex.) (filed Apr. 21, 2021)
PacSec3, LLC v. Cisco Systems, Inc., No. 6:21-cv-00388 (W.D. Tex.) (filed Apr. 21, 2021)
Terminated Cases
PacSec3, LLC v. F5 Networks, Inc., No. 2:20-cv-00697 (D. Utah) (filed Oct. 2, 2020)
PacSec3, LLC v. F5 Networks, Inc., No. 2:20-cv-01828 (W.D. Wash.) (transferred from D. Utah on Dec. 14, 2020)

TABLE OF CONTENTS

I. Certification Regarding No Estoppel 6

II. Statement Pointing Out Substantial new questions of Patentability 6

A. Summary of Substantial New Questions of Patentability 6

B. Overview of the '497 Patent 10

1. Technical Background 10

2. Summary of Alleged Invention 12

C. Priority Date of the '497 Patent 13

D. Prosecution History and Reasons for Allowance 13

E. Claim Construction 20

F. Citation of Prior Art Patents and Printed Publications 20

1. Prior Art Qualification of Cited Prior Art Patents and Printed Publications 21

2. *Savage* is a Printed Publication 22

G. Identification of Substantial New Questions of Patentability 24

1. *Savage* Raises a Substantial New Question of Patentability 24

2. *Maher* and *Savage* Raise a Substantial New Question of Patentability 28

3. *Maher* and *Schuba* Raise a Substantial New Question of Patentability 31

4. The Combination of *Savage*, *Maher*, and *Schuba* Raises a Substantial New Question of Patentability 33

III. Detailed explanation of the pertinence and manner of applying the prior art

references to every claim for which reexamination is requested 34

A. Proposed Rejection #1: Claims 7, 13 and 1 would have been obvious over *Savage* in view of *Maher* and *Schuba* 35

1. Overview of *Savage* 35

2. Overview of *Maher* 37

3. Overview of *Schuba* 40

4. Motivation to Combine *Savage* with *Maher* and *Schuba* 40

5. Claim 7 would have been obvious over *Savage* in view of *Maher* and *Schuba* 48

6. Claim Chart Showing Unpatentability of Claim 7 76

7. Claim 13 would have been obvious over *Savage* in view of *Maher* and *Schuba* 99

8. Claim 1 would have been obvious over *Savage* in view of *Maher* and *Schuba* 109

B. Proposed Rejection #2: Claims 10, 16 and 4 would have been obvious over *Maher* in view of *Savage* and *Schuba* 116

1. Overview of Claim 10 116

2. Motivation to Combine *Maher* with *Savage* and *Schuba* 118

3. Claim 10 would have been obvious over *Maher* in view of *Savage* and *Schuba* 127

4. Claim Chart Showing Unpatentability of Claim 10 135

5. Claim 16 would have been obvious over Maher in view of Savage and Schuba 141

6. Claim 4 would have been obvious over *Maher* in view of *Savage* and *Schuba* 146

IV. List of Exhibits 154

V. Conclusion 157

VI. Certificate of Service 158

I. CERTIFICATION REGARDING NO ESTOPPEL

In accordance with 37 C.F.R. § 1.510(b)(6), Requester hereby certifies that the estoppel provisions of 35 U.S.C. § 315(e)(1) or 35 U.S.C. § 325(e)(1) do not prohibit Requester from filing this *ex parte* reexamination request. Requester has not previously challenged the '497 patent, and has not been involved in any proceeding involving the '497 patent.

II. STATEMENT POINTING OUT SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

A. Summary of Substantial New Questions of Patentability

This Request presents substantial new questions of patentability for claims 1, 4, 7, 10, 13 and 16 of the '497 patent. This Request relies on references that have not been previously considered by the office, and which render obvious the Challenged Claims of the '497 patent.

This Request first addresses claims 7 and 10, which are both method claims. Claims 7 and 10 are substantially similar, and recite the following limitations, with underlining and claim numbering added to show the differences between the claim elements:

[7.1.1] determining a path by which data packets arrive at a <u>host computer</u> via packet marks provided by routers leading to said host computer; (EX1001, 9:49-51)

[10.1.1] determining a path by which data packets arrive at said router via packet marks provided by routers leading to said host computer; (EX1001, 10:29-31)

As discussed in Section II.D below, claim 7 was allowed after the applicant amended claim 7 to define the recited path as "said path comprising all routers in said network via which said packets are routed to said computer." EX1002, 129, 146-147. This limitation is referred to as limitation [7.1.2] in the instant Request. Claim 10 was amended to recite the same limitation of "said path comprising all routers in said network via which said packets are routed to said computer." EX1002, 130. This added limitation is referred to as limitation [10.1.2] in the instant Request.

However, limitations [7.1.1], [7.1.2], [10.1.1], and [10.1.2] are disclosed by *Savage* (EX1005), which was not considered during prosecution of the '497 patent. Therefore, *Savage* raises a substantial new question of patentability because (1) *Savage* was not considered during prosecution of the '497 patent, and (2) *Savage* discloses the allegedly allowable features of claims 7 and 10.

Claims 13 and 16 are system claims that are substantially similar to method claims 7 and 10, respectively. Claim 13 recites limitations [13.1.1] and [13.1.2] that are identical to limitations [7.1.1] and [7.1.2], respectively, except for the addition of the phrase "means for." Similarly, claim 16 recites limitations [13.1.1] and

[13.1.2] that are substantially similar to limitations [10.1.1] and [10.1.2], respectively, except for the addition of the phrase "means for." Claims 13 and 16 were allowed after the addition of limitations [13.1.2] and [16.1.2]. EX1002, 146-147. However, limitations [13.1.1], [13.1.2], [16.1.1] and [16.1.2] are also disclosed by *Savage*, which was not considered during prosecution of the '497 patent. Therefore, *Savage* raises a substantial new question of patentability because (1) *Savage* was not considered during prosecution of the '497 patent, and (2) *Savage* discloses the allegedly allowable features of claims 13 and 16.

Claims 1 and 4 contain a non-substantive variation from limitations [7.1.1] and [10.1.1] above, respectively, of finding information regarding a path, rather than determining a path, as recited in limitations [7.1.1] and [10.1.1]. Below, claim numbering, underlining, and strikethrough text is added to show the differences between limitations [7.1.1] and [1.3.1], and the differences between limitations [10.1.1] and [4.3.1], respectively.

[1.3.1] ~~[7.1.1]~~ means for said computer to find information for packets it receives regarding the ~~determining a~~ path by which ~~data~~ said packets ~~arrive at a host~~ came to said computer via packet marks provided by routers leading to said host computer; (EX1001, 8:18-21)

[4.3.1] ~~[10.1.1]~~ means for said router to find information for packets it receives

> regarding the ~~determining a~~ path by which ~~data~~ said packets ~~arrive at~~ came to said router via packet marks provided by routers leading to said host computer; (EX1001, 9:1-4)

Claims 1 and 4 were allowed after being amended to recite "said path comprising all routers in said network via which said packets are routed to said computer," which is the same limitation that was added to claims 7, 10, 13, and 16 to gain allowance of these claims. EX1002, 126-128, 146-147. The added limitations to claims 1 and 4 are referred to as limitations [1.3.2] and [4.3.2] below. However, limitations [1.3.1], [1.3.2], [4.3.1] and [4.3.2] are also disclosed by *Savage*, which was not considered during prosecution of the '497 patent. Therefore, *Savage* raises a substantial new question of patentability because (1) *Savage* was not considered during prosecution of the '497 patent, and (2) *Savage* discloses the allegedly allowable features of claims 1 and 4.

The remaining limitations of claims 1, 4, 7, 10, 13, and 16, to the extent not expressly disclosed by *Savage*, are merely conventional implementation details that are disclosed by *Maher* (EX1006) and *Schuba* (EX1007). *See* Section III, *infra*. *Maher* and *Schuba* were also not considered during prosecution. Therefore, *Maher* and *Schuba* also raise substantial new questions of patentability because (1) they were not considered during prosecution of the '497 patent, and (2) show that the remaining limitations of claims 1, 4, 7, 10, 13, and 16 are merely well-known

implementation details.

Further, the combinations of *Savage*, *Maher*, and *Schuba*, as presented in this Request, raise a substantial new question of patentability because (1) these references were not considered during prosecution of the '497 patent, and (2) the Office has not considered the combination of these three references as presented in this Request.

A reasonable examiner would have found *Savage*, *Maher*, and *Schuba* relevant to the Challenged Claims.

As shown below and confirmed in the Declaration of Dr. Vijay Madisetti (EX1003), the technology claimed in the '497 patent was not new. The references presented in this Request render obvious the Challenged Claims, which should be canceled for unpatentability.

B. Overview of the '497 Patent

1. Technical Background

The '497 patent relates to "minimizing the effects of packet flooding attacks directed against computers or routers connected to a network." EX1001, 1:13-15. The '497 patent describes a packet flooding attack as when "an attacker tries to use up all the bandwidth [available] to the victim by sending data of little or no value (at least to the victim), thereby making more valuable communication with the victim slow or unreliable." EX1001, 2:6-10.

Other contemporaneous references describe packet flooding attacks as a type of "Denial of Service" (DoS) attack. For example, Malan (EX1010) explains that:

> One problem occurs when a first computer system maliciously sends a flood of packets to a target or second computer system, routing system or network link to overwhelm the reception resources or capacity of the target, which can result in either loss of connectivity to or failure of the target. This flood of packets based attack is commonly known as a denial of service attack ("DoS").

EX1010, ¶ 10.

Similarly, U.S 7,062,782 to Stone et al. (EX1011) explains that:

> A packet flood attack differs from other types of denial-of-service attacks in that a flood attack requires constant and rapid transmission of packets to the victim in order to be effective. The flood attack overwhelms the victim's connection and consumes precious bandwidth on the ISPs' backbone networks.

EX1011, 1:24-29.

As another example, *Maher* discloses that "[a] 'denial of service' (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. DoS attacks are aimed at devices and networks with exposure to the Internet. Their goal is to cripple a device or network so that external users no longer have access to network resources." EX1006, 1:14-17.

One limitation in preventing DoS attacks is identifying the source of the

attack. Attackers often "spoof" or "forge" their source address to prevent discovery of the origin of the attacks. EX1005, 295 at Abstract (discussing "spoofed" source addresses); EX1011, 1:44-54 ("the attacker can forge the source address of the flood packets" to avoid detection); EX1007, 5:62-64 ("Attacker A initiates a SYN flooding attack by sending many connection requests with spoofed source addresses to the victim machine.").

2. Summary of Alleged Invention

The '497 patent's "primary objective…is to defend against 'packet flooding attacks.'" EX1001, 2:6-7. The '497 patent explains that its solution "requires help from the routers that forward packets to the victim." EX1001, 2:27-29. The '497 patent indicates that "[r]outers will supply data about the forwarding path of the packets that arrive at a site," to permit the forwarding path of the packets to be traced, and the "routers will limit the rate at which they forward data packets" to downstream devices. EX1001, 2:54-55, 2:32-36, 3:4-6. The '497 patent describes that "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)." EX1001, 3:62-66.

The '497 patent explains that "routers will limit the rate at which they forward packets" to assist in "limiting the bandwidth used by 'unwanted' packets." EX1001,

3:4-8. The '497 patent classifies packets into "wanted packets" and "unwanted packets" based on whether the packets are expected to be received. EX1001, 3:6-23, 3:34-37, 6:16-20, 6:55-58. The '497 patent explains that the processing or transmission rate for "unwanted data packets" can be decreased to free up network resources. EX1001, 3:8-12, 6:23-25, 6:46-63.

C. Priority Date of the '497 Patent

The '497 patent was filed as U.S. Application No. 10/841,064 ("'064 application") on May 7, 2004. The '497 patent was filed as a continuation of U.S. Patent No. 6,789,190, which was filed as U.S. Application No. 09/715,813 on November 16, 2000. The '497 patent does not claim priority to any earlier application. Accordingly, the priority date of the '497 patent is presumed to be November 16, 2000. All of the prior art cited in the proposed grounds of rejection predates November 16, 2000 (*see* Section II.F below).

D. Prosecution History and Reasons for Allowance

As noted above, the '497 patent was filed as a continuation of U.S. Patent No. 6,789,190 (EX1027), which was filed as Application No. 09/715,813 ("'813 application") (EX1028). The '813 application was filed with claims 1-9. EX1028, 21-26. Claims 1 and 4 of the '813 application contained some features that are generally similar to limitations [7.1.1], [7.2], [7.3], [10.1.1], [10.2], and [10.3] of claims 7 and 10 of the '497 patent. However, claims 1 and 4 of the '813 application

were broader in scope than 7 and 10 of the '497 patent, because claims 1 and 4 of the '813 application did not recite features corresponding to limitations [7.1.2], [7.4], [10.1.2], and [10.4] of claims 7 and 10 of the '497 patent. Claims 7-9 of the '813 application contain features directed to a "firewall" that are not recited in any of claims 7 and 10 of the '497 patent (see firewall 86 in Figures 7-9 of the '190 patent (EX1027) and Figures 7-9 of the '497 patent).

The examiner rejected claims 1-9 of the '813 application as being anticipated by U.S. Patent 5,367,523 by Chang (EX1008). EX1028, 48-54. The applicant requested rehearing of this rejection, arguing that a packet flooding defense system is not equivalent to the applicant's characterization of Chang's teaching of a "flow and congestion control system." EX1028, 61-62. Further, the applicant argued that Chang does not disclose "means for classifying individual packets of data," or "means for determining the path by which the data arrives at the receiver." EX1028, 62, 66. The examiner rejected these arguments and issued a final Office Action. EX1028, 76-80. The applicant then cancelled claims 1-6 of the '813 application in response to a final Office Action maintaining the rejection of claims 1-6 of the '813 application. EX10028, 93-95 (cancellation of claims 1-6). Claims 7-9 of the '813 were identified as allowable over Chang (EX1008) for reciting features directed to a "firewall" that are not recited in any of challenged claims 7 and 10 of the '497 patent. EX1028, 98-99.

The '497 patent was filed as the'064 application" (EX1002) after the '813 application was allowed. The '497 patent issued after the examiner issued two Office Actions (one non-final and one final) in the '064 application. In both Office Actions, the examiner rejected the claims as being anticipated by Chang (EX1008). EX1002, 59-60 (claim 7 rejected for same reasons as claim 1), 61-62 (claim 10 rejected for same reasons as claim 4), 98-101 (same). In response to the non-final Office Action, the applicant argued that "the instant invention detects the path from which the data packets come via packet marks and sorts the data packets into two classes, wanted and unwanted, based on this path. EX1002, 89. The applicant amended claim 7 as follows:

> 7. (currently amended): 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:
>
> determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer;
>
> classifying data packets received at ~~a~~ said host computer into wanted data packets and unwanted data packets by path;
>
> associating a maximum acceptable processing rate with each class of data packet received at said host computer; and
>
> allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets ~~of each class in a desired way~~.

EX1002, 82.

The applicant amended claim 10 as follows:

> 10. (currently amended): 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:
>
> determining a path by which data packets arrive at said router via packet marks provided by routers leading to said host computer;
>
> classifying data packets received at ~~a~~ said router via packet marks provided by routers leading to said host computer by path;
>
> associating a maximum acceptable transmission rate with each class of data packet received at said router; and
>
> allocating a transmission rate equal to or less than said maximum acceptable transmission rate for ~~each class~~unwanted data packets ~~in a desired way~~.

EX1002, 83-84.

The applicant argued that Chang does not disclose "detecting the path from which the data packets come; detecting packet marks; and sorting data packets into two classes, wanted and unwanted." EX1002, 89.[1]

In the final Office Action, the examiner rejected the applicant's argument, finding that Chang discloses determining a path by which data packets arrive at a

[1] In response to the non-final Office Action, the applicant did not contest the examiner's determination that Chang discloses associating a maximum acceptable processing rate with each class of data packet received at the host computer and allocating a processing rate less than or equal to the maximum acceptable processing rate for unwanted data packets (limitations [7.3] and [7.4] above). *See* EX1002, 89.

host computer via packet marks provided by routers leading to the host computer, and classifying data packets received at the host computer into wanted and unwanted data packets by path. EX1002, 99-101.

In response to the final Office Action, at the examiner's suggestion, the applicant amended claim 7 to additionally recite:

> [7.1.1] determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer;
>
> [7.1.2] said path comprising all routers in said network via which said packets are routed to said computer.

EX1002, 129 (additional features shown with underlining, and claim numbering added).

Similar amendments were made to claim 10 (i.e., addition of limitation [10.1.2]), as shown below.

> [10.1.1] determining a path by which data packets arrive at said router via packet marks provided by routers leading to said host computer;
>
> [10.1.2] said path comprising all routers in said network via which said packets are routed to said computer.

EX1002, 130 (additional features shown with underlining, and claim numbering added).

Similar amendments were made to claims 13 and 16 (i.e., addition of

limitations [13.1.2] and [16.1.2]), as shown below.

> [13.1.1] means for determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer;
>
> [13.1.2] said path comprising all routers in said network via which said packets are routed to said computer.

EX1002, 132 (additional features shown with underlining, and claim numbering added).

> [16.1.1] means for a router to determine a path by which said packets came to said router via packet marks provided by routers leading to said router;
>
> [16.1.2] said path comprising all routers in said network via which said packets are routed to said computer.

EX1002, 133 (additional features shown with underlining, and claim numbering added).

Similar amendments were made to claims 1 and 4 (i.e., addition of limitations [13.1.2] and [16.1.2]), as shown below.

> [1.3.1] means for said computer to find information for packets it receives regarding the path by which said packets came to said computer via packet marks provided by routers leading to said host computer;
>
> [1.3.2] said path comprising all routers in said network via which said packets are routed to said computer.

EX1002, 126.

[4.3.1] means for said router to find information for packets it receives regarding the path by which said packets came to said router via packet marks provided by routers leading to said host computer;

[4.3.2] said path comprising all routers in said network via which said packets are routed to said computer.

EX1002, 127-128.

The examiner then allowed the '064 application. EX1002, 142-150. In allowing the application, the examiner remarked that the prior art considered during prosecution did not disclose "path forwarding along the entire path to the victim, said path information encompassing the entire path through the associated routers, and subsequent use of said [path] information to effect filtering via allocation of packet processing rate." EX1002, 146-147. The '064 application was thus allowed due to the addition of limitations [7.1.2], [10.1.2], [13.1.2], [16.1.2], [1.3.2], and [4.3.2].

As described in Section III below, however, limitations [7.1.1], [7.1.2], [10.1.1], [10.1.2], [13.1.1], [13.1.2], [16.1.1], [16.1.2], [1.3.1], [1.3.2], [4.3.1], and [4.3.2] are disclosed by prior art (*Savage*) not considered by the examiner. Limitations [10.1.1] and [10.1.2] are similarly disclosed by prior art (*Savage*) not

considered by the examiner.[2]

E. Claim Construction

The '497 patent is not expired[3]; thus, this Request analyzes the claims according to their broadest reasonable interpretation in light of the specification. MPEP 2258 § I.G. For the purposes of this Request, Requester submits that all terms should be given their broadest reasonable interpretation, and that a specific construction is not necessary for any claim term. No express construction is necessary for this proceeding, that is, to show the unpatentability of the claims. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (construing terms "only to the extent necessary to resolve the controversy").

As noted above, the '497 patent is involved in five pending district court cases, and was involved in two terminated district court cases. No district court has issued a claim construction order in any of the five pending district court cases, or in the two terminated district court cases.

F. Citation of Prior Art Patents and Printed Publications

In accordance with 37 C.F.R. § 1.510(b)(3), reexamination of claims 7, 10,

[2] Notably, claims 7, 10, 13, 16, 1, and 4 do not recite the following phrase contained in the examiner's statement of reasons for allowance: "said information to effect filtering via allocation of packet processing rate." EX1002, 146-147.
[3] Based on the 719 days of patent term adjustment listed on the face of the '497 patent, the estimated expiry of the '497 patent is November 5, 2022.

13, 16, 1, and 4 (the "Challenged Claims") of the '497 patent[4] is requested in view of the following references:

EX1005	Savage et al., "Practical Network Support for IP Traceback," SIGCOMM'00: Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2000, pp. 295-306 ("*Savage*")
EX1006	U.S. Patent 7,058,974 to Maher et al. ("*Maher*")
EX1007	U.S. Patent 6,725,378 to Schuba et al. ("*Schuba*")

1. Prior Art Qualification of Cited Prior Art Patents and Printed Publications

As explained in Section II.F.2 below, *Savage* (EX1005) qualifies as a printed publication because it was publicly accessible to persons interested and ordinary skilled in the art at least by September 1, 2000. *Savage* is thus prior art under 35 U.S.C. §102(a).

Maher was filed June 21, 2000, and issued June 6, 2006. *Maher* is thus prior art under 35 U.S.C. §102(e).

Schuba was filed on April 15, 1999, and issued on April 20, 2004. *Schuba* is prior art under 35 U.S.C. §102(e).

A detailed explanation of the pertinence and manner of applying the patents

[4] The '497 patent issued from an application filed prior to the enactment of the America Invents Act ("AIA"). Thus, the pre-AIA statutory framework applies.

and printed publications to every claim for which reexamination is requested is set forth in Section III below.

2. *Savage* is a Printed Publication

As explained by the Federal Circuit, "public accessibility has been called the touchstone in determining whether a reference constitutes a printed publication." *In re Hall*, 781 F.2d 897, 899 (Fed. Cir. 1986). "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).

Requester submits the Declarations of Dr. Savage (EX1015), Mr. Delman (EX1009), Dr. Hall-Ellis (EX1025), and Dr. Madisetti (EX1003) to show that *Savage* (EX1005) was publicly accessible at least by September 1, 2000. Dr. Savage personally presented *Savage* (EX1005) at the ACM SIGCOMM 2000 Conference (hereinafter "Conference") in Stockholm, Sweden on September 1, 2000. EX1015, ¶¶ 8, 10 (citing EX1017). SIGCOMM is the annual conference of the Special Interest Group on Data Communication (SIGCOMM) of the Association for Computing Machinery (ACM). EX1015, ¶ 9. At the time of the Conference, SIGCOMM was a well-known academic conference that was frequently attended by persons interested and skilled in the relevant art, including professors, students, and professionals in

the field of network communication protocols. EX1015, ¶ 9; *see also* EX1003, ¶¶ 31-34. There were over 300 Conference attendees. EX1015, ¶ 17; EX1009, ¶ 11 (over 400 individuals registered for the Conference).

A printed copy of *Savage* was distributed to all conference attendees in a conference book (EX1021). EX1015, ¶ 15 (citing EX1021); EX1009, ¶ 11 (*Savage* distributed to all conference attendees). Dr. Savage retained his copy of the conference book (EX1021), which indicates that it pertains to the proceedings of the Conference. EX1015, ¶¶ 15-16; EX1021, 1-9. *Savage* was also freely available on the Internet for access by anyone, including conference attendees and non-attendees, by at least August 20, 2000, in advance of the Conference, and could be accessed by searching its title or author. EX1015, ¶¶ 11 (citing EX1018), 12 (Attachment G), 14. Dr. Savage was a person interested and ordinarily skilled in the subject matter of the '497 patent as of the priority date of the '497 patent. EX1015, ¶ 22.

As Dr. Madisetti testifies, a person of ordinary skill in the art ("POSITA") in the relevant time frame would have frequently reviewed ACM SIGCOMM publications and attended ACM SIGCOMM conferences. EX1003, ¶¶ 31-34. Dr. Madisetti had several articles published in ACM publications. EX1003, ¶ 34.

As Dr. Hall-Ellis explains, library records show that *Savage*, as printed in *ACM SIGCOMM 2000 Conference: Applications, Technologies, Architectures, and Protocols for Computer Communication* (EX1021), was shelved at the University of

Cincinnati Library by October 14, 2000. EX1025, ¶¶ 40-45. Further, the date printed on *Savage* itself (August 2000) provides additional evidence of its public accessibility. *See also* EX1021 (date of August 28-September 1, 2000). *Savage* was also indexed by subject matter. EX1025, ¶ 44. As further confirmation that *Savage* was publicly accessible, Dr. Hall-Ellis refers to other documents that cited *Savage* around the time of the priority date of the '497 patent. EX1015, ¶¶ 46-58 (citing EX1041-EX1043).

Accordingly, *Savage* was publicly accessible to POSITAs at least by September 1, 2000.

G. Identification of Substantial New Questions of Patentability

In this Request, substantial new questions (SNQs) of patentability are raised as set forth below. [5]

1. *Savage* Raises a Substantial New Question of Patentability

Savage raises a substantial new question of patentability because it discloses the allegedly allowable features of claims 7, 10, 13, 16, 1 and 4, and *Savage* was not considered during prosecution of the '497 patent.

[5] Unless otherwise specified, all **bold** and ***bold italics*** emphasis below has been added. Text in *italics* is used to signify claim language, while reference names are also *italicized*.

Claims 7 and 10 recite the feature of determining a path by which data packets arrive at a host computer (claim 7) or at a router (claim 10) via packet marks provided by routers leading to the host computer. EX1001, 9:49-51, 10:29-31. Similarly, claim 13 recites the feature of a means for determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to the host computer. EX1001, 11:10-14.

As discussed in Section II.D above, the examiner allowed claims 7, 10, 13, 16, 1, and 4 after the applicant defined the path in these claims to require: "said path comprising all routers in said network via which said packets are routed to said computer." EX1002, 126-130, 132-133, 146-147. However, the allegedly allowable features of claims 7, 10, 13, 16, 1 and 4 are disclosed by *Savage*, which was not considered during prosecution of the '497 patent.

Savage discloses inserting a packet mark at each router that a packet is transmitted through, to aid in identifying the attacker in flood attacks. *Savage* discloses that its "solution is to probabilistically mark packets with partial path information as they arrive at routers." EX1005, 295. With reference to Figure 1 below, *Savage* discloses an exemplary network as seen from a victim V, where every potential attack origin is represented by A*i*, and routers are represented by R*i*. EX1005, 297. The dotted line in Figure 1 represents an attack path that includes the attacker (A_2) as well as all the routers (R_6, R_3, R_2, and R_1) through which the packet

travelled from the attacker (A_2) to the victim (V). EX1005, 298.

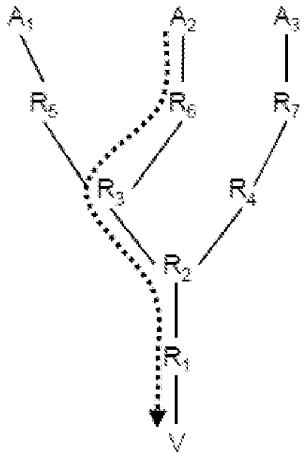


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_j. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1

Savage discloses that each router along the path "'marks' one or more packets by augmenting them with additional information about the path they are traveling." 298, 299 (describing "Node append" algorithm in Figure 2 below as "appending each node's [i.e., router's] address to the end of the packet as it travels through the network from attacker to victim."). *Savage* discloses that "[c]onsequently, every packet received by the victim arrives with **a complete ordered list of the routers it traversed**—a built-in attack path." EX1005, 299.

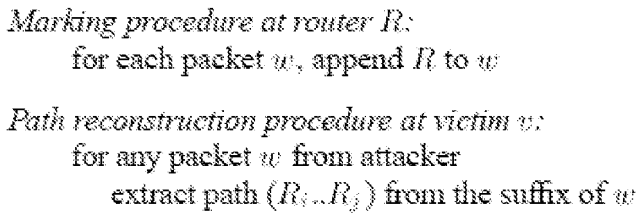


Figure 2: Node append algorithm.

EX1005, Fig. 2

Savage teaches that the victim V then implements a "path reconstruction procedure" to "reconstruct the attack path using only the information in these marked packets." EX1005, 298.

Therefore, *Savage* discloses that each router along the attack path adds a packet mark identifying that router's address to the data packet as the data packets travel along the attack path, to enable a path reconstruction procedure to be performed to determine the "complete ordered list of the routers [the data packet] traversed." EX1005, 295, 298-299. Thus, *Savage* discloses determining a path, including all routers along the path to a host computer, by which data packets arrive at a host computer or router via packets markets provided by routers along the path, as recited in claims 7, 10, and 13.

Likewise, *Savage* discloses *a means for a host computer to find information* (packet marks) *for packets it receives regarding the path by which the packets came to the computer via packet marks provided by routers leading to the host computer*,

as recited in claim 1. As discussed above, *Savage* discloses that the victim host computer receives packets with packet marks inserted by each router through which the packets traveled, so that "every packet received by the victim arrives with **a complete ordered list of the routers it traversed**—a built-in attack path." EX1005, 299.

Accordingly, *Savage* raises a substantial new question of patentability because it discloses the allegedly allowable features of claims 7, 10, 13, and 1, and *Savage* was not considered during prosecution of the '497 patent.

A reasonable examiner would have found *Savage* relevant to the Challenged Claims.

2. *Maher* and *Savage* Raise a Substantial New Question of Patentability

Maher and *Savage* also raise a substantial new question of patentability because (1) *Maher* and *Savage* teach the allegedly allowable features of claims 10, 16, and 4, (2) *Maher* and *Savage* were each not considered during prosecution of the '497 patent, and (3) the Office has not considered the combination of *Maher* and *Savage* as presented in this Request.

To the extent that the determining step of claim 10 (limitations [10.1.1] and [10.1.2]) is interpreted as being performed in a router, the combination of *Maher* and *Savage* renders these limitations obvious. Therefore, *Maher* and *Savage* raise a

substantial new question of patentability because they disclose the allegedly allowable feature of claim 10.

As discussed in Section II.G.1 above, *Savage* discloses determining a path that includes all routers through which data packets were routed to a host computer. *Savage* discloses that the victim V in Figure 1 above "may be a single host under attack, or a **network border device** such as a firewall or intrusion detection system that represents many such hosts." EX1005, 297 (emphasis added). *Maher* discloses a network apparatus "for preventing denial of service type attacks on data networks." EX1006, Abstract, 3:6-9, 6:11-21, 7:27-41. *Maher* discloses that its network apparatus may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67.

Maher and Savage thus raise a substantial new question of patentability because a person of ordinary skill in the art (POSITA), in view of the teachings of *Maher* and *Savage*, would have been motivated to perform the path reconstruction procedure disclosed by *Savage* in a router, in view of *Maher*'s disclosure that routers are configured to perform packet analysis procedures in the event of a QoS attack.

Therefore, *Maher* and *Savage* raise a substantial new question of patentability because (1) *Maher* and *Savage* teach the allegedly allowable feature of claim 10, (2) *Maher* and *Savage* were not considered during prosecution of the '497 patent, and

(3) the Office has not considered the combination of *Maher* and *Savage* as presented in this Request.

Likewise, *Maher* and *Savage* teach a *means for a router to determine a path by which said packets came to said router via packet marks provided by routers leading to said router*, as recited in claim 16, for the same reasons presented above with respect to claim 10.

Claim 4 is largely similar to claim 10 except for two respects: claim 4 is directed to a packet flooding defense system instead of a method for packet flooding defense as in claim 10, and claim 4's recitation of one limitation is slightly different. In particular, claim 4 recites *means for said router to find information for packets it receives regarding the path by which said packets came to said router via packet marks provided by routers leading to said host computer*. But this variation is substantively the same as the limitation in claim 10 of *determining a path* and is not patentably distinct. *Savage* discloses that the victim host computer receives packets with packet marks inserted by each router through which the packets traveled, so that "every packet received by the victim arrives with **a complete ordered list of the routers it traversed**—a built-in attack path." EX1005, 299. Therefore, the victim, which may be a router, as taught by *Maher*, *finds information for packets it receives regarding the path by which said packets came to said router via packet marks provided by routers leading to said host computer*, as recited in claim 4.

Claims 10, 16 and 4 were allowed after these claims were amended to define the recited path as "*said path comprising all routers in said network via which said packets are routed to said computer*," identical to claims 7, 13, and 1. But as described above, *Savage* teaches this allegedly allowable feature of claims 7, 10, 13, 16, 1 and 4.

Therefore, *Maher* and *Savage* raise a substantial new question of patentability because (1) *Maher* and *Savage* teach the allegedly allowable feature of claims 10,1 6 and 4, (2) *Maher* and *Savage* were not considered during prosecution of the '497 patent, and (3) the Office has not considered the combination of *Maher* and *Savage* as presented in this Request.

A reasonable examiner would have found *Maher* relevant to the Challenged Claims.

3. *Maher* and *Schuba* Raise a Substantial New Question of Patentability

Claims 7 and 10 recite conventional implementation details such as classifying data packets received at a host computer or router as wanted data packets or unwanted data packets by path (limitations [7.2] and [10.2] below), associating a maximum acceptable processing rate or maximum acceptable transmission rate with each class of data packets (limitations [7.3] and 10.3] below), and allocating a processing rate or transmission rate less than or equal to the maximum acceptable

processing rate or maximum acceptable transmission rate (limitations [7.4] and [10.4] below).

These features of claims 7 and 10 are merely conventional implementation details for minimizing the severity of a DoS attack (e.g., packet flooding attack). *Maher* and *Schuba* disclose these conventional implementation details, as shown in Section III below.

Maher and *Schuba* were not considered during prosecution of the '497 patent. Therefore, *Maher* and *Schuba* raise a substantial new question of patentability because they (1) were not considered during prosecution of the '497 patent, and (2) show that several limitations of claims 7 and 10 are merely well-known implementation details. *Savage* discloses that its packet traceback technique is intended to be "implemented using conventional technology," such as that disclosed by *Maher* and *Schuba*. EX1005, Abstract.

Likewise, claims 13, 16, 1, and 4 recite conventional implementation details that correspond to the above-described limitations [7.2]-[7.4] and [10.2]-[10.4], i.e., limitations [13.2]-[13.4], [16.2]-[16.4], [1.1], [1.2], [1.4], and [4.1], [4.2] and [4.4], which are disclosed by *Maher* and *Schuba*. Therefore, *Maher* and *Schuba* also raise a substantial new question of patentability for claims 13, 16, 1 and 4, for the same reasons presented above with respect to claims 7 and 10.

A reasonable examiner would have found *Schuba* relevant to the Challenged

Claims.

4. The Combination of *Savage*, *Maher*, and *Schuba* Raises a Substantial New Question of Patentability

The Office has not considered the combination of *Savage*, *Maher*, and *Schuba*, as presented in this Request. *Savage*, *Maher*, and *Schuba* were not considered during prosecution of the '497 patent. As discussed above in Section II.G.1, *Savage* discloses the allegedly allowable features of claims 7, 10, 13, 16, 1, and 4. Further, as discussed above in Section II.G.2, *Maher* and *Savage* teach the allegedly allowable features of claims 10, 16, and 4. As discussed above in Section II.G.3, *Maher* and *Schuba* disclose conventional implementation details that are recited in claims 7, 10, 13, 16, 1, and 4.

Accordingly, the combination of *Savage*, *Maher*, and *Schuba* raises a substantial new question of patentability, because *Savage*, *Maher*, and *Schuba* disclose all the recited features of claims 7, 10, 13, 16, 1, and 4, including the allegedly allowable features of these claims, and render these claims obvious. The Office has not considered the combination of *Savage*, *Maher*, and *Schuba*, as presented in this Request.

A reasonable examiner would have found *Savage*, *Maher*, and *Schuba* relevant to the Challenged Claims.

III. DETAILED EXPLANATION OF THE PERTINENCE AND MANNER OF APPLYING THE PRIOR ART REFERENCES TO EVERY CLAIM FOR WHICH REEXAMINATION IS REQUESTED

Each of the proposed rejections detailed below show claims 1, 4, 7, 10, 13, and 16 of the '497 patent are unpatentable. The proposed rejection of claim 7, a method claim, is set forth first in Section III.A below. The proposed rejections of system claims 13 and 1, which are substantially similar to method claim 7, are then set forth in Section III.A below after the analysis of claim 7.

In Section III.B below. the proposed rejection of method claim 10 is set forth first. The proposed rejections of system claims 16 and 4, which are substantially similar to method claim 10, are then set forth in Section III.B below after the analysis of claim 10.

The proposed rejections of claims 7, 13, 1, 10, 16, and 4, in this order, are set forth in narrative form first. In support of the proposed rejections, and for the convenience of the examiner, Requester also presents claim charts in Sections III.A.6 and III.B.4 below to show that each limitation of claims 7 and 10 is rendered obvious by the cited prior art. The non-substantive differences between claim 7 and claims 13 and 1 are identified in Sections III.A.7 and III.A.8 below. The non-substantive differences between claim 10 and claims 16 and 14 are identified in Sections III.B.5 and III.B.6 below.

A. Proposed Rejection #1: Claims 7, 13 and 1 would have been obvious over *Savage* in view of *Maher* and *Schuba*

1. Overview of *Savage*

Like the '497 patent, *Savage* teaches a packet flooding defense method, by disclosing "a technique for tracing anonymous packet flooding attacks in the Internet back towards their source." EX1005, 295 (Abstract). Like the '497 patent, *Savage* teaches inserting a packet mark at each router that a packet is transmitted through, to aid in identifying the attacker in flood attacks. *Savage* discloses that its "solution is to probabilistically mark packets with partial path information as they arrive at routers." EX1005, 295. With reference to Figure 1 below, *Savage* discloses an exemplary network as seen from a victim V, where every potential attack origin is represented by A*i*, and routers are represented by R*i*. EX1005, 297. The dotted line in Figure 1 represents an attack path that includes the attacker (A_2) as well as all the routers (R_6, R_3, R_2, and R_1) through which the packet travelled from the attacker (A_2) to the victim (V). EX1005, 298.

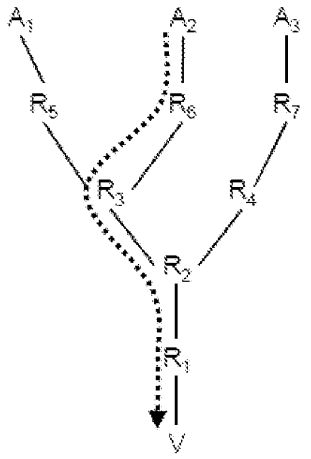


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1

Savage discloses that each router along the path "'marks' one or more packets by augmenting them with additional information about the path they are traveling." 298, 299 (describing "Node append" algorithm in Figure 2 below as "appending each node's [i.e., router's] address to the end of the packet as it travels through the network from attacker to victim.").[6] *Savage* discloses that "[c]onsequently, every packet received by the victim arrives with **a complete ordered list of the routers it**

[6] Dr. Madisetti explains that the concept of marking packets to convey information to devices receiving the packets was well-known. EX1003, ¶¶ 66, 85-90 (citing EX1036-1039).

traversed—a built-in attack path." EX1005, 299.

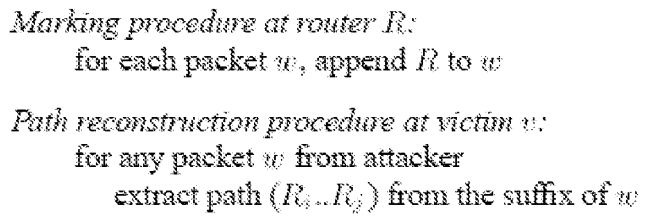


Figure 2: Node append algorithm.

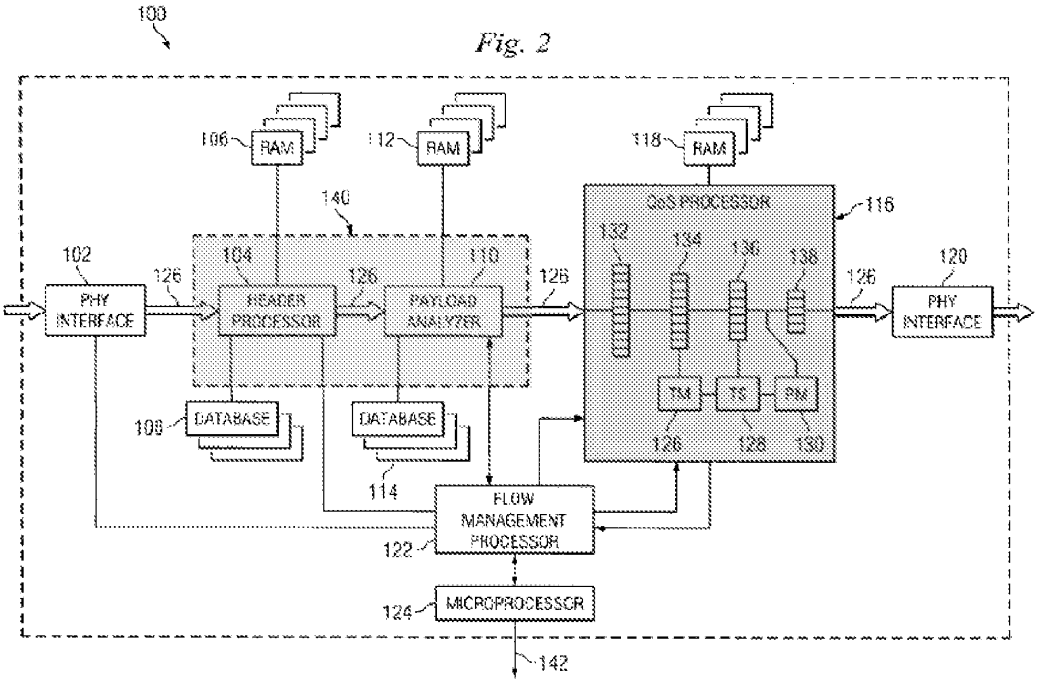
EX1005, Fig. 2

Savage teaches that the victim V then implements a "path reconstruction procedure" to "reconstruct the attack path using only the information in these marked packets." EX1005, 298.

2. Overview of *Maher*

Like the '497 patent, *Maher* is directed to "a method and apparatus for preventing denial of service type attacks on data networks." EX1006, Abstract; *see also id.*, 1:8-10, 2:52-53. Figure 2 of *Maher* below shows a network apparatus 100 "for preventing DoS attacks" that includes a traffic flow scanning engine 140 and a quality of service (QoS) processor 116. EX1006, 3:6-9, 6:11-21, 7:27-41, Abstract. *Maher* discloses that its network apparatus 100 may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67.

Fig. 2



EX1006, Fig. 2 (annotated)

The "traffic flow scanning engine is [] operable to scan the contents of the data packets, including the header and payload, and to associate data packets with particular data flows," including "determin[ing] whether each traffic flow is [] validated or non-validated." EX1006, 3:9-15, Abstract. The QoS processor then "uses the conclusion from the traffic flow scanning engine to place the data packets in the appropriate quality of service queue" (i.e., service queues 132 in Figure 2). EX1006, 3:25-27, 7:38-44. *Maher* discloses that "[d]ata packets associated with validated traffic flow are placed in a higher priority queues and transmitted back onto the network according to the protocol for the particular queue." EX1006, 3:27-

30. Conversely, "[d]ata packets not assigned to a validated traffic flow are placed in [a] low priority QoS queue," such that unvalidated traffic flow packets "receive no more than a small percentage (i.e., 5%) of the available bandwidth thereby preventing the attacker from flooding downstream network equipment." EX1006, 3:30-35, 7:67-8:3.

Maher discloses that data packets are classified (qualified) according to the path of network traffic based on the sources and destinations of the packets. *Maher* discloses that a "network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and **verifying that the contents contain valid network traffic between known sources and destinations**. Traffic flows that have not been verified **because they are from unknown sources** or because they are new unclassified flows can be assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic." EX1006, 7:54-63.

Thus, *Maher* discloses that incoming packets are scanned by the network apparatus 100, which verifies whether the contents of the packets contain valid network traffic between known sources and destinations. EX1006, 7:54-63. The scanning and analysis of the source and destination addresses in packets constitutes an analysis of the path between the source and destination of the packets. EX1003, ¶ 96.

3. Overview of *Schuba*

Like the '497 patent, *Schuba* is directed to a "computer network monitoring technique" that provides a "defense for denial of service attacks." EX1007, 1:58-60. *Schuba* discloses that messages transmitted to a network are classified as being acceptable, unacceptable, or suspect type, based on the source address of the packets. EX1007, Abstract, 2:1-5, 2:22-26, 3:8-13. *Schuba* thus teaches that incoming packets are classified into one of three states (acceptable, unacceptable, or suspect) based on the incoming packets' source address. *Id.*

4. Motivation to Combine *Savage* with *Maher* and *Schuba*

For the following reasons, a POSITA would have been motivated to combine *Savage* with *Maher* and *Schuba* to include conventional network implementation details, as disclosed by *Maher*, and to implement preventive measures to reduce the severity of denial of service attacks, as disclosed by *Maher* and *Schuba*. EX1003, ¶ 100. These references are analogous art to the challenged claims. As discussed in Sections III.A.1-III.A.3 above, *Savage*, *Maher*, and *Schuba* are each directed to addressing denial of service of attacks, like the '497 patent, and thus are each in the same field of endeavor as the '497 patent. EX1001, 1:13-15 ("the invention relates to systems for minimizing the effects of packet flooding attacks directed against computers or routers connected to a network."); EX1003, ¶ 100. Further, *Savage*, *Maher*, and *Schuba* are each directed to defending against QoS attacks, and thus are

each pertinent to a particular problem allegedly solved by the '497 patent. EX1001, 2:6-7 ("The primary objective of the present invention is to defend against 'packet flooding attacks.'"); EX1003, ¶ 100.

a. A POSITA would have been motivated to modify *Savage* to incorporate *Maher*'s conventional network implementation details

Savage teaches inserting a packet mark at each router through which a packet is transmitted, to enable the victim computer to identify the attacker in flood attacks. EX1005, 298-299. *Savage* explains that its technique is "for tracing anonymous flooding attacks in the Internet back toward their source." EX1005, Abstract. As shown in Figure 1 below, *Savage* discloses a network configuration from the perspective of a victim. EX1005, 298; EX1003, ¶ 101.

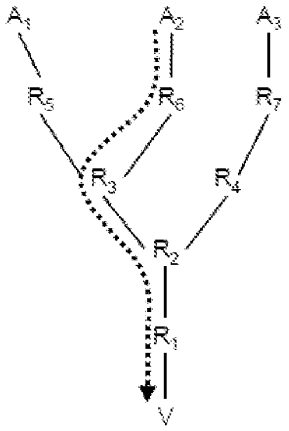


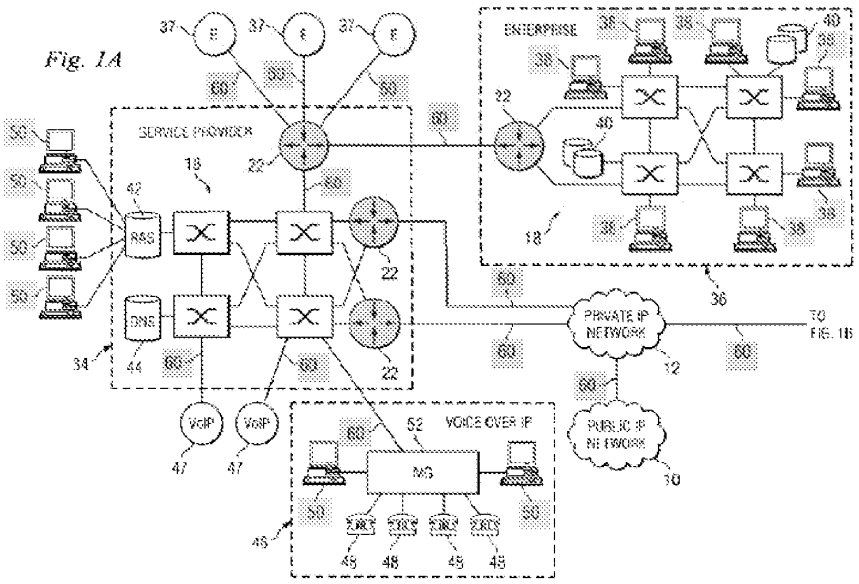
Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1.

Savage teaches that the victim V "may be a single host under attack, or a network border device such as a firewall or intrusion detection system that represents many such hosts." EX1005, § 3.1, 297. Thus, *Savage* discloses that the victim V in Figure 1 above may be a single host computer, or a network border device representing many host computers downstream of routers. EX1003, ¶ 102. By disclosing a network architecture from the perspective of a victim, *Savage* does not expressly disclose some components of a network architecture that are well-known to exist in conventional networks.

However, *Savage* explains that its technique "can be efficiently implemented using conventional technology." EX1005, Abstract. Thus, a POSITA would have been motivated to include conventional network implementation details as taught by *Maher* to implement *Savage*'s tracing technique in a network connected to the Internet. EX1005, Abstract ("This paper describes a technique for tracing anonymous packet flooding attacks in the Internet back towards their source."); EX1006, 4: (describing network topology in Fig. 1A as an "example of [a] network infrastructure[] that connect[s]…to a broader public IP network 10 such as the Internet."). As shown in Figure 1A of *Maher* below, the network topology includes a plurality of host computers (PCs) 38, 50, a plurality of routers 22, communication lines (aggregation points) 60, and transmitted data packets. EX1006, 4:3-10, 4:43-5:26. *Maher* discloses that the "method involves scanning the

contents of the data packets then verifying that the contents of the data packets conform to a set of predetermined requirements." EX1006, 2:53-55; EX1003, ¶¶ 103-104.



EX1006, Fig. 1A (annotated); EX1003, ¶ 104

Thus, in view of *Maher*'s disclosure that its network architecture connects host computers and routers to a public network such as the Internet, a POSITA would have been motivated to modify *Savage* to include the conventional implementation details of *Maher* to connect its network components to the Internet. EX1003, ¶ 105. This modification would have involved the combination of prior art elements (a QoS attack support technique as taught by *Savage*, with *Maher*'s conventional network architecture to connect host computers and routers to the Internet) according to

known methods (connecting host computers and routers to the Internet, as taught by *Maher*) to yield the predictable results of implementing *Savage*'s IP traceback technique in *Maher*'s conventional network architecture. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007); EX1003, ¶ 106. Further, a POSITA would have had a reasonable expectation of success in making this modification because *Maher* discloses that its network architecture (Fig. 1A) connects the components of its network "to a broader public IP network 10 such as the Internet." EX1006, 4:3-6. Therefore, a POSITA would have been motivated to modify *Savage* to incorporate *Maher*'s conventional network implementation details and would have a reasonable expectation of success in doing so. EX1003, ¶ 107.

b. A POSITA would have been motivated to modify *Savage* to additionally classify network traffic and limit the processing rate for unwanted data packets to reduce the severity of QoS attacks.

Savage teaches inserting a packet mark at each router that a packet is transmitted through, to aid in identifying the attacker in flood attacks. EX1005, 295 (Abstract), 298-299 (marking procedure and path reconstruction procedure). Thus, *Savage* is directed to tracking and identifying the attacker when there is a packet flooding attack, but *Savage* does not expressly disclose what preventive measures are performed in the network on unwanted packets when a packet flooding attack has occurred. *Savage* is directed to preventing continuation of a packet flooding

attack by "trac[ing] attacks back towards their origin—ideally stopping an attacker at the source." EX1005, 295; EX1003, ¶ 111.

A POSITA would have been motivated to modify *Savage* to include conventional features of *Schuba* and *Maher* to provide preventive measures in the network after there has been a detection of unwanted packets (e.g., a packet flooding attack) to reduce the severity of the attack. EX1003, ¶ 112.

Schuba teaches that packets are classified as unwanted packets or wanted packets based on the source address of the packets. EX1007, Abstract, 2:1-5, 2:22-26, 3:8-13. *Maher* discloses that the contents of packets transmitted to a network are scanned to verify whether the contents contain valid network traffic between known sources and destinations. EX1006, 7:54-63. *Schuba* and *Maher* thus teach that data packets are classified into wanted and unwanted data packets. EX1003, ¶ 113.

Further, *Maher* teaches that when packets are classified as unwanted packets, the unwanted data packets are assigned to a low quality of service queue, and the data processing rate is significantly decreased (e.g., 5% of available bandwidth) for those unwanted packets, to reduce the severity and impact of a DoS attack. EX1006, 7:59-8:3. A POSITA would have been motivated to modify *Savage* to, once there has been a detection of unwanted data, limit the data processing rate (e.g., to 5% as disclosed by *Maher*) to curtail the impact of the packet flood attack. EX1003, ¶ 114. *Savage* leaves open and does not address the implementation details regarding

preventive measures such as classifying incoming data packets and limiting the data processing rate for unwanted data packets. But *Maher* and *Schuba* both provide a number of beneficial reasons why including these preventive measures in a system like *Savage* would be advantageous. For example, *Maher* provides an explicit motivation, as it teaches that incoming data packets that have been classified as low quality are processed separately in low priority service queues, which "ensures that DoS traffic would receive no more tha[n] a small percentage (i.e. 5%) of the available bandwidth thereby preventing the attacker from flooding downstream network equipment." EX1006, 7:59-8:3, 12:7-19 (limiting the amount of bandwidth available to low quality data packets so that "the attack is never allowed to consume enough network bandwidth to overwhelm the network."). Similarly, *Schuba* also provides an explicit motivation, disclosing that when an unwanted (unacceptable) data packet is received, the corresponding communication session (TCP connection) is closed to "free[] resources of the targeted destination host." EX1007, 8:18-33. Incorporating these modifications to *Savage* involves the combination of prior art elements (combining *Savage*'s traceback technique with *Maher* and *Schuba*'s classification of packets, and *Maher*'s limiting of the processing rate for unwanted data packets) according to known methods to yield predictable results (implementing *Maher* and *Schuba*'s classification of packets and reduction of the processing rate for unwanted packets). *See KSR*, 550 U.S. at 416. EX1003, ¶ 114. Further, this

obvious modification would involve the use of a known technique (*Maher* and *Schuba*'s classification of packets, and *Maher*'s limiting of the processing rate for unwanted data packets) to improve similar devices or methods in the same way, as taught by *Maher* and *Schuba*. *See KSR*, 550 U.S. at 401. EX1003, ¶ 114.

A POSITA would have been motivated to modify *Savage* in view of *Maher* to limit throughput of unwanted data packets to minimize the amount of unwanted data packets being transmitted to their destination, as disclosed by *Maher*. EX1006, 7:63-8:3; EX1003, ¶ 115. It was well-known in the art to limit the rate of traffic between a transmitting device and a receiving device. *See, e.g.*, EX1013 (Munger), at Abstract (disclosing "a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver"), 6:5-7 (same), 42:14-43:4 (limiting bandwidth available for a transmitter to prevent packet flooding attacks); EX1012 (Cheriton), 3:47-50 (detecting DoS attacks and/or high rates of data transmitted into network), 8:23-44 (utilizing a rate-limiting policer that sets a maximum transmission rate when there is excessive traffic entering the network). EX1003, ¶ 115.

Accordingly, a POSITA would have been motivated to modify *Savage* to additionally classify network traffic as unwanted data packets or wanted data packets and limit the processing rate for unwanted data packets to reduce the severity of QoS attacks, as taught by *Maher* and *Schuba*. EX1003, ¶ 116.

5. Claim 7 would have been obvious over *Savage* in view of *Maher* and *Schuba*

[7.0] 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:

To the extent that the preamble is limiting, it is rendered obvious by *Savage* in view of *Maher*. *Pacing Techs., LLC v. Garmin Intern., Inc.*, 778 F.3d 1021, 1023-24 (Fed. Cir. 2015) (preambles not normally limiting); EX1003, ¶ 135.

Savage discloses *a method of providing packet flooding defense for a network*. EX1003, ¶ 136. *Savage* discloses "a technique for tracing anonymous **packet flooding attacks** in the **Internet** back towards their source." EX1005, Abstract. *Savage* discloses "a general purpose traceback mechanism based on probabilistic packet marking in the network. Our approach allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs)." EX1005, Abstract. *Savage* explains that its technique "can be efficiently implemented using conventional technology." EX1005, Abstract; EX1003, ¶ 136.

With reference to Figure 1 below, *Savage* discloses a network comprising a plurality of host computers (attackers A_1-A_3 and victim V), routers (R_1-R_7), and communication lines (paths between attackers, routers, and victim V). EX1005, 298; EX1003, ¶ 137.

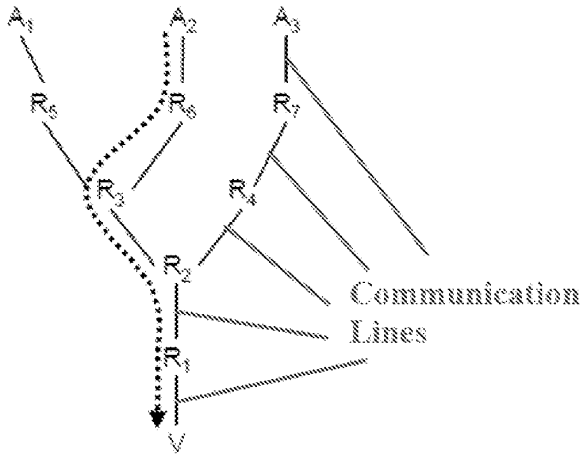


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

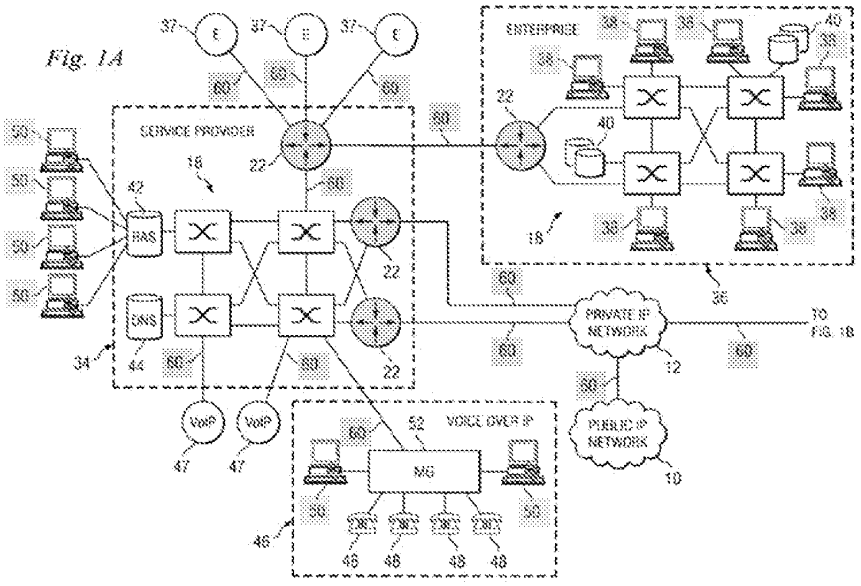
EX1005, Fig. 1 (annotated); EX1003, ¶ 137

Savage discloses that its "solution is to probabilistically mark packets with partial information as they arrive at routers." EX1005, 195. Thus, *Savage* explicitly discloses a method of providing packet flooding defense for a network comprising routers, communication lines and transmitted data packets. EX1003, ¶ 138.

Savage suggests a plurality of host computers that may be victims. EX1005, 295 (discussing plural "victims"). Further, *Savage* discloses that the victim V in Figure 1 above "may be a single host under attack, or a network border device such as a firewall or intrusion detection system that **represents many such hosts**." EX1005, 297. Thus, *Savage* discloses a network including a plurality of host computers. EX1003, ¶ 139.

To the extent that *Savage* does not expressly disclose the network configuration recited in limitation [7.0], the network configuration is a conventional feature as disclosed by *Maher*. EX1003, ¶ 140.

Maher teaches "[a] method and apparatus for preventing denial of service type attacks on data networks." EX1006, Abstract; *see also id.*, 1:8-10 ("method and device that prevents denial of service type internet attacks."), 2:52-53 ("method of preventing DoS attacks."). With reference to Figure 1A below, *Maher* discloses a network topology that connects several network infrastructures to a broader public IP network 10 such as the Internet. EX1006, 4:3-6. *Maher* discloses that the network includes a plurality of host computers 38, 50, routers 22, communication lines ("aggregation points") 60, and transmitted data packets. EX1005, 4:19-5:26. *Maher* discloses that the "method involves scanning the contents of the data packets then verifying that the contents of the data packets conform to a set of predetermined requirements." EX1006, 2:53-55; EX1003, ¶ 141.



EX1006, Fig. 1A (annotated); EX1003, ¶ 141

Thus, *Maher* discloses *a network comprising a plurality of host computers, routers, communication lines and transmitted data packets*. EX1003, ¶ 142. A POSITA would have been motivated to modify *Savage* to incorporate *Maher*'s conventional network implementation details, for the reasons presented above in Section II.A.4.a. EX1003, ¶ 142.

Accordingly, *Savage* in view of *Maher* renders obvious limitation [7.0]. EX1003, ¶ 143.

[7.1.1] determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer;

Savage discloses, or at least renders obvious, *determining a path by which data packets arrive at a host computer via packet marks provided by routers leading*

to said host computer, because *Savage* discloses determining a path by which data packets arrive at a victim V (host computer) via packet marks ("mark packets") provided by each router that forwarded the packet to the victim host computer. EX1003, ¶ 144.

Savage's "solution is to probabilistically **mark packets with partial path information as they arrive at routers**." *Savage*, 295. *Savage* explains that "[w]hile each marked packet represents only a 'sample' of the path it has traversed, by combining a modest number of such packets a victim can **reconstruct the entire path**." EX1005, 295. With reference to Figure 1 below, *Savage* discloses a **marking procedure** implemented by routers, and a **path reconstruction procedure** implemented by the victim. EX1005, 298; EX1003, ¶ 145.[7]

[7] Dr. Madisetti also reviews additional background art showing that the concept of marking packets to provide information to downstream devices was well-known. EX1003, ¶¶ 85-90 (citing EX1036, §§ 5, 6.1.1; EX1037, §§ 3, 7.1; EX1038, § A.2; EX1039, §§ 5.1-5.2).

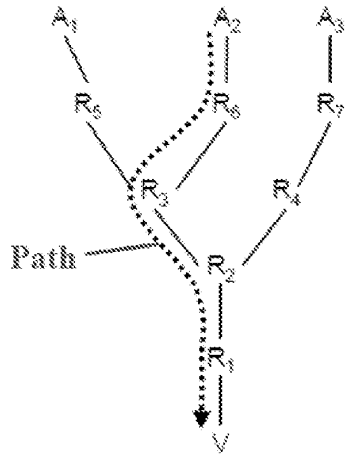


Figure 1: Network as seen from the victim of an attack, *V*. Routers are represented by *Ri*, and potential attackers by *Ai*. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1 (annotated); EX1003, ¶ 145

Savage discloses that the "attack path from [attacker] A_i is the **unique ordered list of routers between *Ai* and *V*.**" EX1005, 298. In the **marking procedure**, "[a] router 'marks' one or more packets by augmenting them with additional information about the paths they are traveling." EX1005, 298. In the **path reconstruction procedure**, the victim "reconstruct[s] the attack path using only the information in these marked packets." EX1005, 298; EX1003, ¶ 146; *see also* EX1003, ¶¶ 108-110 (providing example of path marking based on path shown in Figure 1 of *Savage*).

With reference to Figure 2 below, *Savage* discloses that "[t]he simplest marking algorithm…is to **append each node's [router's] address to the end of the**

packet as it travels through the network from attacker to victim (see Figure 2). Consequently, **every packet received by the victim arrives with a complete ordered list of the routers it traversed**—a built-in attack path." EX1005, 299. Each packet traveling through a router R is marked with that router's address, and the path encompassing each router along the path is extracted. EX1003, ¶ 147.

Marking procedure at router R:
for each packet w, append R to w

Path reconstruction procedure at victim v:
for any packet w from attacker
extract path (R_1 ...R_k) from the suffix of w

Figure 2: Node append algorithm.

EX1005, Fig. 2 (annotated); EX1003, ¶ 147

Thus, *Savage* discloses *determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer*. EX1003, ¶ 148.

[7.1.2] said path comprising all routers in said network via which said packets are routed to said computer;

Savage discloses, or at least renders obvious, limitation [7.1.2] because *Savage* teaches that each router through which a packet travels inserts a packet mark with that router's address, to permit the victim V to implement a path reconstruction procedure to determine the ordered list of routers from the attacker to the victim.

EX1003, ¶ 149. As described in Section II.B above, the examiner identified limitation [7.1.2] as the allowable feature. However, limitation [7.1.2] is disclosed by *Savage*, which was not considered by the examiner. EX1003, ¶ 149.

As shown in Figure 1 below, *Savage* discloses that the path includes all routers R in the network via which packets are routed to the computer (victim V). EX1003, 150.

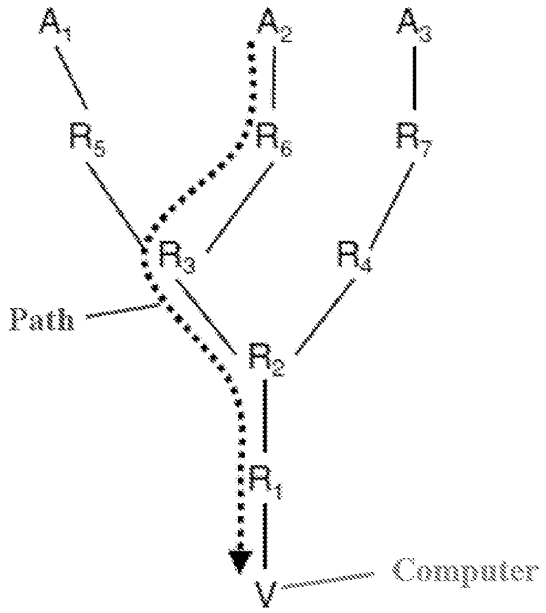


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, 298, Fig. 1 (annotated); EX1003, ¶ 150

Savage discloses that "the attack path from Ai is the **unique ordered list of**

routers between Ai and V. For instance, if an attack originates from A2 then to reach V it must first traverse the path R6, R3, R2, and R1—as shown by the dotted line in Figure 1." EX1005, 298; EX1003, ¶ 151.

With reference to Figure 2 below, *Savage* discloses that "[t]he simplest marking algorithm…is to append each node's [router's] address to the end of the packet as it travels through the network from attacker to victim (see Figure 2). Consequently, **every packet received by the victim arrives with a complete ordered list of the routers it traversed**—a built-in attack path." EX1005, 299; EX1003, ¶ 152.

Marking procedure at router R:
for each packet *w*, append *R* to *w*

Path reconstruction procedure at victim v:
for any packet *w* from attacker
extract path ($R_1 \ldots R_k$) from the suffix of *w*

Figure 2: Node append algorithm.

EX1005, Fig. 2 (annotated); EX1003, ¶ 152

Accordingly, in the following annotated example of Figure 1, *Savage* appends to the packet the addresses of routers R_6, R_3, R_2 and R_1 along the path between attacker A_2 and victim V. EX1005, 298; EX1003, ¶ 153.

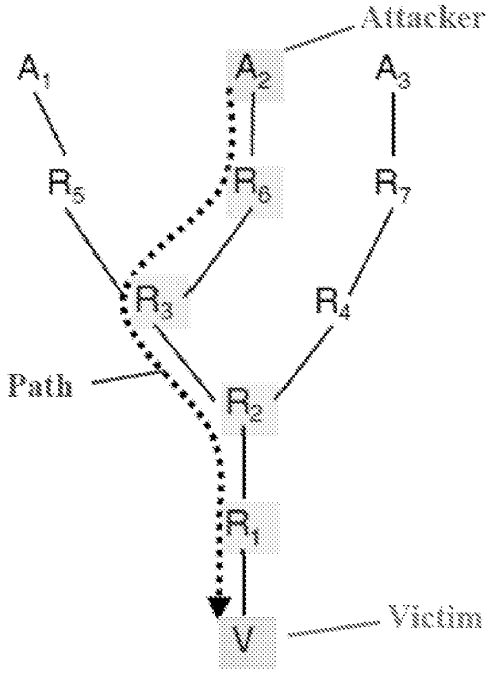


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1 (annotated); EX1003, ¶ 153

Thus, by teaching that each router along a path between an attacker and a victim inserts a packet mark constituting that router's address into the packet, *Savage* discloses *said path comprising all routers in said network via which said packets are routed to said computer*. EX1003, ¶ 154.

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

Limitation [7.2] is rendered obvious over *Savage* in view of *Schuba* and

Maher. EX1003, ¶ 155.

As described above with respect to limitations [7.1.1] and [7.1.2], *Savage* teaches that packets received at the victim host computer are marked with the respective address of each router along the path from the attacker to the victim host computer. *Schuba* teaches that incoming data packets are classified as wanted or unwanted data packets based on partial path information (source address). *Maher* teaches that data packets are classified based on path flow according to the sources and destinations of packets. For the following reasons, a POSITA would have been motivated to modify *Savage* to classify incoming data packets into wanted data packets and unwanted data packets, as taught by *Schuba*, and classify the incoming packets according to a path of the packets, as taught by *Maher*. EX1003, ¶ 155.

Like the '497 patent, *Schuba* is directed to a "computer network monitoring technique" that provides a "defense for denial of service attacks." EX1007, 1:58-60. *Schuba* discloses that messages transmitted to a network are classified as being acceptable, unacceptable, or suspect type, based on the source address of the packets. EX1007, Abstract, 2:1-5, 2:22-26, 3:8-13. *Schuba* thus teaches that incoming packets are classified into one of three states (acceptable, unacceptable, or suspect)

based on the source address of the incoming packets.[8] *Id*; EX1003, ¶ 156.

With reference to Figure 3 below, *Schuba* discloses that a monitoring resource 51 in the network system 20 performs the classification of data packets transmitted to host computers 54 in the local area network 22 over a public network such as the Internet 24. EX1007, 7:10-22, 6:46-67 (explaining network architecture); EX1003, ¶ 158.

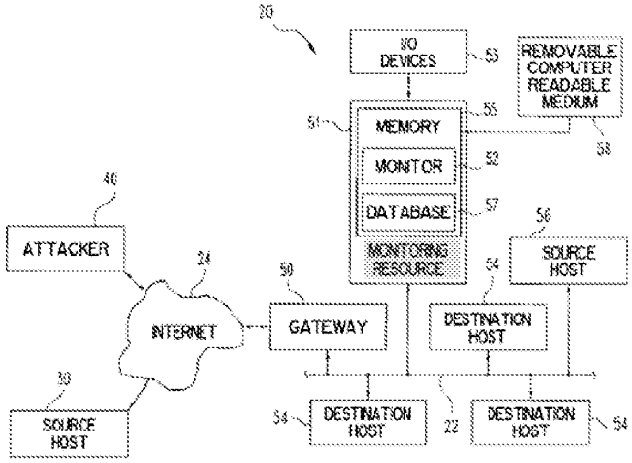


Fig. 3

EX1007, Fig. 3 (annotated); EX1003, ¶ 158

[8] Neither the specification nor the claims of the '497 patent require a classification into **only** "wanted data packets" and "unwanted data packets." The '497 patent does not exclude another category besides "wanted" or "unwanted" data packets. EX1003, ¶ 157.

Schuba explains that the monitoring resource 51 does not interfere with traffic to the host computers 54 but rather monitors incoming traffic to classify it for the host computer 54 that is the intended recipient:

> Monitor 52 [of monitoring resource 51] is preferably arranged to capture IP/TCP datagrams passing along network 22 regardless of source or destination…. Preferably, **monitor 52 does not block or interfere with the transmission of packets to destination hosts 54, but rather examines the packets** and reacts by selectively generating packets for one or more of destination hosts 54.

EX1007, 7:38-51. Thus, *Schuba* discloses that the monitoring resource 51 receives packets that are received by the host computers 54. EX1003, ¶ 159.

As shown in Figure 4 below, *Schuba* discloses that the monitoring resource 51 performs a classification operation 65 to classify incoming packets according to source addresses as wanted data packets ("ACCEPTABLE ADDRESS?" in step 68) or unwanted data packets ("UNACCEPTABLE ADDRESS?" in step 70). EX1007, 8:3-10; EX1003, ¶ 160.

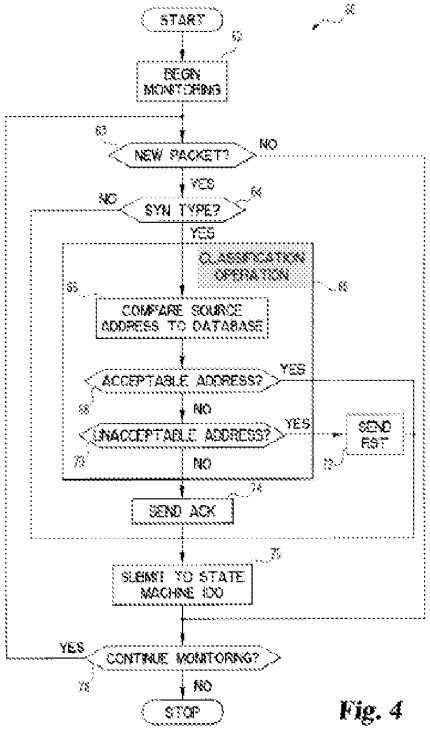


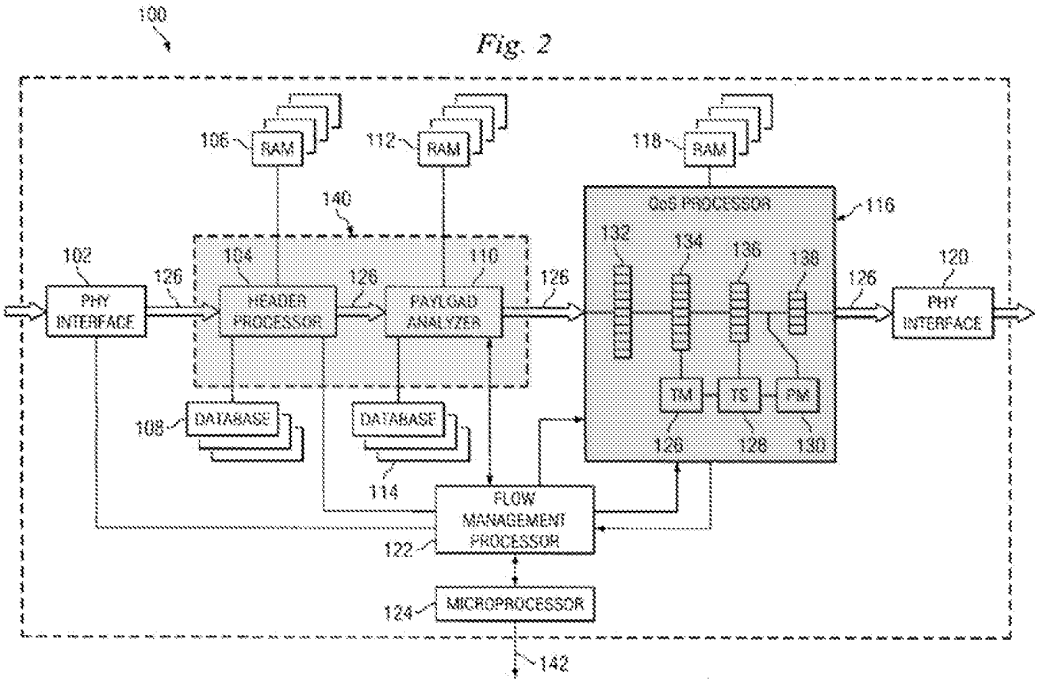
Fig. 4

EX1007, Fig. 4 (annotated); EX1003, ¶ 160

By classifying the packets based on source address, *Schuba* teaches that incoming data packets are classified as unwanted data packets ("unacceptable") or wanted data packets ("acceptable") based on at least partial path information (source address). EX1003, ¶ 161.

As discussed below, *Maher* teaches that data packets are classified (qualified) based on path flow according to the source and destination of packets, which corresponds to a path taken between the source and destination of the packet. EX1003, ¶ 162.

Maher is directed to "a method and apparatus for preventing denial of service type attacks on data networks." EX1006, Abstract; *see also id.*, 1:8-10, 2:52-53. Figure 2 of *Maher* below shows a network apparatus 100 that includes a traffic flow scanning engine 140 and a quality of service (QoS) processor 116. EX1006, 6:11-21, 7:27-41. *Maher* discloses that its network apparatus 100 may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67; EX1003, ¶ 163.



EX1006, Fig. 2 (annotated); EX1003, ¶ 163

The "traffic flow scanning engine is [] operable to scan the contents of the

data packets, including the header and payload, and to associate data packets with particular data flows," including "determin[ing] whether each traffic flow is [] validated or non-validated." EX1006, 3:9-15, Abstract. The QoS processor then "uses the conclusion from the traffic flow scanning engine to place the data packets in the appropriate quality of service queue" (i.e., service queues 132 in Figure 2). EX1006, 3:25-27, 7:38-44. *Maher* discloses that "[d]ata packets associated with validated traffic flow are placed in a higher priority queues and transmitted back onto the network according to the protocol for the particular queue." EX1006, 3:27-30. Conversely, "[d]ata packets not assigned to a validated traffic flow are placed in [a] low priority QoS queue," such that unvalidated traffic flow packets "receive no more than a small percentage (i.e., 5%) of the available bandwidth thereby preventing the attacker from flooding downstream network equipment." EX1006, 3:30-35, 7:67-8:3; EX1003, ¶ 164.

Maher discloses that the data packets are classified (qualified) according to the path of network traffic based on the sources and destinations of the packets. *Maher* discloses that a "network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and **verifying that the contents contain valid network traffic between known sources and destinations**. Traffic flows that have not been verified because they are from unknown sources or because they are new unclassified flows can be assigned to a low quality of service queue until the sources

are verified or the traffic flow classified as valid traffic." EX1007, 7:54-63. The classification (qualification) of data packets based on the sources and destinations of received packets is a classification based on a path between the source of the packet and the destination of the packet (i.e., the path between the source and destination). EX1003, ¶ 165.

Accordingly, *Schuba* teaches that incoming data packets are classified as wanted or unwanted data packets based on partial path information (source address). *Maher* teaches that data packets are classified based on path flow according to the sources and destinations of packets (i.e., by a path flow between a source and destination). Thus, *Schuba* and *Maher* teach *classifying data packets received at said host computer into wanted data packets and unwanted data packets by path*, as recited in limitation [7.2].[9] EX1003, ¶ 166.

A POSITA would have been motivated to modify *Savage* to incorporate the packet classification techniques of *Schuba* and *Maher* for the reasons presented

[9] Limitation [7.2] does not does not recite that the packets are classified "by said path," as recited in limitation [7.1.2], which requires "all routers in said network via which said packets are routed to said computer." Neither the disclosed embodiments of the '497 patent, the claims, nor the prosecution history of the '497 patent require such an interpretation. EX1003, ¶ 167.

above in Section III.A.4.b. In view of the teachings of *Schuba* and *Maher*, a POSITA would have been motivated to modify *Savage* to classify incoming data packets as wanted data packets or unwanted data packets by path in either one of the following two ways. EX1003, ¶ 168.

First, a POSITA would have been motivated to modify *Savage* to include a "bump-in-the-line" type device in the network of the host computer, as taught by both *Schuba* and *Maher*, to receive data packets transmitted to the host computer and classify the received data packets as wanted data packets or unwanted data packets by path. EX1003, ¶ 169. As discussed above, *Schuba* teaches that the monitoring resource 51, which performs the classification operation 65 shown in Figure 4, is a bump-in-the-line type device in the network 22 that "does not block or interfere with the transmission of packets to destination hosts 54, but rather examines the packets" that are transmitted to downstream host computers (e.g., destination hosts 54), as shown in annotated Figure 3 below. EX1007, 7:38-45; EX1003, ¶ 169.

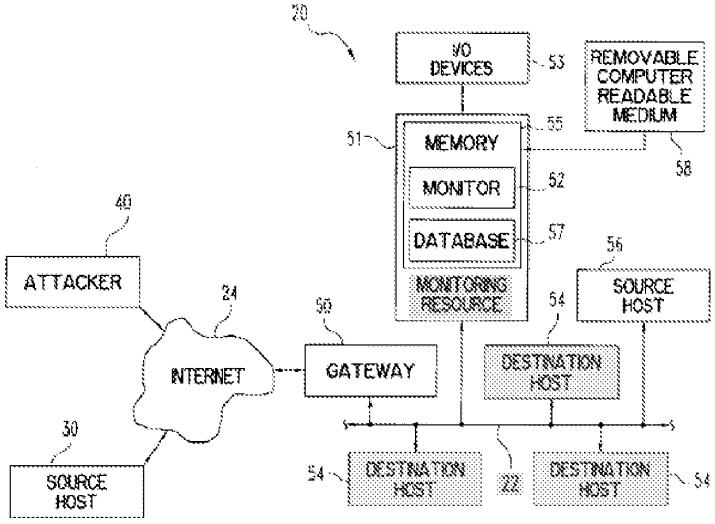


Fig. 3

EX1007, Fig. 3 (annotated); EX1003, ¶ 169

Similarly, *Maher* discloses that the network apparatus 100 (see Figure 2 above), which performs the above-described classification operation, may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. Accordingly, in view of the teachings of *Schuba* and *Maher*, a POSITA would have been motivated to include a bump-in-the-line type network device that receives data packets transmitted to *Savage*'s victim host computer V, as taught by *Schuba* and *Maher*, to *classify[] data packets received at said host computer into wanted data packets and unwanted data packets by path*, as taught by *Schuba* and *Maher*. A POSITA would have been motivated to include this

classification operation in a bump-in-the-line network device in *Savage*'s network to classify data packets as wanted or unwanted and then take preventive measures in the bump-in-the-line network device as taught by *Maher* and *Schuba* (e.g., limiting the amount of bandwidth available to low quality data packets) to curtail the impact of a packet flood attack to the host computer in *Savage*, as discussed above in Section III.A.4.b. EX1003, ¶ 170.

Alternatively, as another obvious modification, a POSITA would have been motivated to modify the host computer in *Savage* to classify incoming data packets into wanted data packets and unwanted data packets according to a path of the packets, as taught by *Schuba* and *Maher*. A POSITA would have been motivated to modify the host computer (victim V) in *Savage* to perform the classification techniques taught by *Schuba* and *Maher*, because *Schuba* and *Maher* teach that their classification features lead to minimizing the effects of a packet flood attack. For example, *Maher* teaches that the available bandwidth for incoming data packets is limited for incoming data packets that are classified as low priority to prevent packet flooding attacks. EX1006, 7:59-8:3, 12:7-19. Similarly, *Schuba* discloses that when an unwanted (unacceptable) data packet is received, the corresponding communication session (TCP connection) is closed to "free[] resources of the targeted destination host." EX1007, 8:18-33. Thus, a POSITA would have been motivated to incorporate the functionality of *Schuba* and *Maher*'s classification

operations in *Savage*'s host computer to minimizing the effects of a packet flood attack, as taught by *Schuba* and *Maher*. EX1003, ¶ 171. It was well-known in the art for a host computer receiving data packets to classify the received data packets as wanted or unwanted by path. For example, Chang (EX1008), which is discussed in the Background section of the '497 patent (EX1001, 1:49-2:5), and which was applied during prosecution to reject the claims of the '497 patent and its parent '190 patent (see Section II.D above), discloses that a receiver node classifies and sets a sender node into one of three modes: a green mode, a yellow mode, and a red mode, based on a "user acceptance rate," so that the flow of data into the network does "not exceed the user acceptance rate." EX1008, 2:60-64, 3:12-30, 10:8-38; EX1003, ¶ 171. Accordingly, Chang shows that it was well-known in the art for a POSITA to classify incoming data packets as wanted or unwanted data packets, as taught by *Schuba* and *Maher*, in a host computer receiving data packets. EX1003, ¶¶ 171-172.

Therefore, limitation [7.2] is rendered obvious by *Savage* in view of *Maher* and *Schuba*. EX1003, ¶ 173.

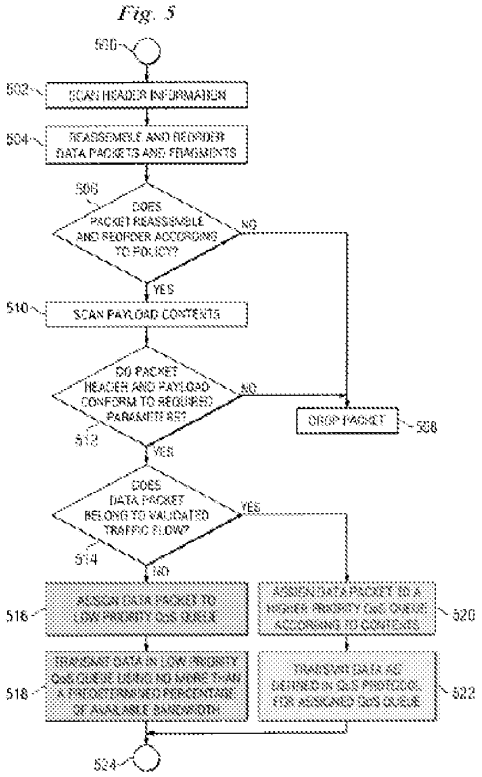
[7.3] associating a maximum acceptable processing rate with each class of data packet received at said host computer; and

Limitation [7.3] is rendered obvious by *Savage* in view of *Maher* and *Schuba*. As described above with respect to limitation [7.2], *Maher* and *Schuba* render obvious classifying incoming data packets as wanted or unwanted. *Maher* teaches

associating a maximum acceptable processing rate with each class of data packet received at the host computer, as recited in limitation [7.3]. EX1003, ¶ 174.

Maher teaches allocating maximum available bandwidth (maximum acceptable processing rate) to validated traffic (wanted data packets) and a small percentage of the available bandwidth (e.g., 5%) to low quality traffic (e.g., DoS traffic). *Maher* discloses that validated traffic (wanted data packets) are placed in different quality of service (QoS) queues than unvalidated (unwanted data packets) for processing. EX1003, ¶ 175.

With reference to Figure 5 below, *Maher* discloses that validated traffic flow (wanted data packets) is assigned to a higher priority QoS queue (YES in step 514, and step 520), which has a greater processing rate as set by the QoS processor, whereas unvalidated traffic flow (unwanted data packets) is transmitted into a low priority QoS queue (NO in step 514, and step 516), and given a limited processing rate (e.g., 5% of available bandwidth). EX1006, 11:66-12:19, 7:59-8:3 (traffic flow that has not been verified (unwanted data packets) is assigned to a low-quality traffic queue that receives limited bandwidth)). EX1003, ¶ 176.



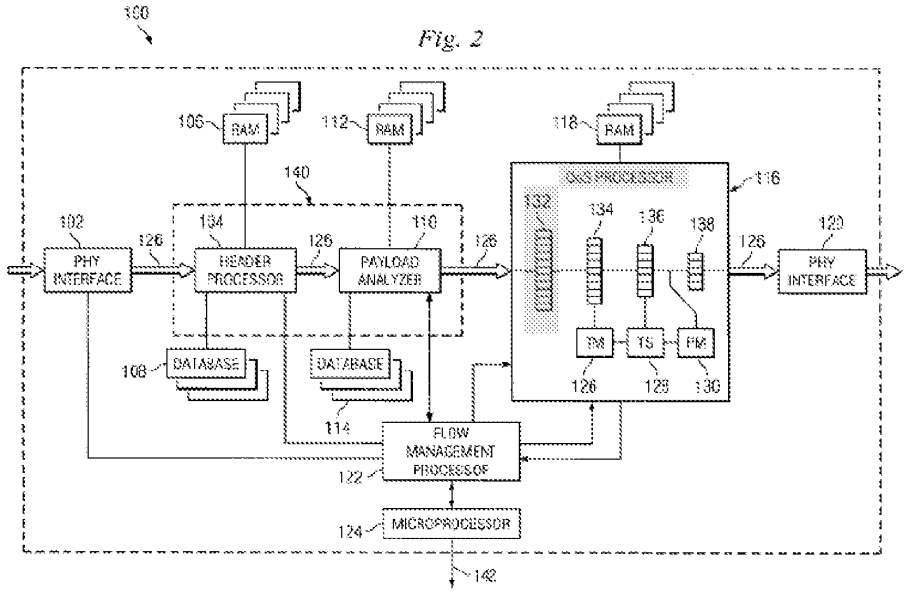
EX1006, Fig. 5 (annotated); EX1003, ¶ 176

With reference to Figure 5, *Maher* discloses that in step 514, there is a determination performed as to whether the data packet belongs to a validated traffic flow. EX1006, 11:66-67. If the packet belongs to a validated traffic flow (wanted data packets), then "**it is assigned to a higher priority QoS queue based on the nature of the traffic flow**, shown in block 520. The data packet is then transmitted onto the network as defined by the QoS protocol for the QoS queue to which it was assigned, as shown by block 522." EX1006, 11:67-12:5. On the other hand, "[i]f the packet does not belong to a validated traffic flow, such as with a Smurf or SYN flood

where valid sessions are never established, it is assigned to a low priority QoS queue, as shown in block 516. **The traffic management and traffic shaping engines 126 and 12[8] of QoS processor 116 from FIG. 2 can be programmed to [e]nsure that the low priority QoS queues are only allowed a predetermined percentage of the available bandwidth**." EX1006, 12:7-14. *Maher* explains that "[t]his [e]nsures that the non-validated data packets cannot consume more than a small portion of the overall traffic flowing through network apparatus 100 as shown in block 518." EX1006, 12:14-16. Accordingly, *Maher* discloses that each class of data packets (validated or unvalidated) is assigned to a different priority QoS queue in the QoS processor 116, where each QoS queue is allocated a different bandwidth rate. EX1003, ¶ 177.

For instance, as shown in Figure 2 below, QoS processor 116 assigns processing rates (bandwidth) by allocating received packets to different "quality of service queues 132" based on the determined quality of the received packet (validated or unvalidated data flows). EX1003, ¶ 178.

Fig. 2



EX1006, Fig. 2 (annotated); EX1003, ¶ 178

Maher discloses that each QoS queue 132 "**can be assigned priority relative to one another or can be assigned a maximum or minimum percentage of the traffic flow through the device.** This allows QoS processor to assign the necessary bandwidth to traffic flows such as VoIP, video and other flows with high quality and reliability requirements while **assigning remaining bandwidth to traffic flows with low quality requirements** such as email and general web surfing to low priority queues." EX1006, 7:38-53. Thus, *Maher* discloses that data packets of unvalidated traffic flow (unwanted data packets) are assigned to a QoS queue with a lower allocation of maximum processing rate than data packets of validated traffic flow (wanted data packets). EX1003, ¶ 179.

Therefore, *Maher* teaches limitation [7.3]. A POSITA would have been motivated to modify *Savage* in view of *Maher* and *Schuba* for the reasons presented above in Sections III.A.4.b and III.A.5[7.2]. As discussed above with respect to limitation [7.2], a POSITA would have been motivated to modify *Savage* to include a "bump-in-the-line" type device in the network of the host computer, as taught by both *Schuba* and *Maher*, to implement the packet flood preventive measures as taught by the *Maher* and *Schuba* in the "bump-in-the-line" device. EX1003, ¶ 180. Alternatively, as discussed above with respect to limitation [7.2], a POSITA would have been motivated to modify *Savage* to implement the packet flood preventive measures of *Maher* and *Schuba* in a host computer in *Savage*'s network. EX1003, ¶ 180.

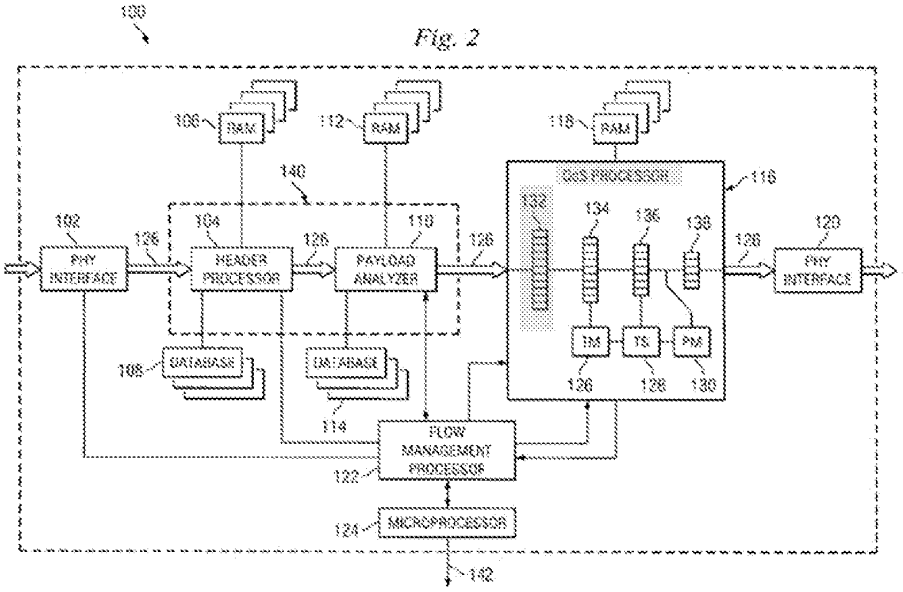
Accordingly, limitation [7.3] is rendered obvious by *Savage* in view of *Maher* and *Schuba*. EX1003, ¶ 180.

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

Limitation [7.4] is rendered obvious by *Savage* in view of *Maher*. *Maher* discloses the features of limitation [7.4], because *Maher* teaches that if received data is detected to be unverified or low quality (e.g., DoS attacks), the router (network apparatus 100) allocates a lower rate (e.g., 5%) to the received data. EX1003, ¶ 181.

With reference to Figure 2 below, *Maher* discloses that "[t]he quality of

service queues 132 [of the QoS Processor 116] also allow network apparatus 100 to manage network attacks such as denial of service (DoS) attacks. Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the contents contain valid network traffic between known sources and destinations." EX1006, 7:54-59. Further, *Maher* discloses that "[t]raffic flows that have not been verified [i.e., unwanted data packets] **because they are from unknown sources**…can be assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic." EX1006, 7:59-63. Thus, *Maher* discloses that unverified data packets (unwanted data packets) are assigned to a lower quality QoS queue 132. As described above with respect to limitation [7.3], *Maher* discloses that each different QoS queue 132 may be assigned a different maximum allocation rate based on available bandwidth in the network. EX1006, 7:38-53. Accordingly, by assigning unverified (unwanted) data packets to a low quality QoS queue 132 in comparison to verified (wanted) data packets, *Maher* discloses that a processing rate less than or equal to the maximum acceptable processing rate for the low quality QoS queue 132 is allocated. EX1003, ¶ 182. In particular, *Maher* discloses that "[t]his ensures that the DoS traffic would receive **no more tha[n] a small percentage (i.e. 5%) of the available bandwidth** thereby preventing the attacker from flooding downstream network equipment." EX1006, 7:67-8:3; EX1003, ¶ 182.



EX1006, Fig. 2 (annotated); EX1003, ¶ 182

A POSITA would have been motivated to modify *Savage* to incorporate the rate allocation techniques of *Maher* for the reasons presented above in Section III.A.4.b. As discussed above with respect to limitations [7.2] and [7.3], a POSITA would have been motivated to modify *Savage* to include a "bump-in-the-line" type device in the network of the host computer, as taught by both *Schuba* and *Maher*, to implement the packet flood preventive measures as taught by *Maher* and *Schuba* in the "bump-in-the-line" device. Thus, a POSITA would have been motivated to incorporate the rate allocation techniques of Maher in a "bump-in-the-line" type device in *Savage*'s network. EX1003, ¶ 183. Alternatively, as discussed above with respect to limitations [7.2] and [7.3], a POSITA would have been motivated to

modify *Savage* to implement the packet flood preventive measures of *Maher*, including *Maher's* rate allocation techniques, in a host computer in *Savage*'s network. EX1003, ¶ 183.

Therefore, limitation [7.4] is rendered obvious by *Savage* in view of *Maher*. EX1003, ¶ 183.

The combined teachings of *Savage*, *Maher*, and *Schuba* thus render obvious every limitation of claim 7.

6. Claim Chart Showing Unpatentability of Claim 7

Claim 7	**Unpatentable over *Savage* in view of *Maher* and *Schuba***
[7.0] 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:	*Savage* discloses *a method of providing packet flooding defense for a network*. EX1003, ¶ 136. *Savage* discloses "a technique for tracing anonymous **packet flooding attacks** in the **Internet** back towards their source." EX1005, Abstract. *Savage* discloses "a general purpose traceback mechanism based on probabilistic packet marking in the network. Our approach allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs)." EX1005, Abstract. *Savage* explains that its technique "can be efficiently implemented using conventional technology." EX1005, Abstract; EX1003, ¶ 136. With reference to Figure 1 below, *Savage* discloses a network comprising a plurality of host computers (attackers A_1-A_3 and victim V), routers (R_1-R_7), and communication lines (paths between attackers, routers, and victim V). EX1005, 298; EX1003, ¶ 137.

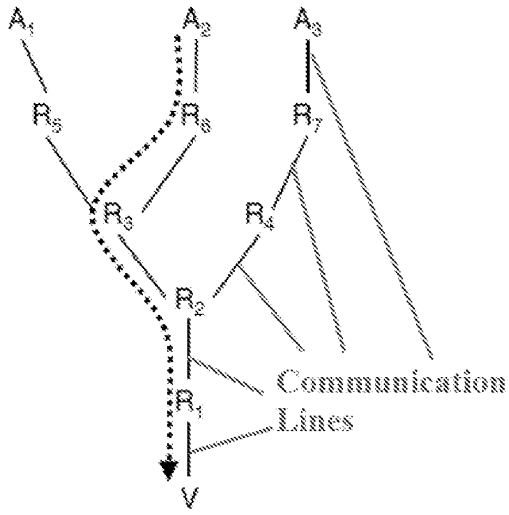


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

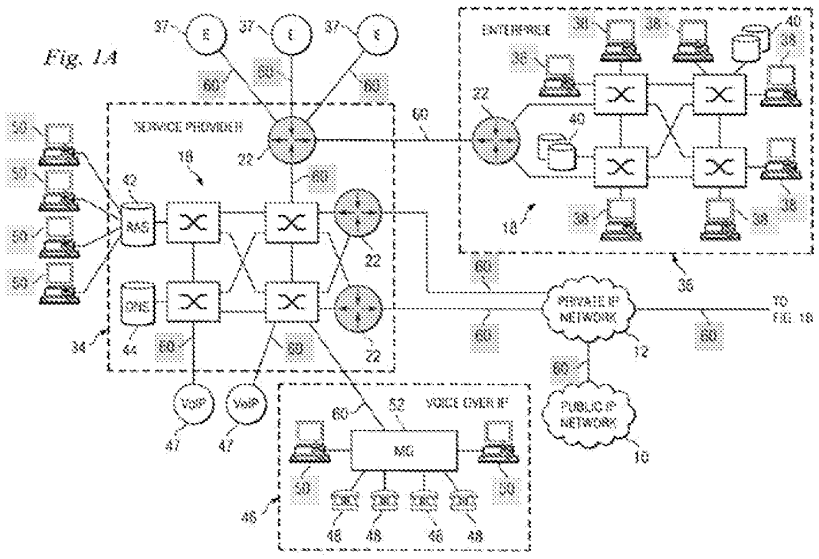
Ex. 1005, Fig. 1 (annotated); EX1003, ¶ 137

Savage discloses that its "solution is to probabilistically mark packets with partial information as they arrive at routers." EX1005, 195. Thus, *Savage* discloses a method of providing packet flooding defense for a network comprising routers, communication lines and transmitted data packets. EX1003, ¶ 138.

Savage suggests a plurality of host computers that may be victims. EX1005, 295 (discussing plural "victims"). Further, *Savage* discloses that the victim V in Figure 1 above "may be a single host under attack, or a network border device such as a firewall or intrusion detection system that **represents many such hosts**." EX1005, 297. Thus, *Savage* discloses a network including a plurality of host computers. EX1003, ¶ 139.

To the extent that *Savage* does not expressly disclose the network configuration recited in limitation [7.0], the network configuration is a conventional feature as disclosed by *Maher* (EX1005). EX1003, ¶ 140.

Maher teaches "[a] method and apparatus for preventing denial of service type attacks on data networks." EX1006, Abstract; *see also id.*, 1:8-10 ("method and device that prevents denial of service type internet attacks."), 2:52-53 ("method of preventing DoS attacks."). With reference to Figure 1A below, *Maher* discloses a network topology that connects several network infrastructures to a broader public IP network 10 such as the Internet. EX1006, 4:3-6. *Maher* discloses that the network includes a plurality of host computers 38, 50, routers 22, communication lines ("aggregation points") 60, and transmitted data packets. EX1005, 4:19-5:26. *Maher* discloses that the "method involves scanning the contents of the data packets then verifying that the contents of the data packets conform to a set of predetermined requirements." EX1006, 2:53-55; EX1003, ¶ 141.



Ex. 1006, Fig. 1A (annotated); EX1003, ¶ 141

Thus, *Maher* discloses *a network comprising a plurality of host*

	computers, routers, communication lines and transmitted data packets. EX1003, ¶ 142. A POSITA would have been motivated to modify *Savage* to incorporate *Maher*'s conventional network implementation details, for the reasons presented above in Section III.A.4.a. EX1003, ¶ 142. Accordingly, *Savage* in view of *Maher* renders obvious limitation [7.0]. EX1003, ¶ 143.
[7.1.1] determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer;	*Savage* discloses, or at least renders obvious, *determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer*, because *Savage* discloses determining a path by which data packets arrive at a victim V (host computer) via packet marks ("mark packets") provided by each router that forwarded the packet to the victim host computer. EX1003, ¶ 144. *Savage*'s "solution is to probabilistically **mark packets with partial path information as they arrive at routers**." *Savage*, 295. *Savage* explains that "[w]hile each marked packet represents only a 'sample' of the path it has traversed, by combining a modest number of such packets a victim can **reconstruct the entire path**." EX1005, 295. With reference to Figure 1 below, *Savage* discloses a **marking procedure** implemented by routers, and a **path reconstruction procedure** implemented by the victim. EX1005, 298; EX1003, ¶ 145.

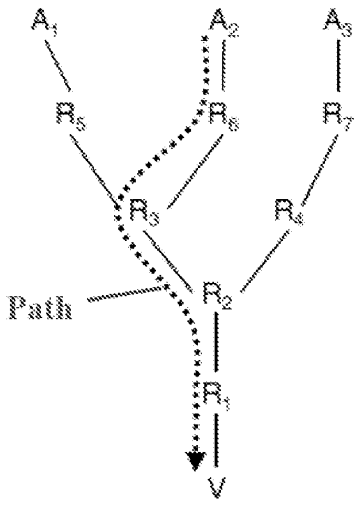


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

Ex. 1005, Fig. 1 (annotated); EX1003, ¶ 145

Savage discloses that the "attack path from [attacker] A_i is the **unique ordered list of routers between A_i and V.**" EX1005, 298. In the **marking procedure**, "[a] router 'marks' one or more packets by augmenting them with additional information about the paths they are traveling." EX1005, 298. In the **path reconstruction procedure**, the victim "reconstruct[s] the attack path using only the information in these marked packets." EX1005, 298; EX1003, ¶ 146; *see also* EX1003, ¶¶ 108-110 (providing example of path marking based on path shown in Figure 1 of *Savage*).

With reference to Figure 2 below, *Savage* discloses that "[t]he simplest marking algorithm…is to **append each node's [router's] address to the end of the packet as it travels through the network from attacker to victim** (see Figure 2). Consequently, **every packet received by the victim arrives with a complete ordered list of the routers it traversed**—a built-in

	attack path." EX1005, 299. Each packet traveling through a router R is marked with that router's address, and the path encompassing each router along the path is extracted. EX1003, ¶ 147. *Marking procedure at router R:* for each packet w, append R to w *Path reconstruction procedure at victim v:* for any packet w from attacker extract path (R_1..R_k) from the suffix of w **Figure 2: Node append algorithm.** Ex. 1005, Fig. 2 (annotated); EX1003, ¶ 147 Thus, *Savage* discloses *determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer*. EX1003, ¶ 148.
[7.1.2] said path comprising all routers in said network via which said packets are routed to said computer;	*Savage* discloses, or at least renders obvious, limitation [7.1.2] because *Savage* teaches that each router through which a packet travels inserts a packet mark with that router's address, to permit the victim V to implement a path reconstruction procedure to determine the ordered list of routers from the attacker to the victim. EX1003, ¶ 149.

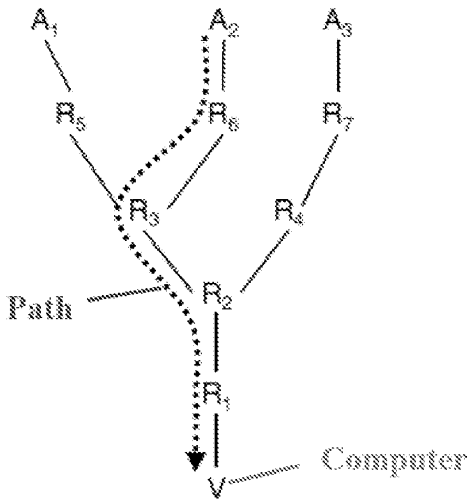


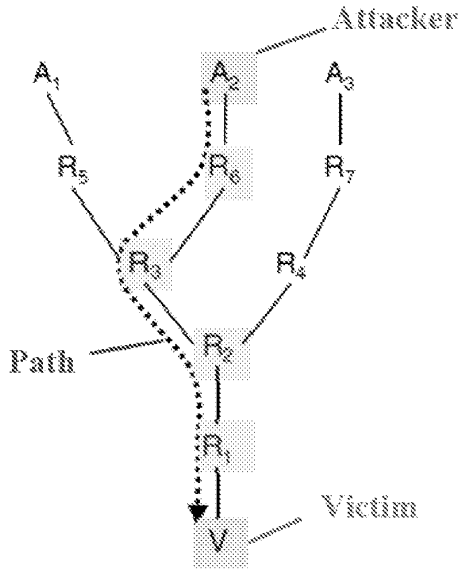
Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

Ex. 1005, Fig. 1 (annotated); EX1003, ¶ 150

Savage discloses that "the attack path from Ai is the **unique ordered list of routers between Ai and V**. For instance, if an attack originates from A2 then to reach V it must first traverse the path R6, R3, R2, and R1—as shown by the dotted line in Figure 1." EX1005, 298; EX1003, ¶ 151.

With reference to Figure 2 below, *Savage* discloses that "[t]he simplest marking algorithm…is to append each node's [router's] address to the end of the packet as it travels through the network from attacker to victim (see Figure 2). Consequently, **every packet received by the victim arrives with a complete ordered list of the routers it traversed**—a built-in attack path." EX1005, 299; EX1003, ¶ 152.

	Marking procedure at router R: for each packet w, append R to w *Path reconstruction procedure at victim v:* for any packet w from attacker extract path (R_1 ..R_k) from the suffix of w **Figure 2: Node append algorithm.** Ex. 1005, Fig. 2 (annotated); EX1003, ¶ 152 Accordingly, in the following annotated example of Figure 1, *Savage* appends to the packet the addresses of routers R_6, R_5, R_2 and R_1 along the path between attacker A_2 and victim V. EX1005, 298; EX1003, ¶ 153.

	 **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. 1005, Fig. 1 (annotated); EX1003, ¶ 153 Thus, by teaching that each router along a path between an attacker and a victim inserts a packet mark constituting that router's address into the packet, *Savage* discloses *said path comprising all routers in said network via which said packets are routed to said computer*. EX1003, ¶ 154.
[7.2] classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;	Limitation [7.2] is rendered obvious over *Savage* in view of *Schuba* and *Maher*. EX1003, ¶ 155. As described above with respect to limitations [7.1.1] and [7.1.2], *Savage* teaches that packets received at the victim host computer are marked with the respective address of each router along the path from the attacker to the victim host computer. *Schuba* teaches that incoming data packets are classified as wanted or unwanted data packets based on partial path information (source address). *Maher* teaches that data packets are classified based on path flow according to the sources and destinations of packets.

	For the following reasons, a POSITA would have been motivated to modify *Savage* to classify incoming data packets into wanted data packets and unwanted data packets, as taught by *Schuba*, and classify the incoming packets according to a path of the packets, as taught by *Maher*. EX1003, ¶ 155. Like the '497 patent, *Schuba* is directed to a "computer network monitoring technique" that provides a "defense for denial of service attacks." EX1007, 1:58-60. *Schuba* discloses that messages transmitted to a network are classified as being acceptable, unacceptable, or suspect type, based on the source address of the packets. EX1007, Abstract, 2:1-5, 2:22-26, 3:8-13. > [N]etwork messages may be classified into one or more other categories besides the suspect category. By way of nonlimiting example, TCP packets may be categorized as having an **unacceptable source address, suspect source address, or acceptable source address**. EX1007, 2:1-5. > The corresponding source address of each SYN packet is classified in one of a plurality of different categories, the categories including **a suspect source address category and an unacceptable source address category**. EX1007, 2:22-26. > In one form, **the process includes classifying source addresses of SYN packets as being of an acceptable, unacceptable, or suspect type**. Suspect source addresses may be further processed in accordance with a state machine having a number of conditionally linked states. EX1007, 3:8-13. *Schuba* thus teaches that incoming packets are classified into one of three states (acceptable, unacceptable, or suspect) based on the source address of the incoming packets. *Id*; EX1003, ¶¶ 156-157.

With reference to Figure 3 below, *Schuba* discloses that a monitoring resource 51 in the network system 20 performs the classification of data packets transmitted to host computers 54 in the local area network 22 over a public network such as the Internet 24. EX1007, 7:10-22, 6:46-67 (explaining network architecture); EX1003, ¶ 158.

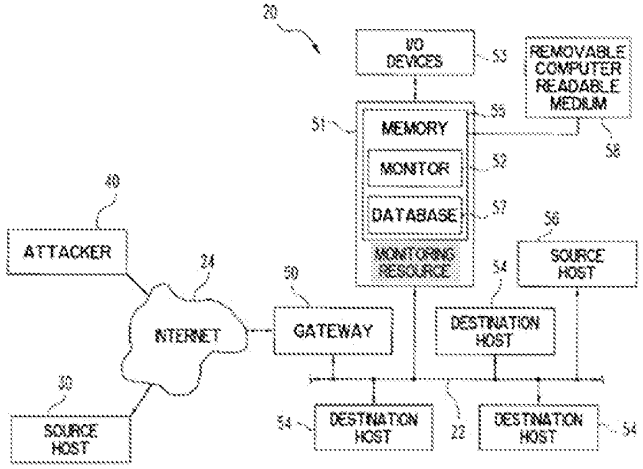


Fig. 3

Ex. 1007, Fig. 3 (annotated); EX1003, ¶ 158

Schuba explains that the monitoring resource 51 does not interfere with traffic to the host computers 54 but rather monitors incoming traffic to classify it for the host computer 54 that is the intended recipient:

> Monitor 52 [of monitoring resource 51] is preferably arranged to capture IP/TCP datagrams passing along network 22 regardless of source or destination…. Preferably, **monitor 52 does not block or interfere with the transmission of packets to destination hosts 54, but rather examines the packets** and reacts by selectively generating packets for one or more of destination hosts 54.

EX1007, 7:38-51. Thus, *Schuba* discloses that the monitoring resource 51 receives packets that are received by the host

computers 54. EX1003, ¶ 159.

As shown in Figure 4 below, *Schuba* discloses that the monitoring resource 51 performs a classification operation 65 to classify incoming packets according to source addresses as wanted data packets ("ACCEPTABLE ADDRESS?" in step 68) or unwanted data packets ("UNACCEPTABLE ADDRESS?" in step 70). EX1007, 8:3-10; EX1003, ¶ 160.

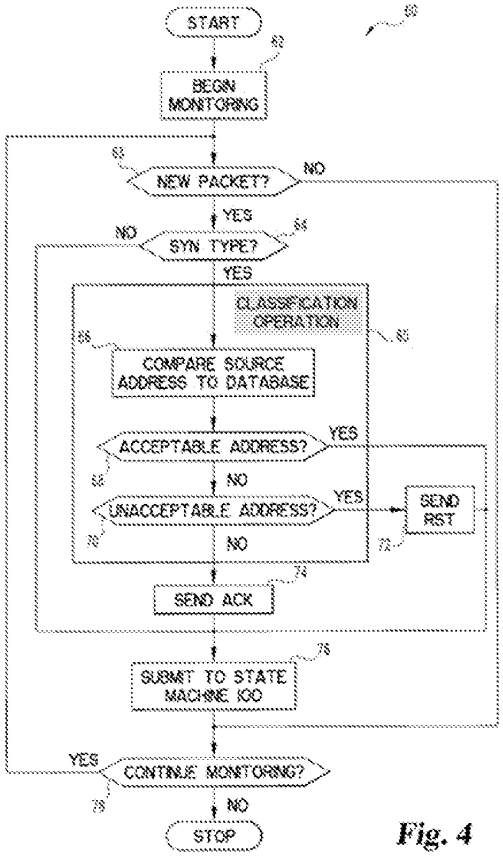


Fig. 4

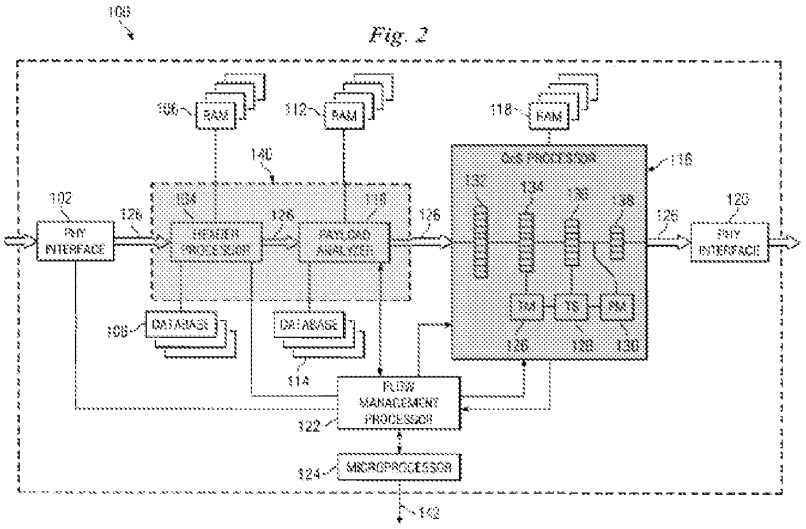
Ex. 1007, Fig. 4 (annotated); EX1003, ¶ 160

By classifying the packets based on source address, *Schuba* teaches that incoming data packets are classified as unwanted data packets ("unacceptable") or wanted data packets ("acceptable") based on at least partial path information (source address).

EX1003, ¶ 161.

As discussed below, *Maher* teaches that data packets are classified (qualified) based on path flow according to the source and destination of packets, which corresponds to a path taken between the source and destination of the packet. EX1003, ¶ 162.

Maher is directed to "a method and apparatus for preventing denial of service type attacks on data networks." EX1006, Abstract; *see also id.*, 1:8-10, 2:52-53. Figure 2 of *Maher* below shows a network apparatus 100 that includes a traffic flow scanning engine 140 and a quality of service (QoS) processor 116. EX1006, 6:11-21, 7:27-41. *Maher* discloses that its network apparatus 100 may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67; EX1003, ¶ 163.



Ex. 1006, Fig. 2 (annotated); EX1003, ¶ 163

The "traffic flow scanning engine is [] operable to scan the contents of the data packets, including the header and payload, and to associate data packets with particular data flows,"

	including "determin[ing] whether each traffic flow is [] validated or non-validated." EX1006, 3:9-15, Abstract. The QoS processor then "uses the conclusion from the traffic flow scanning engine to place the data packets in the appropriate quality of service queue" (i.e., service queues 132 in Figure 2). EX1006, 3:25-27, 7:38-44. *Maher* discloses that "[d]ata packets associated with validated traffic flow are placed in a higher priority queues and transmitted back onto the network according to the protocol for the particular queue." EX1006, 3:27-30. Conversely, "[d]ata packets not assigned to a validated traffic flow are placed in **[a] low priority QoS queue," such that unvalidated traffic flow packets "receive no more than a small percentage (i.e., 5%) of the available bandwidth thereby preventing the attacker from flooding downstream network equipment**." EX1006, 3:30-35, 7:67-8:3; EX1003, ¶ 164. *Maher* discloses that the data packets are classified (qualified) according to the path of network traffic based on the sources and destinations of the packets. *Maher* discloses that its > network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and **verifying that the contents contain valid network traffic between known sources and destinations**. Traffic flows that have not been verified because they are from unknown sources or because they are new unclassified flows can be assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic. EX1007, 7:54-63. The classification (qualification) of data packets based on the sources and destinations of received packets is a classification based on a path between the source of the packet and the destination of the packet (i.e., the path between the source and destination). EX1003, ¶ 165. Accordingly, *Schuba* teaches that incoming data packets are classified as wanted or unwanted data packets based on partial

	path information (source address). *Maher* teaches that data packets are classified based on path flow according to the sources and destinations of packets (i.e., by a path flow between a source and destination). Thus, *Schuba* and *Maher* teach *classifying data packets received at said host computer into wanted data packets and unwanted data packets by path*, as recited in limitation [7.2]. EX1003, ¶¶ 166-167. A POSITA would have been motivated to modify *Savage* to incorporate the packet classification techniques of *Schuba* and *Maher* for the reasons presented above in Section III.A.4.b. In view of the teachings of *Schuba* and *Maher*, a POSITA would have been motivated to modify *Savage* to classify incoming data packets as wanted data packets or unwanted data packets by path in either one of the following two ways. EX1003, ¶ 168. First, a POSITA would have been motivated to modify *Savage* to include a "bump-in-the-line" type device in the network of the host computer, as taught by both *Schuba* and *Maher*, to receive data packets transmitted to the host computer and classify the received data packets as wanted data packets or unwanted data packets by path. EX1003, ¶ 169. As discussed above, *Schuba* teaches that the monitoring resource 51, which performs the classification operation 65 shown in Figure 4, is a bump-in-the-line type device in the network 22 that "does not block or interfere with the transmission of packets to destination hosts 54, but rather examines the packets" that are transmitted to downstream host computers (e.g., destination hosts 54), as shown in annotated Figure 3 below. EX1007, 7:38-45; EX1003, ¶ 169.

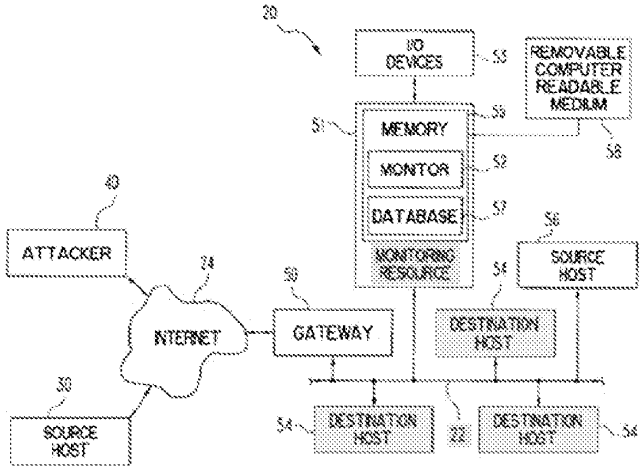


Fig. 3

Ex. 1007, Fig. 3 (annotated); EX1003, ¶ 169

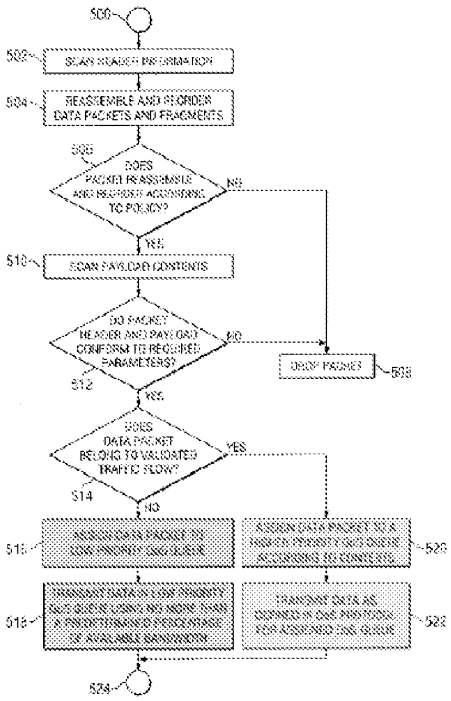
Similarly, *Maher* discloses that the network apparatus 100 (see Figure 2 above), which performs the above-described classification operation, may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. Accordingly, in view of the teachings of *Schuba* and *Maher*, a POSITA would have been motivated to include a bump-in-the-line type network device that receives data packets transmitted to *Savage*'s victim host computer V, as taught by *Schuba* and *Maher*, to *classify[] data packets received at said host computer into wanted data packets and unwanted data packets by path*, as taught by *Schuba* and *Maher*. A POSITA would have been motivated to include this classification operation in a bump-in-the-line network device in *Savage*'s network to classify data packets as wanted or unwanted and then take preventive measures in the bump-in-the-line network device as taught by *Maher* and *Schuba* (e.g., limiting the amount of bandwidth available to low quality data packets) to curtail the impact of a packet flood attack to the host computer in *Savage*, as discussed above in Section III.A.4.b. EX1003, ¶ 170.

	Alternatively, as another obvious modification, a POSITA would have been motivated to modify the host computer in *Savage* to classify incoming data packets into wanted data packets and unwanted data packets according to a path of the packets, as taught by *Schuba* and *Maher*. A POSITA would have been motivated to modify the host computer (victim V) in *Savage* to perform the classification techniques taught by *Schuba* and *Maher*, because *Schuba* and *Maher* teach that their classification features lead to minimizing the effects of a packet flood attack. For example, *Maher* teaches that the available bandwidth for incoming data packets is limited for incoming data packets that are classified as low priority to prevent packet flooding attacks. EX1006, 7:59-8:3, 12:7-19. Similarly, *Schuba* discloses that when an unwanted (unacceptable) data packet is received, the corresponding communication session (TCP connection) is closed to "free[] resources of the targeted destination host." EX1007, 8:18-33. Thus, a POSITA would have been motivated to incorporate the functionality of *Schuba* and *Maher*'s classification operations in *Savage*'s host computer to minimizing the effects of a packet flood attack, as taught by *Schuba* and *Maher*. EX1003, ¶ 171. It was well-known in the art for a host computer receiving data packets to classify the received data packets as wanted or unwanted by path. For example, Chang (EX1008), which is discussed in the Background section of the '497 patent (EX1001, 1:49-2:5), and which was applied during prosecution to reject the claims of the '497 patent and its parent '190 patent (*see* Section II.D above), discloses that a receiver node classifies and sets a sender node into one of three modes: a green mode, a yellow mode, and a red mode, based on a "user acceptance rate," so that the flow of data into the network does "not exceed the user acceptance rate." EX1008, 2:60-64, 3:12-30, 10:8-38; EX1003, ¶ 171. Accordingly, Chang shows that it was well-known in the art for a POSITA to classify incoming data packets as wanted or unwanted data packets, as taught by *Schuba* and *Maher*, in a host computer receiving data packets. EX1003, ¶ 171. Therefore, limitation [7.2] is rendered obvious by *Savage* in view

	of *Maher* and *Schuba*. EX1003, ¶¶ 173, 172 (referencing EX1011 (Stone), which teaches another example of a prior art disclosure of classifying incoming data packets as wanted or unwanted data packets.
[7.3] associating a maximum acceptable processing rate with each class of data packet received at said host computer; and	Limitation [7.3] is rendered obvious by *Savage* in view of *Maher* and *Schuba*. As described above with respect to limitation [7.2], *Maher* and *Schuba* render obvious classifying incoming data packets as wanted or unwanted. *Maher* teaches associating a maximum acceptable processing rate with each class of data packet received at the host computer, as recited in limitation [7.3]. EX1003, ¶ 174. *Maher* teaches allocating maximum available bandwidth (maximum acceptable processing rate) to validated traffic (wanted data packets) and a small percentage of the available bandwidth (e.g., 5%) to low quality traffic (e.g., DoS traffic). *Maher* discloses that validated traffic (wanted data packets) are placed in different quality of service (QoS) queues than unvalidated (unwanted data packets) for processing. > QoS processor 116 takes the conclusion of either or both of header processor 104 and payload analyzer 110 and assigns the data packet to one of its internal quality of service queues 132 based on the conclusion. **The quality of service queues 132 can be assigned priority relative to one another or can be assigned a maximum or minimum percentage of the traffic flow through the device. This allows QoS processor to assign the necessary bandwidth to traffic flows such as VoIP, video and other flows with high quality and reliability requirements while assigning remaining bandwidth to traffic flows with low quality requirements** such as email and general web surfing to low priority queues. **Information in queues that do not have the available bandwidth to transmit all the data currently residing in the queue according to the QoS engine is selectively discarded thereby removing that data from the traffic flow**.

	EX1006, 7:38-53. > The quality of service queues 132 also allow network apparatus 100 to manage network attacks such as denial of service (DoS) attacks. **Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the contents contain valid network traffic between known sources and destinations. Traffic flows that have not been verified because they are from unknown sources or because they are new unclassified flows can be assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic**. Since most DoS attacks send either new session information, data from spoofed sources, or meaningless data, network apparatus 100 would assign those traffic flows to low quality traffic queues. **This ensures that the DoS traffic would receive no more that a small percentage (i.e. 5%) of the available bandwidth thereby preventing the attacker from flooding downstream network equipment**. EX1006, 7:54-8:3; EX1003, ¶ 175. With reference to Figure 5 below, *Maher* discloses that validated traffic flow (wanted data packets) is assigned to a higher priority QoS queue (YES in step 514, and step 520), which has a greater processing rate as set by the QoS processor, whereas unvalidated traffic flow (unwanted data packets) is transmitted into a low priority QoS queue (NO in step 514, and step 516), and given a limited processing rate (e.g., 5% of available bandwidth). EX1006, 11:66-12:19, 7:59-8:3 (traffic flow that has not been verified (unwanted data packets) is assigned to a low-quality traffic queue that receives limited bandwidth)). EX1003, ¶ 176.

Fig. 5

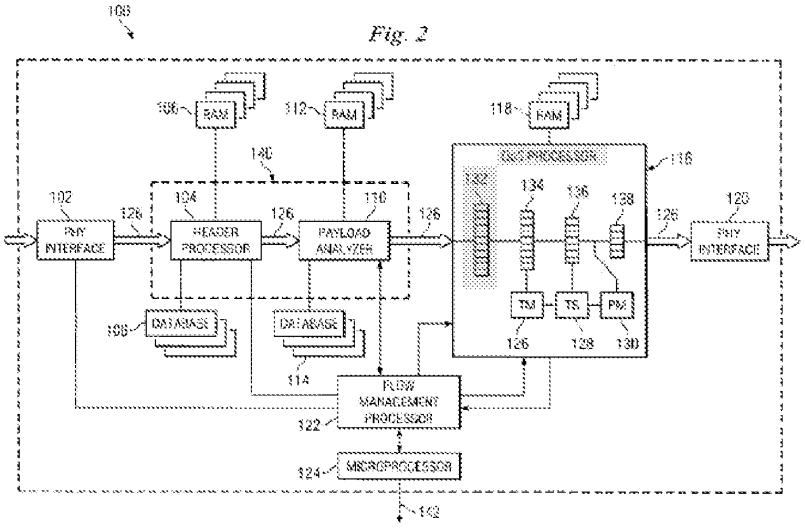


Ex. 1006, Fig. 5 (annotated); EX1003, ¶ 176

With reference to Figure 5 above, *Maher* discloses that in step 514, there is a determination performed as to whether the data packet belongs to a validated traffic flow. EX1006, 11:66-67. If the packet belongs to a validated traffic flow (wanted data packets), then "**it is assigned to a higher priority QoS queue based on the nature of the traffic flow**, shown in block 520. The data packet is then transmitted onto the network as defined by the QoS protocol for the QoS queue to which it was assigned, as shown by block 522." EX1006, 11:67-12:5. On the other hand, "[i]f the packet does not belong to a validated traffic flow, such as with a Smurf or SYN flood where valid sessions are never established, it is assigned to a low priority QoS queue, as shown in block 516. **The traffic management and traffic shaping engines 126 and 12[8] of QoS processor 116 from FIG. 2 can be programmed to [e]nsure that the low priority QoS queues are only allowed a predetermined percentage of the available**

bandwidth." EX1006, 12:7-14. *Maher* explains that "[t]his [e]nsures that the non-validated data packets cannot consume more than a small portion of the overall traffic flowing through network apparatus 100 as shown in block 518." EX1006, 12:14-16. Accordingly, *Maher* discloses that each class of data packets (validated or unvalidated) is assigned to a different priority QoS queue in the QoS processor 116, where each QoS queue is allocated a different bandwidth rate. EX1003, ¶ 177.

For instance, as shown in Figure 2 below, QoS processor 116 assigns processing rates (bandwidth) by allocating received packets to different "quality of service queues 132" based on the determined quality of the received packet (validated or unvalidated data flows). EX1003, ¶ 178.



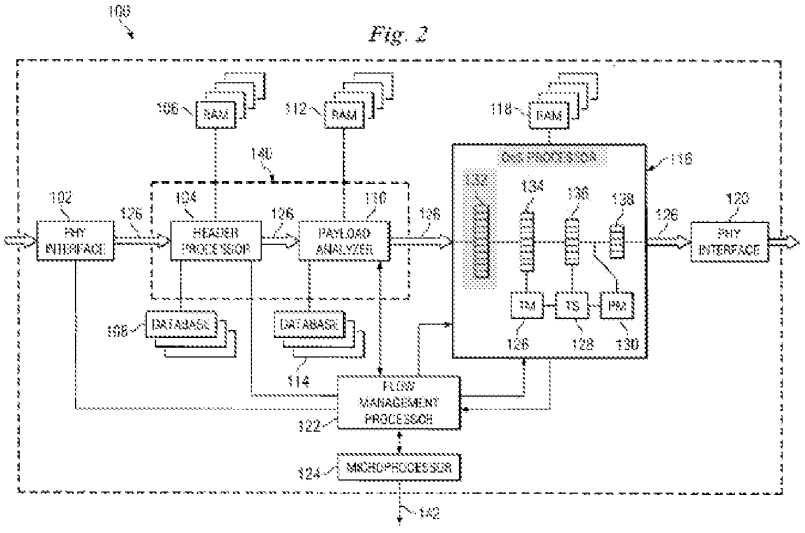
Ex. 1006, Fig. 2 (annotated); EX1003, ¶ 178

Maher discloses that each QoS queue 132 "**can be assigned priority relative to one another or can be assigned a maximum or minimum percentage of the traffic flow through the device.** This allows QoS processor to assign the necessary bandwidth to traffic flows such as VoIP, video and other flows with high quality and reliability requirements while **assigning**

	remaining bandwidth to traffic flows with low quality requirements such as email and general web surfing to low priority queues." EX1006, 7:38-53. Thus, *Maher* discloses that data packets of unvalidated traffic flow (unwanted data packets) are assigned to a QoS queue with a lower allocation of maximum processing rate than data packets of validated traffic flow (wanted data packets). EX1003, ¶ 179. Therefore, *Maher* teaches limitation [7.3]. A POSITA would have been motivated to modify *Savage* in view of *Maher* and *Schuba* for the reasons presented above in Sections III.A.4.b and III.A.5[7.2]. As discussed above with respect to limitation [7.2], a POSITA would have been motivated to modify *Savage* to include a "bump-in-the-line" type device in the network of the host computer, as taught by both *Schuba* and *Maher*, to implement the packet flood preventive measures as taught by the *Maher* and *Schuba* in the "bump-in-the-line" device. EX1003, ¶ 180. Alternatively, as discussed above with respect to limitation [7.2], a POSITA would have been motivated to modify *Savage* to implement the packet flood preventive measures of *Maher* and *Schuba* in a host computer in *Savage*'s network. EX1003, ¶ 180. Accordingly, limitation [7.3] is rendered obvious by *Savage* in view of *Maher* and *Schuba*. EX1003, ¶ 180.
[7.4] allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.	Limitation [7.4] is rendered obvious by *Savage* in view of *Maher*. *Maher* discloses the features of limitation [7.4], because *Maher* teaches that if received data is detected to be unverified or low quality (e.g., DoS attacks), the router (network apparatus 100) allocates a lower rate (e.g., 5%) to the received data. EX1003, ¶ 181. With reference to Figure 2 below, *Maher* discloses that "[t]he quality of service queues 132 [of the QoS Processor 116] also allow network apparatus 100 to manage network attacks such as denial of service (DoS) attacks. Network apparatus 100 can act to qualify traffic flows by scanning the contents of the packets and verifying that the contents contain valid network traffic between known sources and destinations." EX1006, 7:54-59. Further,

Maher discloses that "[t]raffic flows that have not been verified [i.e., unwanted data packets] **because they are from unknown sources**…can be assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic." EX1006, 7:59-63. Thus, *Maher* discloses that unverified data packets (unwanted data packets) are assigned to a lower quality QoS queue 132. As described above with respect to limitation [7.3], *Maher* discloses that each different QoS queue 132 may be assigned a different maximum allocation rate based on available bandwidth in the network. EX1006, 7:38-53. Accordingly, by assigning unverified (unwanted) data packets to a low quality QoS queue 132 in comparison to verified (wanted) data packets, *Maher* discloses that a processing rate less than or equal to the maximum acceptable processing rate for the low quality QoS queue 132 is allocated. EX1003, ¶ 182. In particular, *Maher* discloses that "[t]his ensures that the DoS traffic would receive **no more tha[n] a small percentage (i.e. 5%) of the available bandwidth** thereby preventing the attacker from flooding downstream network equipment." EX1006, 7:67-8:3; EX1003, ¶ 182.

Fig. 2



Ex. 1006, Fig. 2 (annotated); EX1003, ¶ 182

	A POSITA would have been motivated to modify *Savage* to incorporate the rate allocation techniques of *Maher* for the reasons presented above in Section III.A.4.b. As discussed above with respect to limitations [7.2] and [7.3], a POSITA would have been motivated to modify *Savage* to include a "bump-in-the-line" type device in the network of the host computer, as taught by both *Schuba* and *Maher*, to implement the packet flood preventive measures as taught by *Maher* and *Schuba* in the "bump-in-the-line" device. Thus, a POSITA would have been motivated to incorporate the rate allocation techniques of Maher in a "bump-in-the-line" type device in *Savage*'s network. EX1003, ¶ 183. Alternatively, as discussed above with respect to limitations [7.2] and [7.3], a POSITA would have been motivated to modify *Savage* to implement the packet flood preventive measures of *Maher*, including *Maher's* rate allocation techniques, in a host computer in *Savage*'s network. EX1003, ¶ 183. Therefore, limitation [7.4] is rendered obvious by *Savage* in view of *Maher*. EX1003, ¶ 183.

7. Claim 13 would have been obvious over *Savage* in view of *Maher* and *Schuba*

a. Overview of Claim 13

Claim 13 is substantially similar to claim 7, but differs in two respects. First, claim 7 is a "method" claim, whereas claim 13 is a "system" claim. Second, claim 13 recites several "means for" limitations whose functions are substantially identical to the method steps of claim 7. EX1003, ¶ 204.

The following table illustrates the differences between claims 7 and 13, with underlined text denoting the differences between the claims.

Claim 7		Claim 13	
[7.0]	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:	[13.0]	A packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system comprising:
[7.1.1]	determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer;	[13.1.1]	means for determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer;
[7.1.2]	said path comprising all routers in said network via which said packets are routed to said computer;	[13.1.2]	said path comprising all routers in said network via which said packets are routed to said computer;
[7.2]	classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;	[13.2]	means for classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;
[7.3]	associating a maximum acceptable processing rate with each class of data packet received at said host computer; and	[13.3]	means for assigning a maximum acceptable processing rate to each class of data packet; and
[7.4]	allocating a processing rate less than or equal to said maximum acceptable processing rate for	[10.4]	means for allocating a processing rate equal to or less than said maximum acceptable

	unwanted data packets.		processing rate <u>to said</u> unwanted data packets.

The above differences in claim 13 do not make claim 13 patentable. On the contrary, claim 13 would have been obvious to a POSITA over *Savage* in view of *Maher* and *Schuba*, as discussed below. EX1003, ¶ 206.

[13.0] A packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system comprising:

Limitation [13.0] is substantially similar to limitation [7.0], except that limitation [13.0] recites *a packet flooding defense system* for the network recited in limitation [7.0]. EX1003, ¶ 207.

As described above with respect to limitation [7.0], *Savage* discloses "a technique for tracing anonymous **packet flooding attacks** in the **Internet** back towards their source." EX1005, Abstract. Further, as described above with respect to limitation [7.0], *Savage* discloses a network comprising a plurality of host computers (attackers A_1-A_3 and victim V), routers (R_1-R_7), and communication lines (paths between attackers, routers, and victim V), as shown below. EX1005, 298; EX1003, ¶ 208.

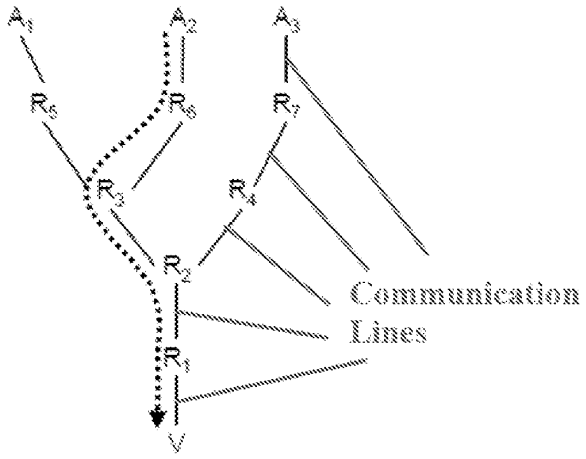


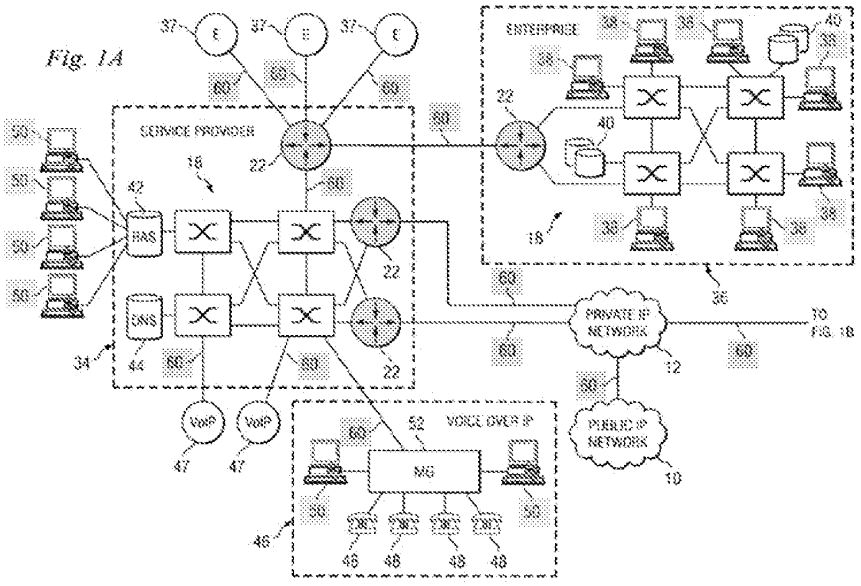
Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1 (annotated); EX1003, ¶ 208

Savage suggests a plurality of host computers that may be victims. EX1005, 295 (discussing plural "victims"). Further, *Savage* discloses that the victim V in Figure 1 above "may be a single host under attack, or a network border device such as a firewall or intrusion detection system that **represents many such hosts**." EX1005, 297. Thus, *Savage* discloses a *packet flooding defense system for a network including a plurality of host computers, routers, communication lines and transmitted data packets*. EX1005, 295, 297; EX1003, ¶ 209.

To the extent that *Savage* does not expressly disclose the network configuration recited in limitation [13.0], the network configuration is a conventional feature as disclosed by *Maher*. *Maher* teaches "[a] method and

apparatus for preventing denial of service type attacks on data networks." EX1006, Abstract; *see also id.*, 1:8-10 ("method and device that prevents denial of service type internet attacks."), 2:52-53 ("method of preventing DoS attacks."). With reference to Figure 1A below, *Maher* discloses a network topology that connects several network infrastructures to a broader public IP network 10 such as the Internet. EX1006, 4:3-6. *Maher* discloses that the network includes a plurality of host computers 38, 50, routers 22, communication lines ("aggregation points") 60, and transmitted data packets. EX1005, 4:19-5:26. *Maher* discloses that the "method involves scanning the contents of the data packets then verifying that the contents of the data packets conform to a set of predetermined requirements." EX1006, 2:53-55; EX1003, ¶ 210.



EX1006, Fig. 1A (annotated); EX1003, ¶ 210

Thus, *Maher* discloses *a packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets*. EX1003, ¶ 211.

A POSITA would have been motivated to modify *Savage* to incorporate *Maher*'s conventional network implementation details, for the reasons presented above in Section II.A.4.a. EX1003, ¶ 212.

Accordingly, *Savage* in view of *Maher* renders obvious limitation [13.0]. EX1003, ¶ 213.

[13.1.1] means for determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer;

Limitation [13.1.1] is substantially identical to limitation [7.1.1], except that

limitation [13.1.1] additionally recites "*means for*." In the district court litigation involving PacSec3 and NetScout Systems (Case No. No. 6:20-cv-00914, hereinafter "the NetScout Case"), Patent Owner filed a "Plaintiff's Opening Claim Construction Brief" (EX1014), in which Patent Owner identified alleged structure in the '497 patent that performs the functions of means-plus-function limitations in the Challenged Claims.

Specifically, Patent Owner identified computer 18 in Figures 1, 4 and 7 as performing the function of *determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer*, as recited in limitation [13.1.1]. EX1014, 27-29 (citing EX1001, 3:30-42, 5:29-33, 6:12-15, and Figures 1, 4 and 7). As described above with respect to limitation [7.1.1], *Savage* discloses that the victim computer V *determin[es] a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer*. Therefore, *Savage* discloses or renders obvious structure corresponding to the alleged structure in the '497 patent that Patent Owner identified as performing the function of limitation [13.1.1]. EX1003, ¶ 215.

[13.1.2] said path comprising all routers in said network via which said packets are routed to said computer;

Limitation [13.1.2] is identical to limitation [7.1.2], and is disclosed or rendered obvious by *Savage*, as described above with respect to limitation [7.1.2].

EX1003, ¶ 216.

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

Limitation [13.2] is substantially similar to limitation [7.2], except that limitation [13.2] additionally recites "means for."

In the NetScout Case, Patent Owner identified router 22 in Figures 1, 4 and 7 of the '497 patent as performing the function of *classifying data packets received at said host computer into wanted data packets and unwanted data packets by path*, as recited in limitation [13.2]. EX1014, 19-21 (citing EX1001, 3:30-42, 5:29-33, 6:12-25, and Figures 1, 4 and 7).

As described above with respect to limitation [7.2], *Maher* discloses that the network apparatus 100, which performs the above-described classification operation, may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. Therefore, *Maher* discloses or renders obvious structure corresponding to the alleged structure in the '497 patent that Patent Owner identified as performing the function of limitation [13.2]. EX1003, ¶ 219.

[13.3] means for assigning a maximum acceptable processing rate to each class of data packet; and

Limitation [13.3] is substantially identical to limitation [7.3], except that limitation [13.3] recites "means for assigning," whereas limitation [7.3] recites

"allocating." As described above with respect to limitation [7.3], *Maher* discloses that each QoS queue 132 "**can be assigned priority relative to one another or can be assigned a maximum or minimum percentage of the traffic flow through the device.** This allows QoS processor to assign the necessary bandwidth to traffic flows such as VoIP, video and other flows with high quality and reliability requirements while **assigning remaining bandwidth to traffic flows with low quality requirements** such as email and general web surfing to low priority queues." EX1006, 7:38-53. Thus, *Maher* discloses that data packets of unvalidated traffic flow (unwanted data packets) are assigned to a QoS queue with a lower allocation of maximum processing rate than data packets of validated traffic flow (wanted data packets). EX1003, ¶ 220.

Therefore, limitation [13.3] is rendered obvious by *Savage* in view of *Maher* and *Schuba*, for reasons similar to those presented above with respect to limitation [7.3]. EX1003, ¶ 221.

In the NetScout Case, Patent Owner identified router 22 in Figures 1, 4 and 7 of the '497 patent as performing the function of *assigning a maximum acceptable processing rate to each class of data packet*, as recited in limitation [13.3]. EX1014, 27-29 (citing EX1001, 3:30-42, 5:29-33, 6:12-25, and Figures 1, 4 and 7).

As described above with respect to limitation [7.2], *Maher* discloses that the network apparatus 100, which performs the above-described classification

operation, may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. Therefore, *Maher* discloses or renders obvious structure corresponding to the alleged structure in the '497 patent that Patent Owner identified as performing the function of limitation [13.3]. EX1003, ¶ 223.

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

Limitation [13.4] is substantially identical to limitation [7.4], except that limitation [13.4] additionally recites "means for."

In the NetScout Case, Patent Owner identified router 22 in Figures 1, 4 and 7 of the '497 patent as performing the function of *allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets*, as recited in limitation [13.4]. EX1014, 28-29 (citing EX1001, 3:30-42, 5:29-33, 6:12-25, and Figures 1, 4 and 7).

As described above with respect to limitation [7.2], *Maher* discloses that the network apparatus 100, which performs the above-described classification operation, may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. Therefore, *Maher* discloses or renders obvious structure corresponding to the alleged structure in the '497 patent that

Patent Owner identified as performing the function of limitation [13.4]. EX1003, ¶ 226.

8. Claim 1 would have been obvious over *Savage* in view of *Maher* and *Schuba*

a. Overview of Claim 1

Claim 1 is substantially similar to claim 7, but differs in three respects. First, claim 7 is a "method" claim, whereas claim 1 is a "system" claim. Second, claim 1 recites several "means for" limitations whose functions are substantially identical to the method steps of claim 7. Third, claim 1 contains a non-substantive variation from limitation [7.1.1], of *finding information regarding a path* (limitation [1.3.1] below), rather than determining a path, as recited in limitation [7.1.1]. EX1003, ¶ 227.

The following table illustrates the differences between claims 7 and 1, with underlined text denoting the differences between the claims.

Claim 7		Claim 1	
[7.0]	A <u>method of providing</u> packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said <u>method</u> comprising <u>the steps of</u>:	[1.0]	A packet flooding defense <u>system</u> for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said <u>system</u> comprising:

[7.1.1]	determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer;	[1.3.1]	means for said computer to find information for packets it receives regarding the path by which said packets came to said computer via packet marks provided by routers leading to said host computer;
[7.1.2]	said path comprising all routers in said network via which said packets are routed to said computer;	[1.3.2]	said path comprising all routers in said network via which said packets are routed to said computer;
[7.2]	classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;	[1.1]	means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;
[7.3]	associating a maximum acceptable processing rate with each class of data packet received at said host computer; and	[1.2]	means for associating a maximum acceptable processing rate with each class of data packet received at said computer;
[7.4]	allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.	[1.4]	means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate.

[1.0] A packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system comprising:

Limitation [1.0] is identical to limitation [13.0]. As described above with respect to limitation [13.0], *Savage* and *Maher* render obvious *a packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets*, as recited in limitation [1.0]. EX1003, ¶ 229.

[1.1] means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;

Limitation [1.1] is substantially similar to limitation [7.2], except that limitation [1.1] recites "means for." In the NetScout Case, Patent Owner identified router 22 in Figures 1, 4 and 7 of the '497 patent as performing the function of *classifying data packets received at a host computer into wanted data packets and unwanted data packets*, as recited in limitation [1.1]. EX1014, 19-21 (citing EX1001, 3:30-42, 5:29-33, 6:12-25, and Figures 1, 4 and 7).

As described above with respect to limitation [7.2], *Maher* discloses that the network apparatus 100, which performs the above-described classification operation, may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. Therefore, *Maher* discloses or renders

obvious structure corresponding to the alleged structure in the '497 patent that Patent Owner identified as performing the function of limitation [1.1]. EX1003, ¶ 231.

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

Limitation [1.2] is substantially similar to limitation [7.3], except that limitation [1.1] recites "means for." In the NetScout Case, Patent Owner identified router 22 in Figures 1, 4 and 7 of the '497 patent as performing the function of *associating a maximum acceptable processing rate with each class of data packet received at said computer*, as recited in limitation [1.2]. EX1014, 19-21 (citing EX1001, 3:30-42, 5:29-33, 6:12-25, and Figures 1, 4 and 7).

As described above with respect to limitation [7.2], *Maher* discloses that the network apparatus 100, which performs the above-described classification operation, may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. Therefore, *Maher* discloses or renders obvious structure corresponding to the alleged structure in the '497 patent that Patent Owner identified as performing the function of limitation [1.2]. EX1003, ¶ 233.

[1.3.1] means for said computer to find information for packets it receives regarding the path by which said packets came to said computer via packet marks provided by routers leading to said host computer;

Limitation [1.3.1] is substantially similar to limitation [7.1.1], except that

limitation [1.3.1] recites "*means for said computer to find information for packets it receives regarding the path*," whereas limitation [7.1.1] recites "*determining a path*." This difference in wording is immaterial with respect to patentability, because *Savage* discloses that a victim computer finds information for packets it receives regarding the path by which the packets came to the victim computer. EX1003, ¶ 234.

Savage discloses that each router along the path "'marks' one or more packets by augmenting them with additional information about the path they are traveling." 298, 299 (describing "Node append" algorithm in Figure 2 below as "appending each node's [i.e., router's] address to the end of the packet as it travels through the network from attacker to victim."). *Savage* discloses that "[c]onsequently, every packet received by the victim arrives with **a complete ordered list of the routers it traversed**—a built-in attack path." EX1005, 299; EX1003, ¶ 235.

Marking procedure at router R:
for each packet w, append R to w

Path reconstruction procedure at victim v:
for any packet w from attacker
extract path $(R_1..R_j)$ from the suffix of w

Figure 2: Node append algorithm.

EX1005, Fig. 2

Savage teaches that the victim V then implements a "path reconstruction

procedure" to "reconstruct the attack path using only the information in these marked packets." EX1005, 298; EX1003, ¶ 236.

Therefore, *Savage* discloses that each router along the attack path adds a packet mark identifying that router's address to the data packet as the data packets travel along the attack path, to enable a path reconstruction procedure to be performed to determine the "complete ordered list of the routers [the data packet] traversed." EX1005, 295, 298-299. Thus, *Savage* discloses the victim computer V, which performs the path reconstruction procedure, *find[s] information* (i.e., packet marks) *for packets it receives regarding the path by which said packets came to said computer via packet marks provided by routers leading to said host computer*, as recited in limitation [1.3.1]. EX1003, ¶ 237.

In the NetScout Case, Patent Owner identified computer 18 in Figures 3, 6, and 9 of the '497 patent as performing the function of *find[ing] information for packets it receives regarding the path by which said packets came to said computer via packet marks provided by routers leading to said host computer*, as recited in limitation [1.3.1]. EX1014, 19-21 (citing EX1001, 3:62-4:20, 5:40-44, 6:46-51, and Figures 1, 4 and 7).

As described above, *Savage* discloses that the victim computer V *find[s] information* (i.e., packet marks) *for packets it receives regarding the path by which said packets came to said computer via packet marks provided by routers leading to*

said host computer, as recited in limitation [1.3.1]. Therefore, *Savage* discloses or renders obvious structure corresponding to the alleged structure in the '497 patent that Patent Owner identified as performing the function of limitation [1.3.1]. EX1003, ¶ 239.

[1.3.2] said path comprising all routers in said network via which said packets are routed to said computer; and

Limitation [1.2.2] is identical to limitation [7.1.2], and is disclosed or rendered obvious by *Savage*, as described above with respect to limitation [7.1.2]. EX1003, ¶ 240.

[1.4] means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate.

Limitation [1.4] is substantially similar to limitation [7.3], except that limitation [1.4] recites "means in said computer for using said information to allocate the processing rate…," whereas limitation [7.3] recites "allocating a processing rate…."

In the NetScout Case, Patent Owner identified computer 18 in Figures 1, 4 and 7 of the '497 patent as performing the function of *using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate*, as recited in limitation [1.4]. EX1014, 25-26 (citing EX1001, 3:30-42, 5:29-33, 6:12-25, and Figures 1, 4 and 7).

As described above with respect to limitation [7.4], a POSITA would have been motivated to modify *Savage* to include a "bump-in-the-line" type device in the network of the host computer, as taught by both *Schuba* and *Maher*, to implement the packet flood preventive measures as taught by *Maher* and *Schuba* in the "bump-in-the-line" device. Therefore, *Savage* as modified by *Maher* or *Schuba* renders obvious the structure corresponding to the alleged structure in the '497 patent that Patent Owner identified as performing the function of limitation [1.4]. EX1003, ¶ 243.

B. Proposed Rejection #2: Claims 10, 16 and 4 would have been obvious over *Maher* in view of *Savage* and *Schuba*

1. Overview of Claim 10

Claim 10 is generally similar in scope to claim 7, but differs in three respects. First, the determining, classifying, and associating steps of claim 7 (limitations [7.1.1], [7.2] and [7.3]) refer to the "host computer." By contrast, the determining, classifying, and associating steps of claim 10 (limitations [10.1.1], [10.2] and [10.3]) refer to "said router," rather than the "host computer." Second, claim 7 recites that the received data packets are classified into "wanted data packets" and "unwanted data packets" by path (limitation [7.2]), whereas claim 10 recites that the received data packets are classified "at said router via packet marks." Third, the allocating step of claim 7 (limitation [7.4]) recites "allocating a processing rate," whereas the

allocating step of claim 10 (limitation [10.4]) recites "allocating a transmission rate."[10] Thus, some features of claim 7 are performed by the host computer, whereas some features of claim 10 are performed by a router in the path leading to the host computer. EX1003, ¶ 185.

The following table illustrates the differences between claims 7 and 10, with underlined text denoting the differences between the claims.

Claim 7		Claim 10	
[7.0]	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:	[10.0]	A method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said method comprising the steps of:
[7.1.1]	determining a path by which data packets arrive at <u>a host computer</u> via packet marks provided by routers leading to said host computer;	[10.1.1]	determining a path by which data packets arrive at <u>said router</u> via packet marks provided by routers leading to said host computer;
[7.1.2]	said path comprising all routers in said network via which said packets	[10.1.2]	said path comprising all routers in said network via which said packets

[10] Limitation [7.4] contains the alternative phrase "less than or equal to," which is equivalent to the alternative phrase "equal to or less than" in limitation [10.4]. EX1003, ¶ 185.

	are routed to said computer;		are routed to said computer;
[7.2]	classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;	[10.2]	classifying data packets received at said router via packet marks provided by routers leading to said host computer by path;
[7.3]	associating a maximum acceptable processing rate with each class of data packet received at said host computer; and	[10.3]	associating a maximum acceptable transmission rate with each class of data packet received at said router; and
[7.4]	allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.	[10.4]	allocating a transmission rate equal to or less than said maximum acceptable transmission rate for unwanted data packets.

The above differences in claim 10 do not make claim 10 patentable. On the contrary, claim 10 would have been obvious to a POSITA over *Maher* in view of *Savage* and *Schuba*, as discussed below. EX1003, ¶ 186.

2. Motivation to Combine *Maher* with *Savage* and *Schuba*

A POSITA would have been motivated to combine *Maher* with *Savage* and *Schuba* to determine a path by which data packets arrive at a router via packet marks provided by routers along the path, as disclosed by *Savage*, and to implement preventive measures to reduce the severity of denial of service attacks by classifying data packets, as disclosed by *Schuba*. EX1003, ¶ 117. These references are

analogous art to the claims of the '497 patent. As discussed in Sections III.A.1-III.A.3 above, *Maher*, *Savage* and *Schuba* are each directed to addressing denial of service of attacks, like the '497 patent, and thus are each in the same field of endeavor as the '497 patent. EX1001, 1:13-15 ("the invention relates to systems for minimizing the effects of packet flooding attacks directed against computers or routers connected to a network."); EX1003, ¶ 117. Further, *Maher*, *Savage* and *Schuba* are each directed to defending against QoS attacks, and thus are each pertinent to a particular problem allegedly solved by the '497 patent ("The primary objective of the present invention is to defend against 'packet flooding attacks.'"). EX1001, 2:6-7; EX1003, ¶ 117.

a. A POSITA would have been motivated to modify *Maher* to incorporate *Savage*'s technique of determining the path of data packets via packet marks provided by routers along the path

As discussed above in Section III.A.2, *Maher* is directed to "a method and apparatus for preventing denial of service type attacks on data networks." EX1006, Abstract; *see also id.*, 1:8-10, 2:52-53. Further, *Maher* discloses that the incoming data packets are classified (qualified) according to the path of network traffic based on the sources and destinations of the packets. EX1006, 7:54-63 (verifying traffic flow based on whether the source of data packets is known). EX1003, ¶ 118.

As discussed above in Section III.A.4.a and in Section IIIA.5.[7.1.2] below,

Savage teaches inserting a packet mark at each router through which a packet is transmitted, to identify the attacker in flood attacks. EX1005, 298-299. *Savage* explains that its technique is "for tracing anonymous flooding attacks in the Internet back toward their source." EX1005, Abstract; EX1003, ¶ 119. A POSITA would have been motivated to modify *Maher* to incorporate *Savage*'s technique of tracing the path from the attacker to the victim host computer, through the addition of packet marks by each router along the path through which packets traveled from the attacker to the host computer. EX1003, ¶ 119. *Savage* discloses that "mark[ing] packets with path information as they arrive at routers" allows for a victim host computer to "reconstruct the entire path." EX1005, 295. *Savage* discloses that "trac[ing] attacks back towards their origin [] ideally stop[s] an attacker at the source." EX1005, 295. Thus, a POSITA would have been motivated to modify *Maher* to incorporate *Savage*'s tracing technique of using packet marks to "stop[] an attacker at the source." EX1005, 295; EX1003, ¶ 119.

Maher is directed to a "method and apparatus for preventing denial of service attacks on data networks." EX1006, Abstract. *Maher* teaches limiting the available bandwidth for incoming data packets that have been classified as low quality to prevent a DoS attack from flooding downstream network equipment. EX1006, 7:59-8:3, 12:7-19. A POSITA would have been motivated to modify *Maher* to incorporate *Savage*'s traceback technique to "stop[] an attacker at the source," (EX1005, 295),

in view of *Maher*'s focus on "preventing denial of service attacks on data networks." EX1006, Abstract; EX1003, ¶ 120. With reference to Figure 1 below, *Savage* discloses that the victim V, which determines the path of a packet based on packet marks inserted into the packet, "may be a single host under attack, or a network border device such as a firewall or intrusion detection system that represents many such hosts." EX1005, 297; EX1003, ¶ 120.

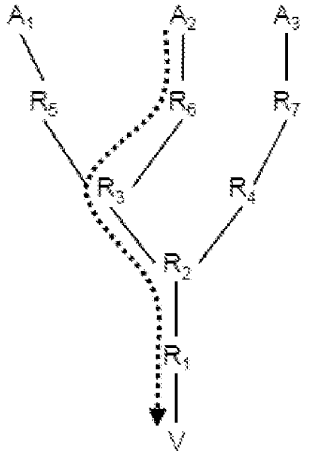
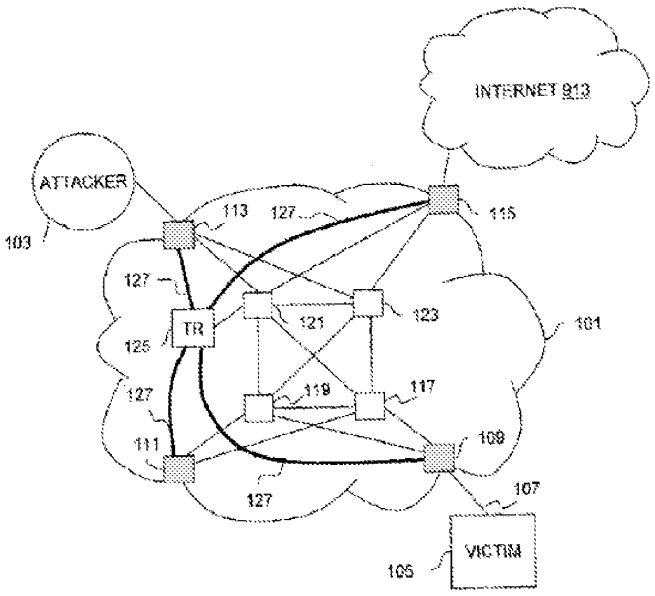


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1.

Thus, a POSITA would have been motivated to modify *Maher* to incorporate *Savage*'s traceback technique in two alternative ways. First, in view of *Savage*'s teaching that the victim V may be network border device, a POSITA would have been motivated to modify *Maher* to incorporate *Savage*'s traceback technique in any

router, switch, or "bump-in-the-line type device in *Maher*'s network. *Maher* discloses that its network apparatus 100 may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67; EX1003, ¶ 121. It was well-known in the art that network border devices may be routers in a network. For example, Stone (EX1011), which is directed to "tracking denial-of-service (DoS) flood attacks" (EX1011, Abstract), teaches that routers may be provided as network border devices, as shown by edge routers 109, 111, 113, 115 in network 101 in Figure 1 of Stone below. EX1011, 5:12-14; EX1003, ¶ 122.



EX1011, Fig. 1 (annotated); EX1003, ¶ 122

Second, in view of *Savage*'s teaching that the victim V may be a single host

computer under attack, a POSITA would have been motivated to incorporate *Savage*'s traceback technique in host computers downstream of *Maher*'s network apparatus 100. EX1003, ¶ 123.

Accordingly, a POSITA would have been motivated to modify *Maher* to incorporate *Savage*'s technique of determining the path of data packets via packet marks provided by routers along the path that the packets travelled to the host computer, as taught by *Savage*. This modification would have involved the combination of prior art elements (combining a traceback technique as taught by *Savage* with *Maher*'s conventional network architecture for preventing DoS-type attacks) according to known methods (determining the path of data packets via packet marks, as taught by *Savage*) to yield the predictable results of implementing *Maher*'s technique of preventing DoS-type attacks with *Savage*'s IP traceback technique. *See KSR*, 550 U.S. at 416 (2007); EX1003, ¶ 124. Further, a POSITA would have had a reasonable expectation of success in making this modification because *Savage* explains that its technique "can be efficiently implemented using conventional technology." EX1005, Abstract; EX1003, ¶ 124.

b. A POSITA would have been motivated to modify *Maher* to incorporate *Schuba*'s conventional technique of classifying data packets, and *Savage*'s technique of including packet marks

A POSITA would have been motivated to modify *Maher* to include

conventional features of *Schuba* to classify incoming data packets as wanted or unwanted data packets to provide preventive measures in reducing the severity of a packet flood (QoS) attack. EX1003, ¶ 125.

Maher discloses that the contents of packets transmitted to a network are scanned to verify whether the contents contain valid network traffic between known sources and destinations. EX1006, 7:54-63; EX1003, ¶ 126. As discussed above in Section III.A.5[7.1.2], *Schuba* teaches that packets are classified as unwanted packets or wanted packets based on the source address of the packets. EX1007, Abstract, 2:1-5, 2:22-26, 3:8-13. *Schuba* discloses that when an unwanted (unacceptable) data packet is received, the corresponding communication session (TCP connection) is closed to "free[] resources of the targeted destination host." EX1007, 8:18-33. Thus, *Schuba*'s classification technique provides an advantage of closing a communication session when a received packet is classified as unwanted (unacceptable). EX1003, ¶ 126.

Maher discloses that the network apparatus 100 (see Figure 2), which performs the above-described classification operation, may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67, 3:58-59. Similarly, *Schuba* teaches that its monitoring resource 51, which classifies incoming data packets into wanted or unwanted data packets, is a bump-in-the-line

type device that does not interfere with traffic to the host computers 54, as shown in annotated Figure 3 below. EX1007, 7:38-51; EX1003, ¶ 127.

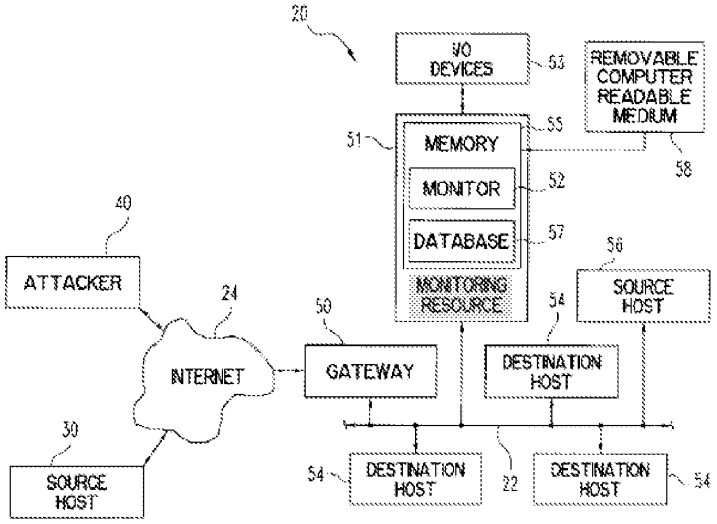


Fig. 3

EX1007, Fig. 3 (annotated); EX1003, ¶ 127

A POSITA would therefore have been motivated to implement *Schuba*'s classification technique in *Maher*'s network apparatus 100 to prevent further data communications with a source when data packets are classified as unwanted, to "free[] resources of the targeted destination host." EX1007, 8:18-33; EX1003, ¶ 128.

Further, a POSITA would have been motivated to modify *Maher* to incorporate *Savage*'s traceback technique using packet marks, to facilitate *Maher*'s classification of data packets by the source and destination of the packets. EX1003, ¶ 129. As discussed above in Section III.A.1, *Savage* discloses that each router along

the path "'marks' one or more packets by augmenting them with additional information about the path they are traveling." 298-299. *Maher* discloses that the contents of packets transmitted to a network are scanned to verify whether the contents contain valid network traffic between known sources and destinations. EX1006, 7:54-63. Having the entire path that incoming data packets took before reaching *Maher*'s network apparatus 100 would improve *Maher*'s classification of incoming network traffic based on path information using the source and destination of packets up to that point, because *Savage* teaches that the entire path from the attacker to the host computer can be determined using the packet marks inserted by the routers along the path on which a packet is transmitted. EX1005, 299 ("[E]very packet received by the victim arrives with **a complete ordered list of the routers it traversed**—a built-in attack path."). Accordingly, a POSITA would have been motivated to modify *Maher* to classify data as taught by *Schuba* (e.g., as wanted or unwanted data packets), and to insert packet marks in transmitted data packets that identify information about the entire path in the data packets received by the host computer, as taught by *Savage*. EX1003, ¶ 129. These modifications involve the combination of prior art elements (combining *Maher*'s classification technique with *Schuba*'s classification of packets as wanted or unwanted, and *Savage*'s teaching of adding packet marks at routers along the path of data flow to aid in the identification of the path of the data packets) to yield predictable results (implementing *Maher* and

Schuba's classification of packets and reduction of the processing rate for unwanted packets, and *Savage*'s marking of packets at routers). *See KSR*, 550 U.S. at 416; EX1003, ¶ 130. Further, a POSITA would have had a reasonable expectation of success in making this modification because *Maher* and *Schuba* disclose that the classification operations may be performed at a network router and/or a bump-in-the-line type device in a network, as discussed above, and *Savage* teaches that the reconstruction of the path based on the added packet marks may be performed at a network device such as a bump-in-the-line type device or by a downstream host computer. EX1005, 297 (disclosing that the victim V, which determines the path of the packet based on packet marks added to the packet, "may be a single host under attack, or a network border device such as a firewall or intrusion detection system that represents many such hosts."); EX1003, ¶ 131.

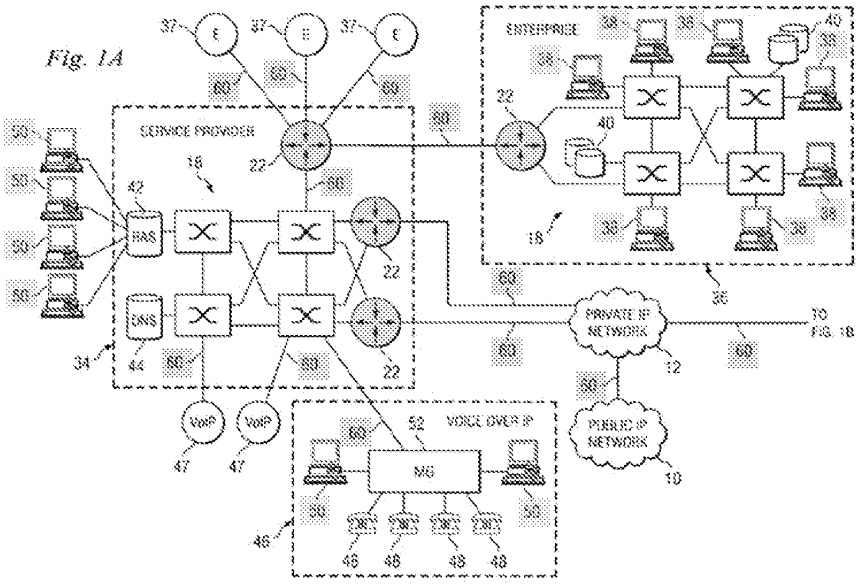
3. Claim 10 would have been obvious over *Maher* in view of *Savage* and *Schuba*

[10.0] 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:

Limitation [10.0] is identical to limitation [7.0], and is rendered obvious by *Maher* and *Savage*, as described above with respect to limitation [7.0]. *Maher* discloses *a method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data*

packets. EX1003, ¶ 187.

Maher teaches "[a] method and apparatus for preventing denial of service type attacks on data networks." EX1006, Abstract; *see also id.*, 1:8-10 ("method and device that prevents denial of service type internet attacks."), 2:52-53 ("method of preventing DoS attacks."). With reference to Figure 1A below, *Maher* discloses a network topology that connects several network infrastructures to a broader public IP network 10 such as the Internet. EX1005, 4:3-6. *Maher* discloses that the network includes a plurality of host computers 38, 50, routers 22, communication lines ("aggregation points") 60, and transmitted data packets. EX1006, 4:19-5:26. *Maher* discloses that the "method involves scanning the contents of the data packets then verifying that the contents of the data packets conform to a set of predetermined requirements." EX1006, 2:53-55; EX1003, ¶ 188.



EX1006, Fig. 1A (annotated); EX1003, ¶ 188

Therefore, *Maher* discloses *a method of providing packet flooding defense for a network*, where the *network compris[es] a plurality of host computers, routers, communication lines and transmitted data packets*. EX1003, ¶ 189.

[10.1.1] determining a path by which data packets arrive at said router via packet marks provided by routers leading to said host computer;[11]

Limitation [10.1.1] is similar to limitation [7.1.1], except that limitation

[11] The phrase "said host computer" in limitation [10.1.1] lacks antecedent basis. Challenges under 35 U.S.C. § 112 may not be raised in a request for *ex parte* reexamination. For purposes of showing that claim 10 is unpatentable as obvious

[10.1.1] recites that the path is determined "by which data packets arrive at said router…," whereas limitation [7.1.1] recites that the path is determined "by which data packets arrive at a host computer" (differences shown with underlining). As described above with respect to limitation [7.1.1], *Savage* discloses that the victim V in Figure 1 below performs a "path reconstruction procedure" to determine the "attack path from [attacker] A_i [that] is the **unique ordered list of routers between A_i and V**." EX1005, 298, 295; EX1003, ¶ 190.

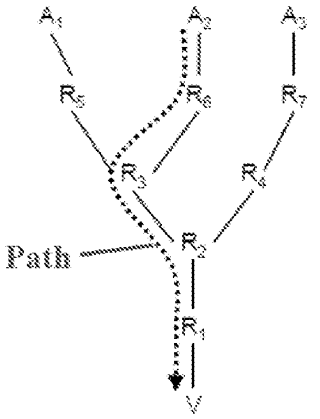


Figure 1: Network as seen from the victim of an attack, *V*. Routers are represented by *R_x*, and potential attackers by *A_x*. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1 (annotated); EX1003, ¶ 190

over the prior art cited in this Request, Requester assumes that the phrase "said host computer" refers to one of "plurality of host computers" as recited in the preamble of claim 10.

Savage discloses that the victim V in Figure 1 above "may be a single host under attack, or a **network border device** such as a firewall or intrusion detection system that represents many such hosts." EX1005, 297. *Maher* discloses that its network apparatus 100 may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. A POSITA would therefore have been motivated to perform the path reconstruction procedure disclosed by *Savage* in a router, in view of *Maher*'s disclosure that routers are configured to perform packet analysis procedures in the event of a QoS attack. Alternatively, as discussed above in Section III.B.2.b, *Savage* discloses that the operation of determining a path by which data packets arrive at said router via packet marks provided by routers leading to said host computer may be performed by a victim host computer downstream from a router. EX1005, 298-299; EX1003, 191.

Thus, *Maher* in view of *Savage* renders obvious limitation [10.1.1]. EX1003, ¶ 192.

[10.1.2] said path comprising all routers in said network via which said packets are routed to said computer;

Limitation [10.1.2] is identical to limitation [7.1.2], and is disclosed or rendered obvious by *Savage*, as described above with respect to limitation [7.1.2]. EX1003, ¶ 193.

Thus, *Maher* in view *Savage* renders obvious this limitation. EX1003, ¶ 194.

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

As described above with respect to limitation [7.2], *Maher* and *Schuba* render obvious classifying data packets as wanted and unwanted data packets received at the host computer by path. Limitation [10.2] recites "classifying data packets received at said router…," whereas limitation [7.2] recites "classifying data packets received at said host computer..." (differences shown with underlining). EX1003, ¶ 195.

Maher discloses that its network apparatus 100 may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. Accordingly, as described above in Section III.B.2.b, the classification functions of *Maher* are disclosed as being performed in a router. Therefore, *Maher* also teaches the features of limitation [10.2]. EX1003, ¶ 196.

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

Limitation [10.3] is similar to limitation [7.3] above, except that limitation [10.3] recites "associating a maximum acceptable transmission rate with each class

of data packet received at said router,"[12] whereas limitation [7.3] recites "associating a maximum acceptable processing rate with each class of data packet received at said host computer" (differences shown with underlining). EX1003, ¶ 197.

As described above, *Maher* discloses the features of limitation [7.3]. EX1003, ¶¶ 198, 174-180. *Maher* discloses that its network apparatus 100 may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. *Maher's* functions of allocating maximum available bandwidth ("*maximum acceptable transmission rate*") to validated traffic (wanted data packets) versus low quality traffic (unwanted data packets) (EX1006, 7:63-8:3) performed in a router teaches *associating a maximum acceptable transmission rate with each class of data packet received at said router*, because *Maher*'s router allocates the amount of data that would be transmitted to downstream devices serviced by the router. EX1006, 6:63-67 (describing that the disclosed "network apparatus," which performs the bandwidth allocation features and which is illustrated as a bump-in-the-line type

[12] With reference to the embodiment of Figure 3, the '497 patent explains that "the router 22 is controlling the rate of transmission of each class 38 of data packets 30 to the computer." EX1001, 6:46-51, 6:69-53 (similar disclosure with reference to Figure 4). EX1003, ¶ 199.

device in Figure 2 (EX1006, 3:58-60), may alternately "operate as a network router or switch."). Accordingly, *Maher*'s functions of associating a maximum acceptable rate are disclosed as being performed in a router that transmits data to a downstream device. EX1003, ¶ 199.

Therefore, *Maher* also teaches the features of limitation [10.3]. EX1003, ¶ 200.

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

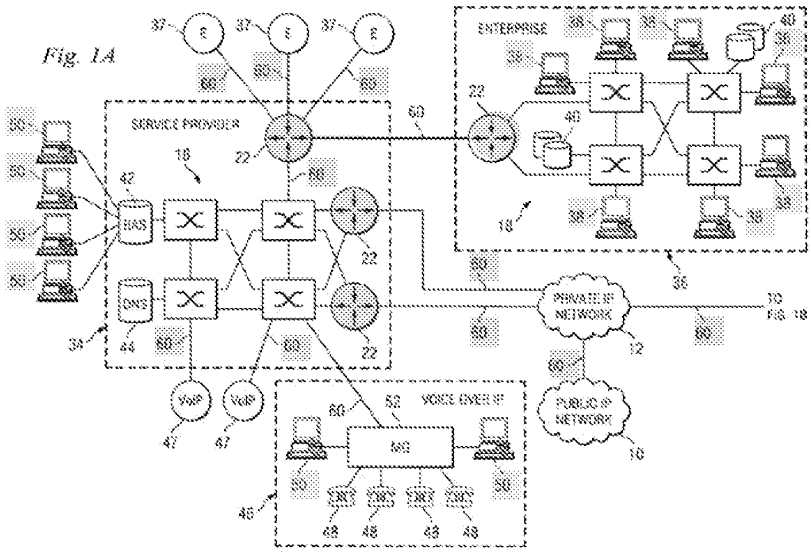
Limitation [10.4] is similar to limitation [7.4] above, except that limitation [10.4] recites "allocating a transmission rate…," whereas limitation [7.4] recites "allocating a processing rate…" (differences shown with underlining). EX1003, ¶ 201.

Maher discloses that its network apparatus 100 may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. Accordingly, *Maher*'s functions of allocating a processing rate are disclosed as being performed in a router that transmits data to a downstream device. Therefore, *Maher* also teaches allocating a transmission rate equal to or less than said maximum acceptable transmission rate for unwanted data packets, as recited in limitation [10.4], for the reasons presented above with respect to limitation [7.4]. EX1003, ¶

202.

4. Claim Chart Showing Unpatentability of Claim 10

Claim 10	Unpatentable over *Maher* in view of *Savage* and *Schuba*
[10.0] 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:	Limitation [10.0] is identical to limitation [7.0], and is rendered obvious by *Maher* and *Savage*, as described above with respect to limitation [7.0]. *Maher* discloses *a method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets*. EX1003, ¶ 187. *Maher* teaches "[a] method and apparatus for preventing denial of service type attacks on data networks." EX1006, Abstract; *see also id.*, 1:8-10 ("method and device that prevents denial of service type internet attacks."), 2:52-53 ("method of preventing DoS attacks."). With reference to Figure 1A below, *Maher* discloses a network topology that connects several network infrastructures to a broader public IP network 10 such as the Internet. EX1005, 4:3-6. *Maher* discloses that the network includes a plurality of host computers 38, 50, routers 22, communication lines ("aggregation points") 60, and transmitted data packets. EX1006, 4:19-5:26. *Maher* discloses that the "method involves scanning the contents of the data packets then verifying that the contents of the data packets conform to a set of predetermined requirements." EX1006, 2:53-55; EX1003, ¶ 188.

	 Ex. 1006, Fig. 1A (annotated); EX1003, ¶ 188 Therefore, *Maher* discloses *a method of providing packet flooding defense for a network*, where the *network compris[es] a plurality of host computers, routers, communication lines and transmitted data packets*. EX1003, ¶ 189.
[10.1.1] determining a path by which data packets arrive at said router via packet marks provided by routers leading to said host computer;	Limitation [10.1.1] is similar to limitation [7.1.1], except that limitation [10.1.1] recites that the path is determined "by which data packets arrive at said router…," whereas limitation [7.1.1] recites that the path is determined "by which data packets arrive at a host computer" (differences shown with underlining). As described above with respect to limitation [7.1.1], *Savage* discloses that the victim V in Figure 1 below performs a "path reconstruction procedure" to determine the "attack path from [attacker] A_i [that] is the **unique ordered list of routers between A_i and V**." EX1005, 298, 295; EX1003, ¶ 190.

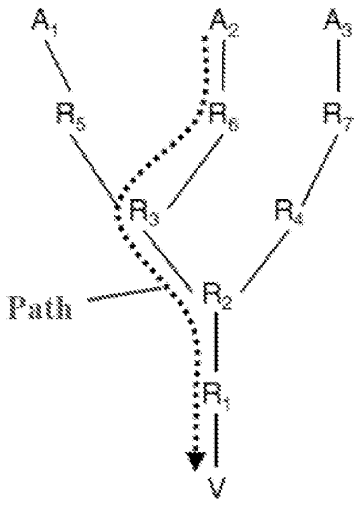


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

Ex. 1005, Fig. 1 (annotated); EX1003, ¶ 190

Savage discloses that the victim V in Figure 1 above "may be a single host under attack, or a **network border device** such as a firewall or intrusion detection system that represents many such hosts." EX1005, 297. *Maher* discloses that its network apparatus 100 may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. A POSITA would therefore have been motivated to perform the path reconstruction procedure disclosed by *Savage* in a router, in view of *Maher*'s disclosure that routers are configured to perform packet analysis procedures in the event of a QoS attack. EX1003, ¶ 191. Alternatively, as discussed above in Section III.B.2.b, *Savage* discloses that the operation of determining a path by which data packets arrive at said router via packet marks provided by routers leading to said host computer may be performed by a victim host computer downstream from a router. EX1005, 298-299; EX1003, ¶ 191.

	Thus, *Maher* in view of *Savage* renders obvious limitation [10.1.1]. EX1003, ¶ 192.
[10.1.2] said path comprising all routers in said network via which said packets are routed to said computer;	Limitation [10.1.2] is identical to limitation [7.1.2], and is disclosed or rendered obvious by *Savage*, as described above with respect to limitation [7.1.2]. EX1003, ¶¶ 193-194.
[10.2] classifying data packets received at said router via packet marks provided by routers leading to said host computer by path;	As described above with respect to limitation [7.2], *Maher* and *Schuba* render obvious classifying data packets as wanted and unwanted data packets received at the host computer by path. Limitation [10.2] recites "classifying data packets received at said router…," whereas limitation [7.2] recites "classifying data packets received at said host computer..." (differences shown with underlining). EX1003, ¶ 195. *Maher* discloses that its network apparatus 100 may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. > [A] network apparatus can be constructed according to the principles of the present invention, which is **able to operate as a network router** or switch. EX1006, 6:63-67. > Network apparatus 100, as shown, acts as a "bump-in-the-line" type device by accepting data received from a high-speed network line, processing the data, and then placing the data back on the line. EX1006, 5:62-67. Accordingly, as described above in Section III.B.2.b, the classification functions of *Maher* are disclosed as being

	performed in a router. Therefore, *Maher* also teaches the features of limitation [10.2]. EX1003, ¶ 196.
[10.3] associating a maximum acceptable transmission rate with each class of data packet received at said router; and	Limitation [10.3] is similar to limitation [7.3] above, except that limitation [10.3] recites "associating a maximum acceptable transmission rate with each class of data packet received at said router,"[13] whereas limitation [7.3] recites "associating a maximum acceptable processing rate with each class of data packet received at said host computer" (differences shown with underlining). EX1003, ¶ 197. As described above, *Maher* discloses the features of limitation [7.3]. EX1003, ¶ 198. *Maher* discloses that its network apparatus 100 may be a router or switch in the network, or a "bump-in-the-line" type device that accepts and processes the data, and then places the processed data back on the line. EX1006, 6:63-67, 5:62-67. *Maher's* functions of allocating maximum available bandwidth ("*maximum acceptable transmission rate*") to validated traffic (wanted data packets) versus low quality traffic (unwanted data packets) (EX1006, 7:63-8:3) performed in a router teaches *associating a maximum acceptable transmission rate with each class of data packet received at said router*, because *Maher*'s router allocates the amount of data that would be transmitted to downstream devices serviced by the router. EX1006, 6:63-67 (describing that the disclosed "network apparatus," which performs the bandwidth allocation features and which is illustrated as a bump-in-the-line type device in Figure 2 (EX1006, 3:58-60), may alternately "operate as a network router

[13] With reference to the embodiment of Figure 3, the '497 patent explains that "the router 22 is controlling the rate of transmission of each class 38 of data packets 30 to the computer." EX1001, 6:46-51, 6:69-53 (similar disclosure with reference to Figure 4). EX1003, ¶ 199.