	or switch."). EX1003, ¶¶ 198-199. 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. 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. > [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, *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.

5. Claim 16 would have been obvious over Maher in view of Savage and Schuba

a. Overview of Claim 16

Claim 16 is substantially similar to claim 10, but differs in two respects. First, claim 10 is a "method" claim, whereas claim 16 is a "system" claim. Second, claim 16 recites several "means for" limitations whose functions are substantially identical to the method steps of claim 10. EX1003, ¶ 244.

The following table illustrates the differences between claims 10 and 16, with underlined text denoting the differences between the claims.

Claim 10		Claim 16	
[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:	[16.0]	A packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system comprising:
[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;	[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;
[10.1.2]	said path comprising all routers in said network via which said packets are routed to said	[16.1.2]	said path comprising all routers in said network via which said packets are routed to said

	computer;		computer;
[10.2]	classifying data packets received at said router via packet marks provided by routers leading to said host computer by path;	[16.2]	means for classifying data packets received at said router into wanted data packets and unwanted data packets by path;
[10.3]	associating a maximum acceptable transmission rate with each class of data packet received at said router; and	[16.3]	means for associating a maximum acceptable transmission rate with each class of data packet received at said router; and
[10.4]	allocating a transmission rate equal to or less than said maximum acceptable transmission rate for unwanted data packets.	[16.4]	means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate.

[16.0] A packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system comprising:

As described above with respect to limitation [13.0], *Maher* discloses *a packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets*. Therefore, *Maher* discloses or renders obvious limitation [16.0]. EX1003, ¶ 246.

[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;

Limitation [16.1.1] is substantially similar to limitation [10.1.1], except that limitation [16.1.1] additionally recites "means for a router to determine." Thus, limitation [16.1.1] expressly recites that a router performs the functional language. As described above with respect to limitation [10.1.1], a POSITA 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* in view of *Savage* renders obvious limitation [16.1.1]. EX1003, ¶ 247.

[16.1.2] said path comprising all routers in said network via which said packets are routed to said computer;

Limitation [16.1.2] is identical to limitations [7.1.2] and [10.1.2], and is disclosed or rendered obvious by *Savage*, as described above with respect to limitations [7.1.2] and [10.1.2]. EX1003, ¶ 248.

[16.2] means for classifying data packets received at said router into wanted data packets and unwanted data packets by path;

Limitation [16.2] is substantially similar to limitation [10.2], except that limitation [16.2] additionally recites "means for." Further, limitation [16.2] additionally recites that the data packets are classified into wanted data packets and unwanted data packets by path. Both of these differences are obvious. EX1003, ¶

249.

As described above with respect to limitation [7.2], *Maher* and *Schuba* render obvious classifying data packets into wanted data packets and unwanted data packets by path, as recited in limitation [16.2]. EX1003, ¶ 250.

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 router into wanted data packets and unwanted data packets by path*, as recited in limitation [16.2]. EX1014, 19-24 (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 [16.2]. EX1003, ¶ 252.

Further, as described above with respect to limitation [7.2], 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*. EX1003, ¶ 253.

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

Limitation [16.3] is substantially similar to limitation [10.3], except that limitation [16.3] additionally recites "means for."

In the NetScout Case, Patent Owner identified router 22 in Figures 2, 5 and 8 of the '497 patent as performing the function of *associating a maximum acceptable transmission rate with each class of data packet received at said router*, as recited in limitation [16.3]. EX1014, 20-23 (citing EX1001, 3:43-61, 5:33-39, 6:26-46, and Figures 2, 5 and 8).

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 [16.3]. EX1003, ¶ 256.

[16.4] means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate.

Limitation [16.4] is substantially similar to limitation [10.4], except that

limitation [16.4] additionally recites "means for said router to allocate...." Thus, limitation [16.4] expressly recites that a router performs the functional language. As described above with respect to limitation [10.4], *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 means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate, as recited in limitation [16.4]. EX1003, ¶ 257.

6. Claim 4 would have been obvious over *Maher* in view of *Savage* and *Schuba*

a. Overview of Claim 4

Claim 4 is substantially similar to claim 10, but differs in three respects. First, claim 10 is a "method" claim, whereas claim 4 is a "system" claim. Second, claim 4 recites several "means for" limitations whose functions are substantially identical to the method steps of claim 10. Third, claim 4 contains a non-substantive variation from limitation [7.1.1], of *finding information regarding a path* (limitation [4.3.1] below), rather than determining a path, as recited in limitation [10.1.1]. EX1003, ¶ 258.

The following table illustrates the differences between claims 10 and 4, with underlined text denoting the differences between the claims.

Claim 10		Claim 4	
[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:	[4.0]	A packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system comprising:
[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;	[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;
[10.1.2]	said path comprising all routers in said network via which said packets are routed to said computer;	[4.3.2]	said path comprising all routers in said network via which said packets are routed to said computer;
[10.2]	classifying data packets received at said router via packet marks provided by routers leading to said host computer by path;	[4.2]	means for classifying data packets received at a router into wanted data packets and unwanted data packets;
[10.3]	associating a maximum acceptable transmission rate with each class of data packet received at said router; and	[4.3]	means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

[10.4]	allocating a transmission rate equal to or less than said maximum acceptable transmission rate for unwanted data packets.	[4.4]	means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate.

[4.0] A packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said system comprising:

As described above with respect to limitation [13.0], *Maher* discloses *a packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets*. Therefore, *Maher* discloses or renders obvious limitation [4.0]. EX1003, ¶ 260.

[4.1] means for classifying data packets received at a router into wanted data packets and unwanted data packets;

Limitation [4.1] is substantially similar to limitation [16.2], except that it is broader because it does not require classifying data packets "by path," as recited in limitation [16.2]. Limitation [4.1] is rendered obvious for the reasons presented above with respect to limitation [16.2], which also shows that the prior art renders obvious the alleged structure that Patent Owner identified as corresponding to the "means for" features of limitation [4.1]. EX1003, ¶ 261.

[4.2] means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

Limitation [4.2] is identical to limitation [16.3], and is rendered obvious for the same reasons presented above with respect to limitation [16.3]. EX1003, ¶ 262.

[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;

Limitation [4.3.1] is substantially similar to limitation [10.1.1], except that limitation [4.3.1] recites "*means for said router computer to find information for packets it receives regarding the path*," whereas limitation [10.1.1] recites "*determining a path*." This difference in wording is immaterial with respect to patentability, because *Savage* discloses a network device receiving packets finds information for packets it receives regarding the path by which the packets came to that network device. EX1003, ¶ 263.

As described above with respect to limitation [10.1.1], *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, ¶ 264.

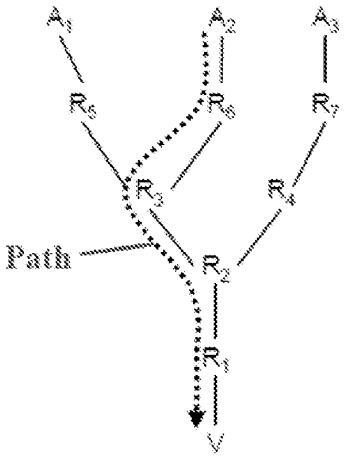


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1 (annotated); EX1003, ¶ 264

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, ¶ 265.

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, ¶ 266.

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 $(R_0..R_j)$ 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, ¶ 267.

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 may be a router, as taught by *Maher*, 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 [4.3.1]. EX1003, ¶ 268.

In the NetScout Case, Patent Owner identified router 22 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 router via packet marks provided by routers leading to said host computer*, as recited in limitation [4.3.1]. EX1014, 26-29 (citing EX1001, 3:62-4:20, 5:40-44, 6:46-51, and Figures 1, 4 and 7).

As described above with respect to limitation [7.2], *Maher* discloses that the 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. 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 [4.3.1]. EX1003, ¶ 270.

[4.3.2] said path comprising all routers in said network via which said packets are routed to said computer; and

Limitation [4.3.2] is identical to limitations [7.1.2] and [10.1.2], and is disclosed or rendered obvious by *Savage*, as described above with respect to limitations [7.1.2] and [10.1.2]. EX1003, ¶ 271.

[4.4] 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.

Limitation [4.4] is substantially identical to limitation [16.4], except that limitation [4.4] recites "means in said router," whereas limitation [16.4] recites "means for said router." Limitation [4.4] is rendered obvious for the same reasons as presented above with respect to limitation [16.4]. EX1003, ¶ 272.

IV. 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")

V. CONCLUSION

For the reasons set forth above, substantial new questions of patentability are raised in connection with claims 1, 4, 7, 10, 13, and 16, by this Request for *Ex Parte* Reexamination, because claims 1, 4, 7, 10, 13, and 16 are rendered obvious in view of the above-listed prior art references. Therefore, Requester asks that this request for reexamination be granted and that claims 1, 4, 7, 10, 13, and 16 be canceled.

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 Request, 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,

May 3, 2021

/Raghav Bajaj/
Raghav Bajaj
Counsel for Third Party Requester
Registration No. 66,630

CERTIFICATE OF TRANSMISSION
I hereby certify that this correspondence is being filed with the U.S. Patent and Trademark Office via EFS Web on May 3, 2021.

/Krista Myrick/
Krista Myrick

VI. CERTIFICATE OF SERVICE

The undersigned certifies that copies of the following,

(1) Request for Ex Parte Reexamination Transmittal Form;

(2) PTO 1449 Modified Form;

(3) Request for Ex Parte Reexamination Under 35 U.S.C. §§ 302-306; and

(4) Exhibits 1001 to 1018, 1020 to 1028, and 1036 to 1045

in their entirety were served 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 3rd day of May 2021.

Dated: May 3, 2021

/Raghav Bajaj/
Raghav Bajaj
Registration No. 66,630

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	PACKET FLOODING DEFENSE SYSTEM
First Named Inventor/Applicant Name:	Donald N. Cohen
Filer:	Raghav Bajaj/Krista Myrick
Attorney Docket Number:	50348.65

Filed as Large Entity

Filing Fees for ex parte reexam

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
EX PARTE REEXAMINATION (1.510(A)) NON-STREAMLINED	1812	1	12600	12600
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**12600**

Electronic Acknowledgement Receipt	
EFS ID:	42620806
Application Number:	90014746
International Application Number:	
Confirmation Number:	9957
Title of Invention:	PACKET FLOODING DEFENSE SYSTEM
First Named Inventor/Applicant Name:	Donald N. Cohen
Customer Number:	27683
Filer:	Raghav Bajaj/Krista Myrick
Filer Authorized By:	Raghav Bajaj
Attorney Docket Number:	50348.65
Receipt Date:	03-MAY-2021
Filing Date:	
Time Stamp:	16:45:59
Application Type:	Reexam (Third Party)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$12600
RAM confirmation Number	E202153G46493221
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Copy of patent for which reexamination is requested	EX1001_US7523497.pdf	1848225 d6a9c95f691ec61f6234323b5268e89e442f1f64	no	17
Warnings:					
Information:					
2	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1002_497_PH.pdf	14281559 379f8bfb37f5adfbddcc8be190d0a760d2a296b3	no	166
Warnings:					
Information:					
3	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1003_Madisetti_Expert_Declaration_497.pdf	5665191 41963f25447a0a002114ec1e5234a9fa748be63d	no	151
Warnings:					
Information:					
4	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1004_Madisetti_CV.pdf	788959 a0cc86ee8c7e6792c2b4ea6d08754bf10ab0ec5d	no	28
Warnings:					
Information:					
5	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1005_Savage_et_al_Practical_Network_Support_for_IP_Traceback.pdf	1461434 08c3b294418d014546bc74fd22b606274bbd2989	no	13
Warnings:					
Information:					
6	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1006_Maher_US7058974.pdf	2122793 cbeed17e6b16d9c68e4f9d66f51536a5f6fd375c	no	15
Warnings:					
Information:					

7	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1007_Schuba_US6725378.pdf	1886872 0add24b078904b3846420ced28c7f070c08edd9b	no	14
Warnings:					
Information:					
8	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1008_Chang_US5367523.pdf	2979495 103789b9a7ca7a0ecce5b95e4fe50d0276f04bb3	no	17
Warnings:					
Information:					
9	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1009_Delman_Declaration.pdf	2185249 cdb532b50de577fd0844c4777cf308418497955f	no	22
Warnings:					
Information:					
10	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	Ex1010_Malan_US20020032871A1.pdf	2262902 59138d496648014ee5f22db56fc110af8b176366	no	16
Warnings:					
Information:					
11	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1011_Stone_US7062782.pdf	2072137 416986721301930ce71d232a50ba440d10c8ed1b	no	19
Warnings:					
Information:					
12	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1012_Cheriton_US7120931.pdf	1770315 e44b04307a726e46bbfbf7db4d12df0564881e88	no	15
Warnings:					
Information:					
13	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1013_Munger_US6502135.pdf	9563143 3c48a4111980ad2f74c4981a64068e6ec4cda899	no	73
Warnings:					
Information:					

14	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1014_PacSec3_Opening_Claim_Construction_Brief.pdf	1760808 489307f08873dc73f9a6e92c70e7acf6d259a567	no	35
Warnings:					
Information:					
15	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1015_Savage_Declaration_FINAL_Reexam.pdf	23890243 e35c92e6ba7a226134515aef2a848cbd3f2553a3	no	210
Warnings:					
Information:					
16	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1016_Savage_CV.pdf	598265 4bea92fabcd2f2b07855d3b95e8acc343e99dde3	no	30
Warnings:					
Information:					
17	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1017_ACM_SIGCOMM_2000_Final_Program.pdf	225540 1c945e95bff3bdda82399e265860b44a962de069	no	3
Warnings:					
Information:					
18	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1018_Internet_Archive_ACM_SIGCOMM_2000_Conference_Program.pdf	451685 05516569561b8fb127a045b9b84a399f262d0ecc	no	4
Warnings:					
Information:					
19	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1020_Savage_et_al_Presentation_Slides_at_ACM_SIGCOMM_2000_Conference.pdf	1089460 0ff72416d004e6da51bd5a6f08b0e3229f79b355	no	27
Warnings:					
Information:					
20	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1021_Excerpt_of_Conference_Proceedings_Book.pdf	19062863 7f8d1ecb9aa32ea7f86821d0890a369e28fac3c2	no	22
Warnings:					
Information:					

21	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1022_About_the_ACM_Organization.pdf	134891 9095c7148ce3ff31252a1cd49aefe5eadf25a61c	no	6
Warnings:					
Information:					
22	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1023_ACM_SIGCOMM_website.pdf	152381 d4dff93e36d62375097b6b4be32cfed7f61d1d18	no	7
Warnings:					
Information:					
23	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1024_SIGCOMM_Conference.pdf	127524 4a8cb63a308e719be24ac1c14ccb14c457265b42	no	3
Warnings:					
Information:					
24	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1025_HallEllis_draft_declaration_Reexam.pdf	17311980 8c61d7254d9011bf2ef2c87a3fcef50d043156d1	no	219
Warnings:					
Information:					
25	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1026_HallEllis_CV.pdf	761570 3ea0a96c681cb7ce794ebc2684a26b9b2903f755	no	51
Warnings:					
Information:					
26	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1027_Cohen_US6789190.pdf	1368079 3626a4200ca7b485c066a97c3a70c02e83518e88	no	15
Warnings:					
Information:					
27	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1028_US_6789190_File_History.pdf	8892247 918b6404f84ba0e6437c3f35fe634962fa693d56	no	129
Warnings:					
Information:					

28	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1036_RFC_2481.pdf	134780 ec2282ee61186dba8aa8274494ca1dda0a68244a	no	26
Warnings:					
Information:					
29	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1037_RFC_2474.pdf	124437 7aa7366011281defce5c40d7c158102c340258a7	no	21
Warnings:					
Information:					
30	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1038_RFC_2475.pdf	154733 f021f7f7ee75529cc249bd40cbb3bd7b45d9b19b	no	37
Warnings:					
Information:					
31	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1039_Stoica_ACM_SIGCOMM_99.pdf	1716383 ee3909a306c536abc05aaaf3f489a7d7c831761d	no	15
Warnings:					
Information:					
32	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1040_Excerpt_of_ACM_SIGCOMM_2000_Conference.pdf	3001445 c6c9bb6941aca008cd911bae164586c5fa2b6747	no	18
Warnings:					
Information:					
33	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1041_Park.pdf	1603662 b8deed39a5e2db4e577766cb43f4d520d7c1a6d9	no	26
Warnings:					
Information:					
34	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1042_Gil_Dissertation.pdf	1350440 6a09e4bea3374e172dc1031ecb3f2352ede2949c	no	52
Warnings:					
Information:					

35	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1043_Eronen.pdf	240255 6eba7b05b78a2775e1d217830102068596ac06dd	no	14
Warnings:					
Information:					
36	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1044_RFC_791.pdf	154875 742328e86d47f5f0749e7b1275d2b71ad7dbb561	no	50
Warnings:					
Information:					
37	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX1045_RFC_1180.pdf	130779 e6e0f2c2e173344f0e794a3734913f18d3b68e6	no	29
Warnings:					
Information:					
38	Transmittal of New Application	50348-65_Transmittal_RequestforExParteReexamination.pdf	247419 cc3f40126f9c9e75f611b905a450a783934d6a47	no	3
Warnings:					
Information:					
39	Information Disclosure Statement (IDS) Form (SB08)	50348-65_PTO1449form_ExParteReexamRequest.pdf	122489 4634748f2faab34ff97d70462e59182a8b2cc919	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
40	Power of Attorney	497_Reexam_POA.pdf	130542 5d8a18c8bfb9bde645c2821978beaa4ab7b00c1c	no	1
Warnings:					
Information:					
41		Reexam_Request_PacSec3_20210503.pdf	7709556 67310e9c4fc307f466c823a6282575d4fa3f6787	yes	158
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	

	Receipt of Orig. Ex Parte Request by Third Party		1	157	
	Reexam Certificate of Service		158	158	
Warnings:					
Information:					
42	Fee Worksheet (SB06)	fee-info.pdf	30162 6832bee265e4b480f8db9ffdcc1fd1de3b4a2801	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	141567767		

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.

Exhibit 1001

U.S. Patent 7,523,497 by Donald N. Cohen ("'497 patent")

Customer No.: 000027683

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651.5000
Fax [214] 200.0853

US007523497B2

(12) **United States Patent**
Cohen

(10) **Patent No.: US 7,523,497 B2**
(45) **Date of Patent: Apr. 21, 2009**

(54) **PACKET FLOODING DEFENSE SYSTEM**

(76) Inventor: **Donald N. Cohen**, 2815 Haddington Dr., Los Angeles, CA (US) 90064

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 719 days.

(21) Appl. No.: **10/841,064**

(22) Filed: **May 7, 2004**

(65) **Prior Publication Data**

US 2004/0230839 A1 Nov. 18, 2004

Related U.S. Application Data

(63) Continuation of application No. 09/715,813, filed on Nov. 16, 2000, now Pat. No. 6,789,190.

(51) **Int. Cl.**
G06F 11/30 (2006.01)

(52) **U.S. Cl.** **726/22**; 726/25; 709/235; 709/238; 709/239; 709/240; 370/229; 370/231; 370/235; 370/237

(58) **Field of Classification Search** 726/22
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,007,052 A * 4/1991 Flammer 370/389
5,353,353 A * 10/1994 Vijeh et al. 380/29
5,367,523 A * 11/1994 Chang et al. 370/235
5,434,860 A * 7/1995 Riddle 370/232
5,455,865 A * 10/1995 Perlman 713/153
5,581,559 A * 12/1996 Crayford et al. 370/392
5,850,515 A * 12/1998 Lo et al. 714/43
6,044,402 A * 3/2000 Jacobson et al. 709/225
6,088,804 A * 7/2000 Hill et al. 726/25
6,412,000 B1 * 6/2002 Riddle et al. 709/224
2002/0032871 A1 * 3/2002 Malan et al. 713/201

OTHER PUBLICATIONS

Yaar, A., et al, "StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense", IEEE Journal on Selected Areas in Communications, vol. 24, No. 10, Oct. 2006, entire document, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01705617.*

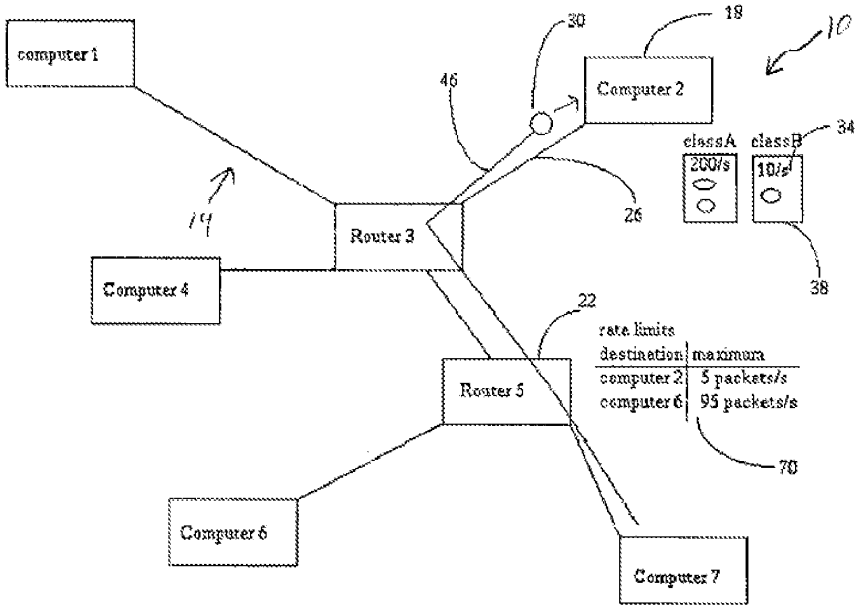
* cited by examiner

Primary Examiner—Kambiz Zand
Assistant Examiner—Ronald Baum
(74) *Attorney, Agent, or Firm*—David A. Belasco; Belasco Jacobs & Townsley, LLP

(57) **ABSTRACT**

The invention prevents "packet flooding", where an attacker uses up all available bandwidth to a victim with useless data. It can also be used to prevent some other related denial of service attacks. The defense is distributed among cooperating sites and routers. The sites identify data they don't want. The routers help sites to determine which routers forward that data. The sites then ask these routers to reduce the rate at which such data is forwarded. Variations of the defense protect against packet flooding attacks on routers and attacks in which an attacker tries to use up some service offered by a site.

18 Claims, 9 Drawing Sheets



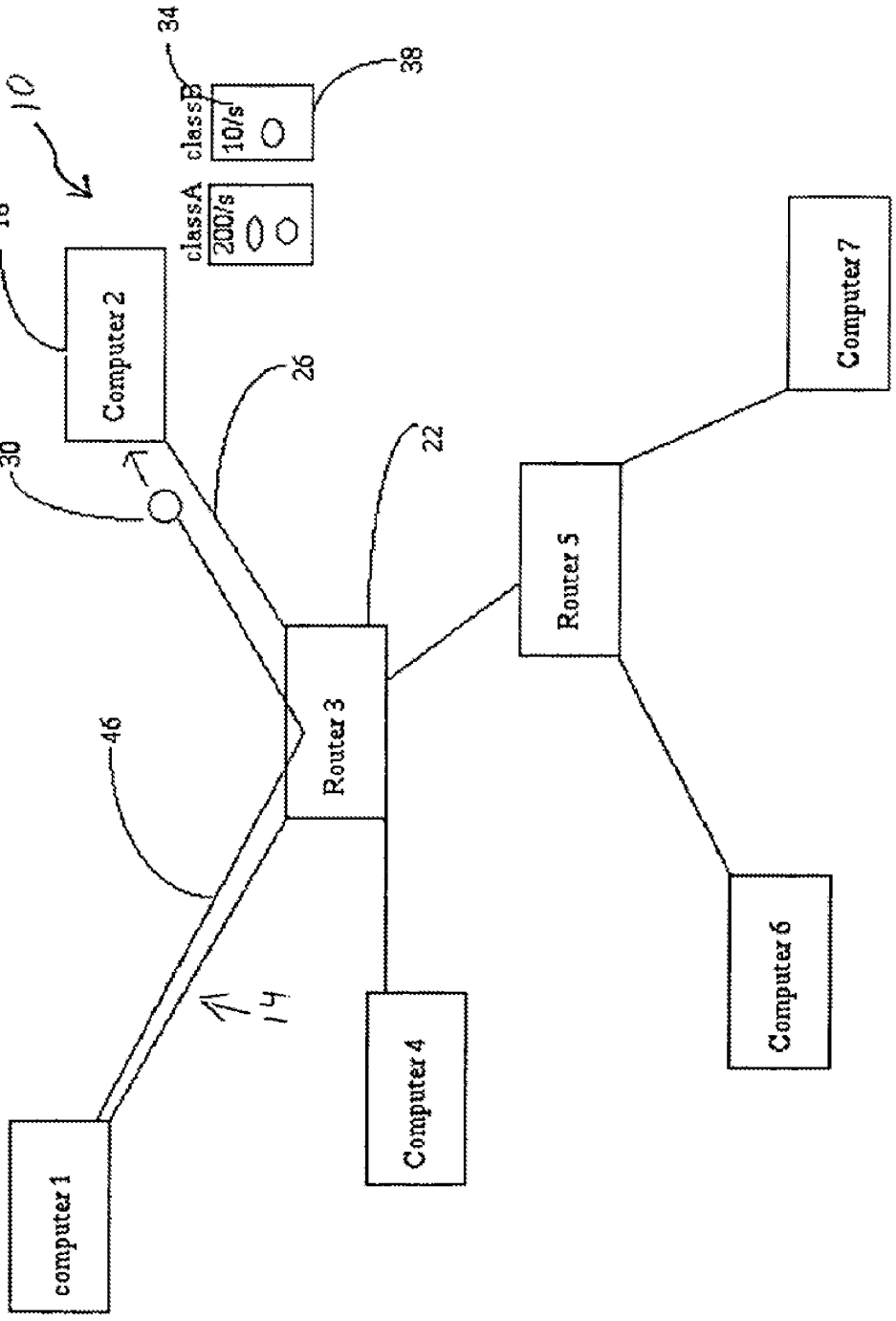

10
34
classB
10/s
38
classA
200/s
18
Computer 2
26
30
22
Router 5
Computer 7
Router 3
46
14
Computer 4
Computer 6
computer 1

Figure 1

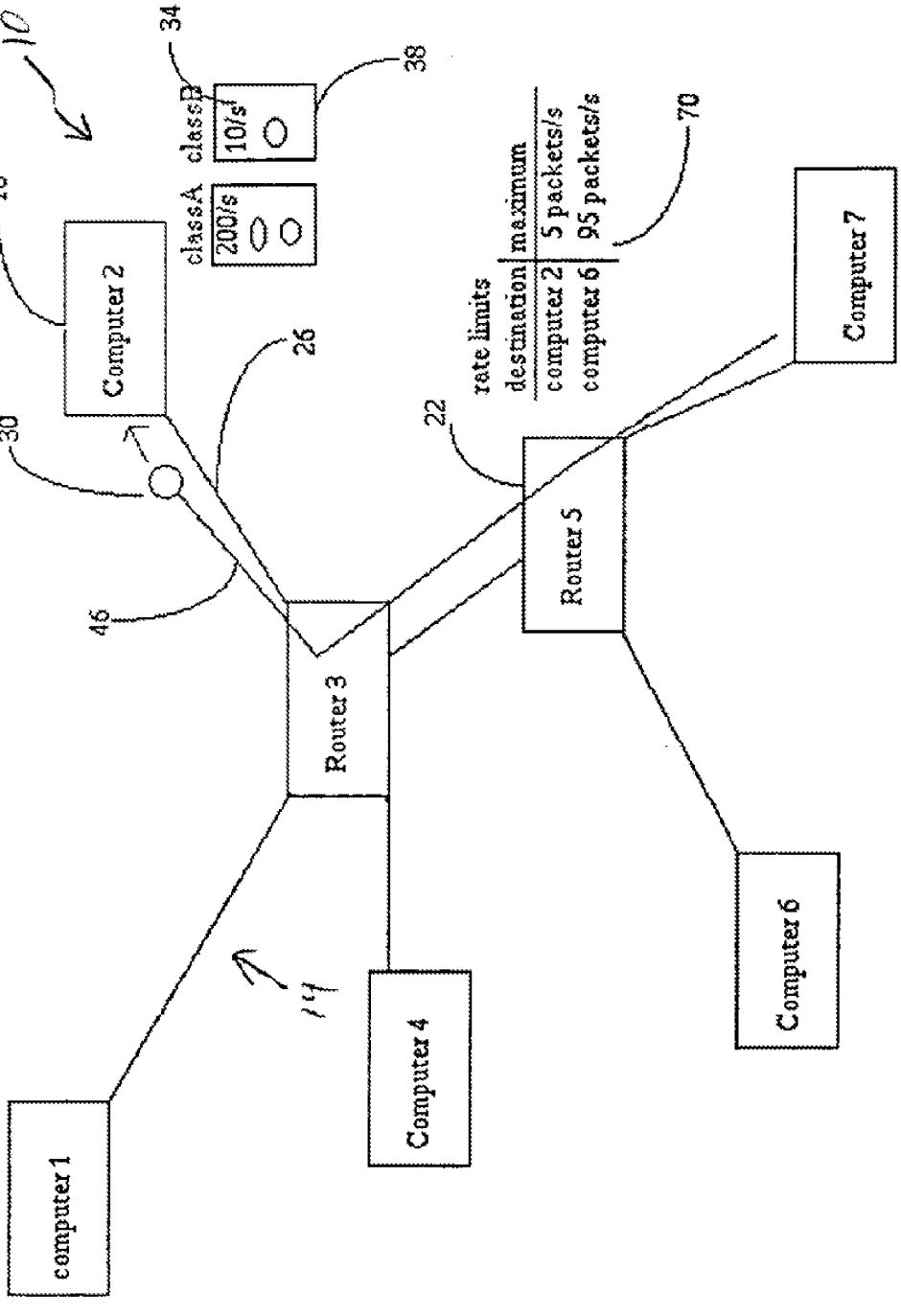

10
34
38
classB
10/s
classA
200/s
18
Computer 2
26
30
46
rate limits
destination | maximum
computer 2 | 5 packets/s
computer 6 | 95 packets/s
70
22
Router 5
Computer 7
Router 3
14
Computer 4
Computer 6
computer 1

Figure 2

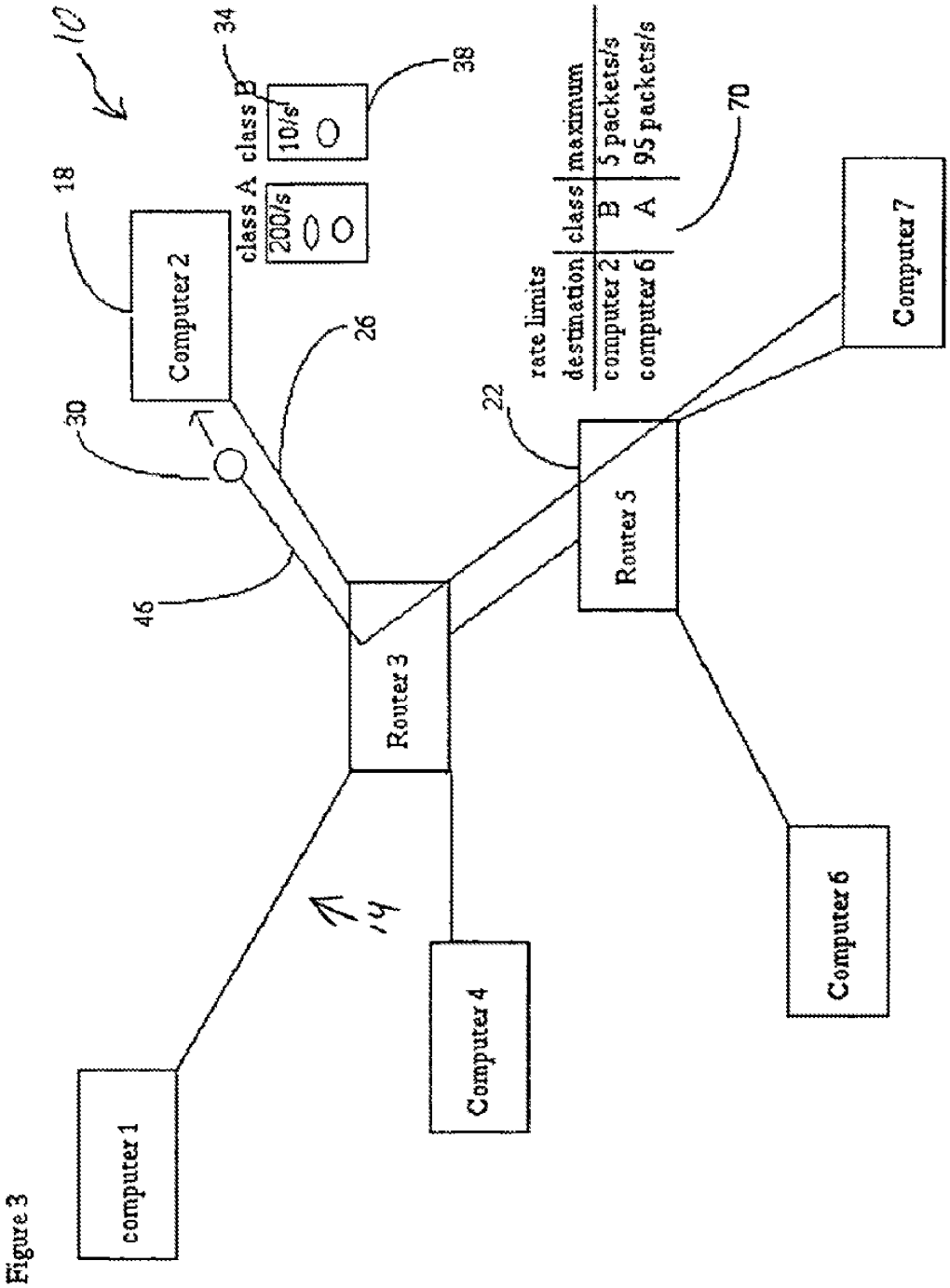

10
34
class B
10/s
38
class A
200/s
18
Computer 2
26
30
46
22
rate limits
destination | class | maximum
computer 2 | B | 5 packets/s
computer 6 | A | 95 packets/s
70
Computer 7
Router 5
Router 3
14
Computer 4
Computer 6
computer 1

Figure 3

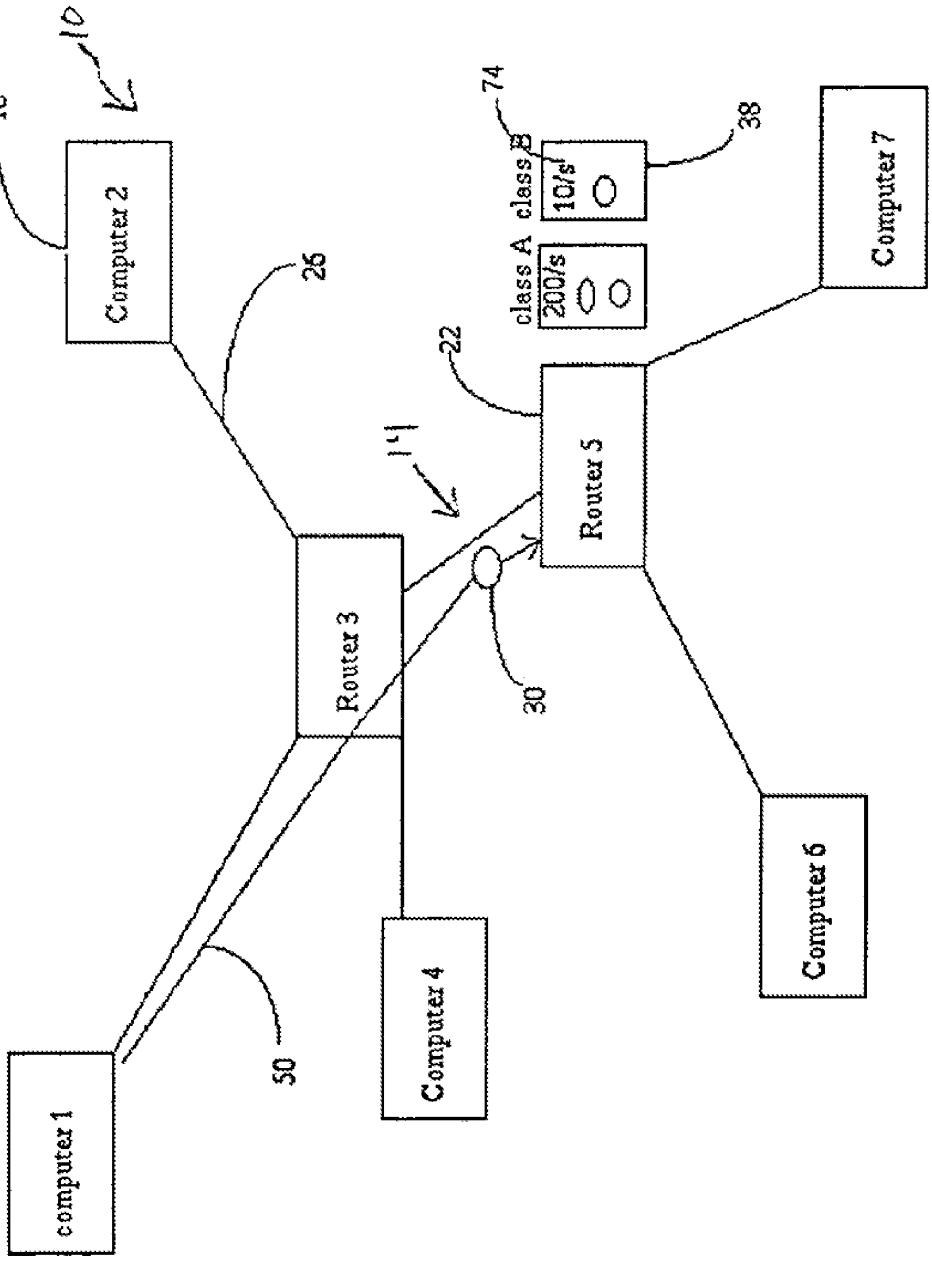

10
18
Computer 2
26
74
class B
10/s
38
class A
200/s
Computer 7
22
Router 5
14
Router 3
30
Computer 6
Computer 4
50
computer 1

Figure 4

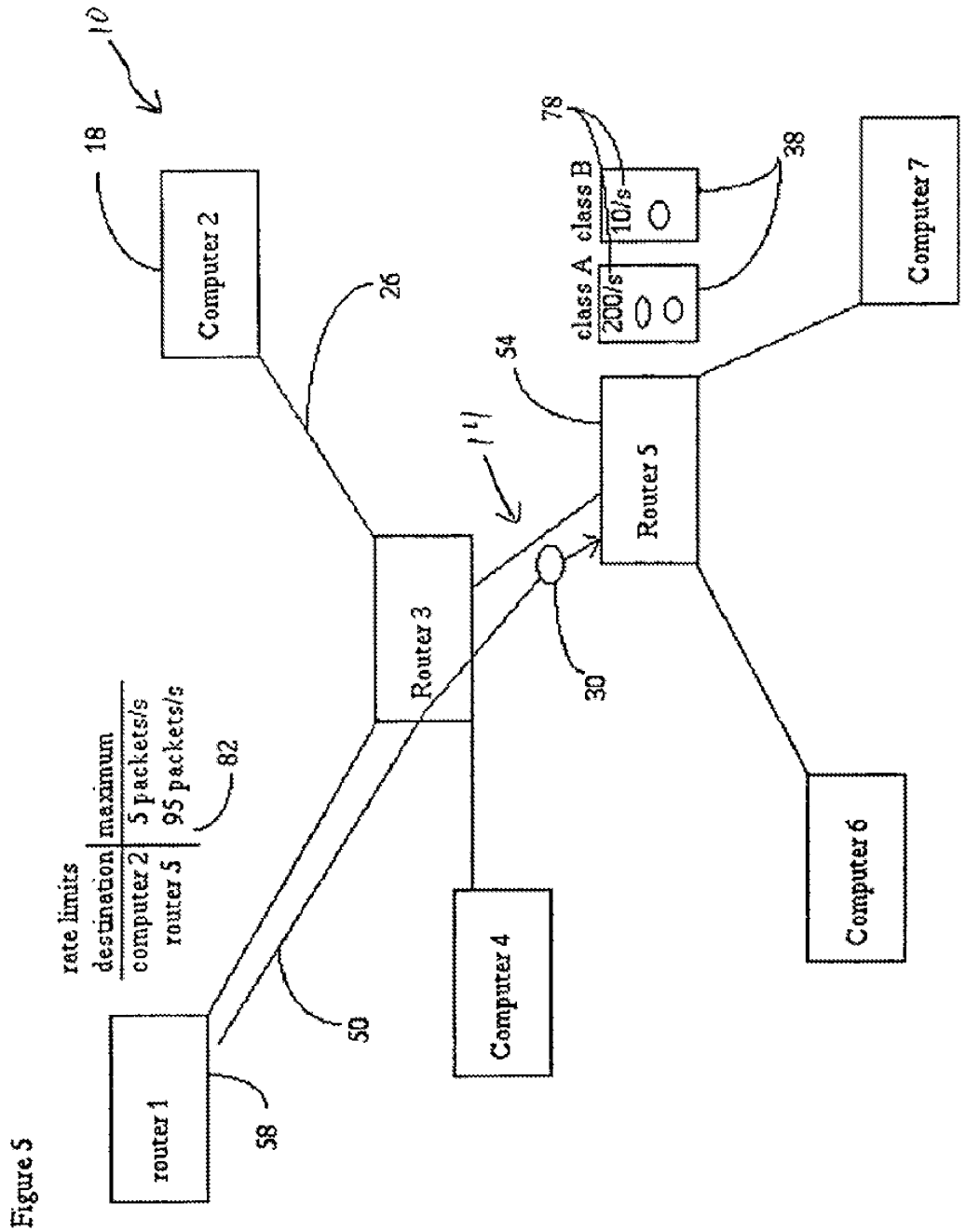

10
18
Computer 2
26
78
class A
200/s
class B
10/s
38
Computer 7
54
14
Router 5
Router 3
30
rate limits
destination
maximum
computer 2
5 packets/s
router 5
95 packets/s
82
Computer 4
Computer 6
50
58
router 1

Figure 5

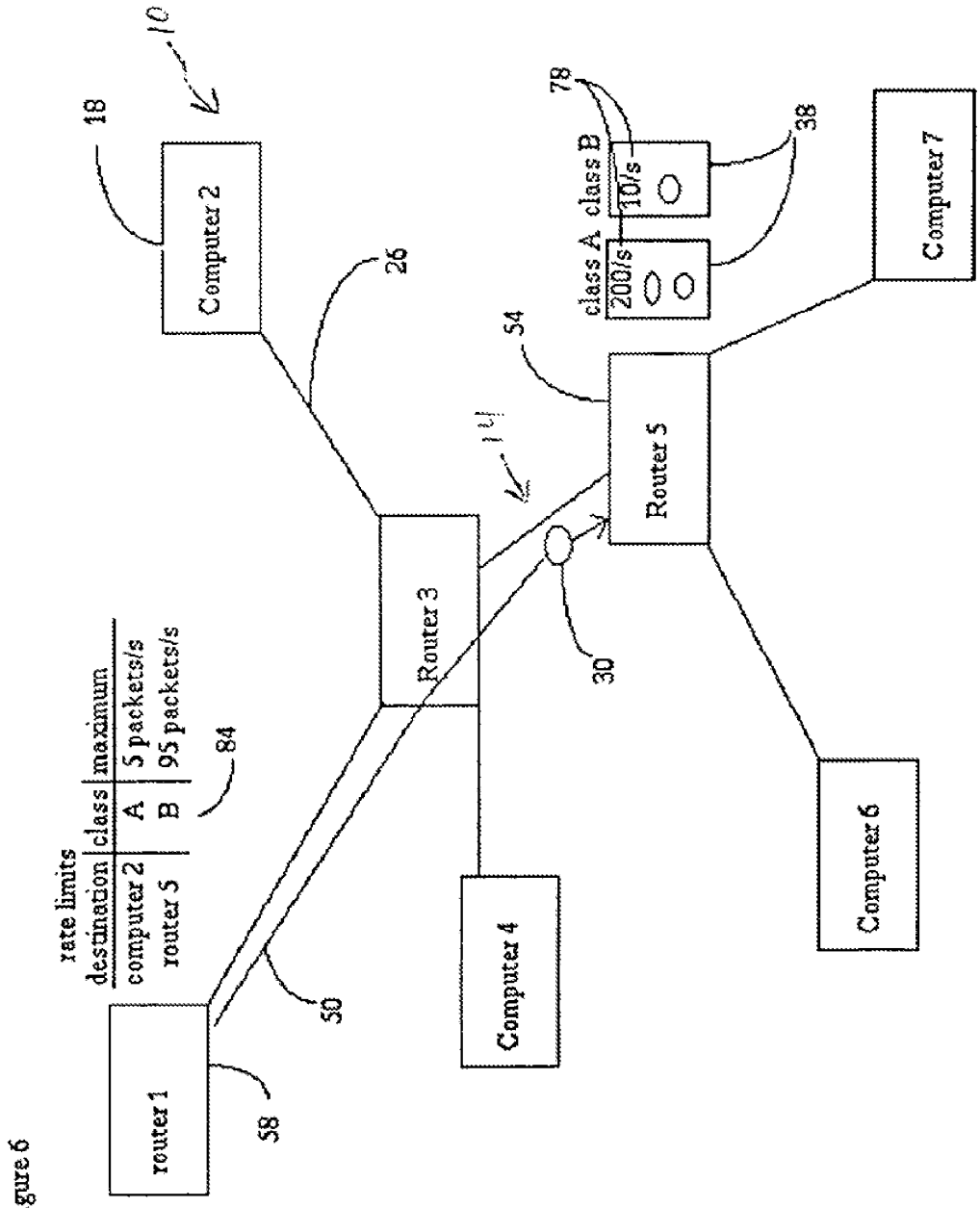

10
18
Computer 2
26
78
class A class B
200/s
10/s
38
Computer 7
54
Router 5
14
Router 3
30
Computer 4
Computer 6
50
58
router 1
rate limits
destination | class | maximum
computer 2 | A | 5 packets/s
router 5 | B | 95 packets/s
84

Figure 6

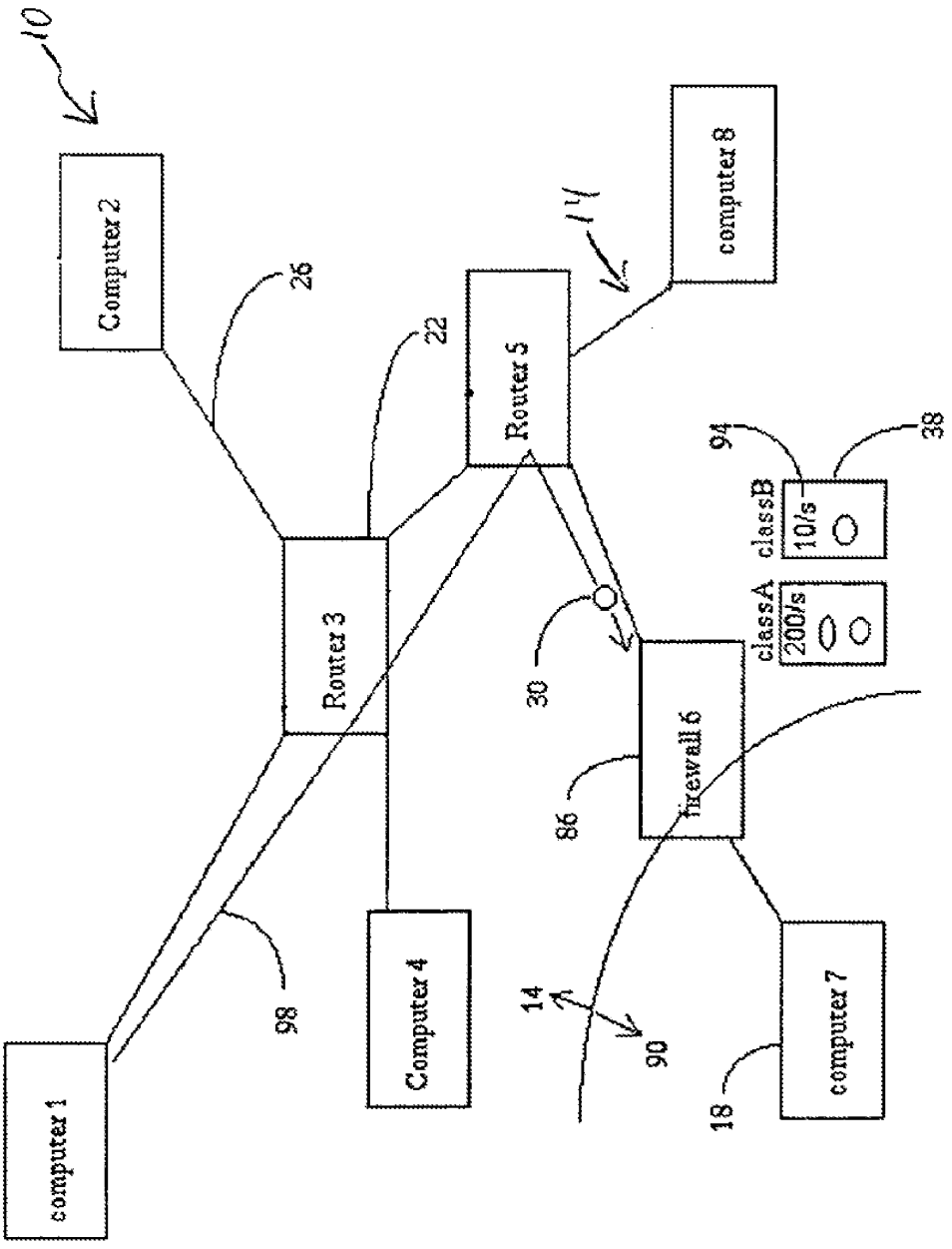

10
Computer 2
26
22
Router 5
14
computer 8
94
38
classB
10/s
classA
200/s
30
Router 3
Firewall 6
86
98
Computer 4
14
90
18
computer 7
computer 1

Figure 7

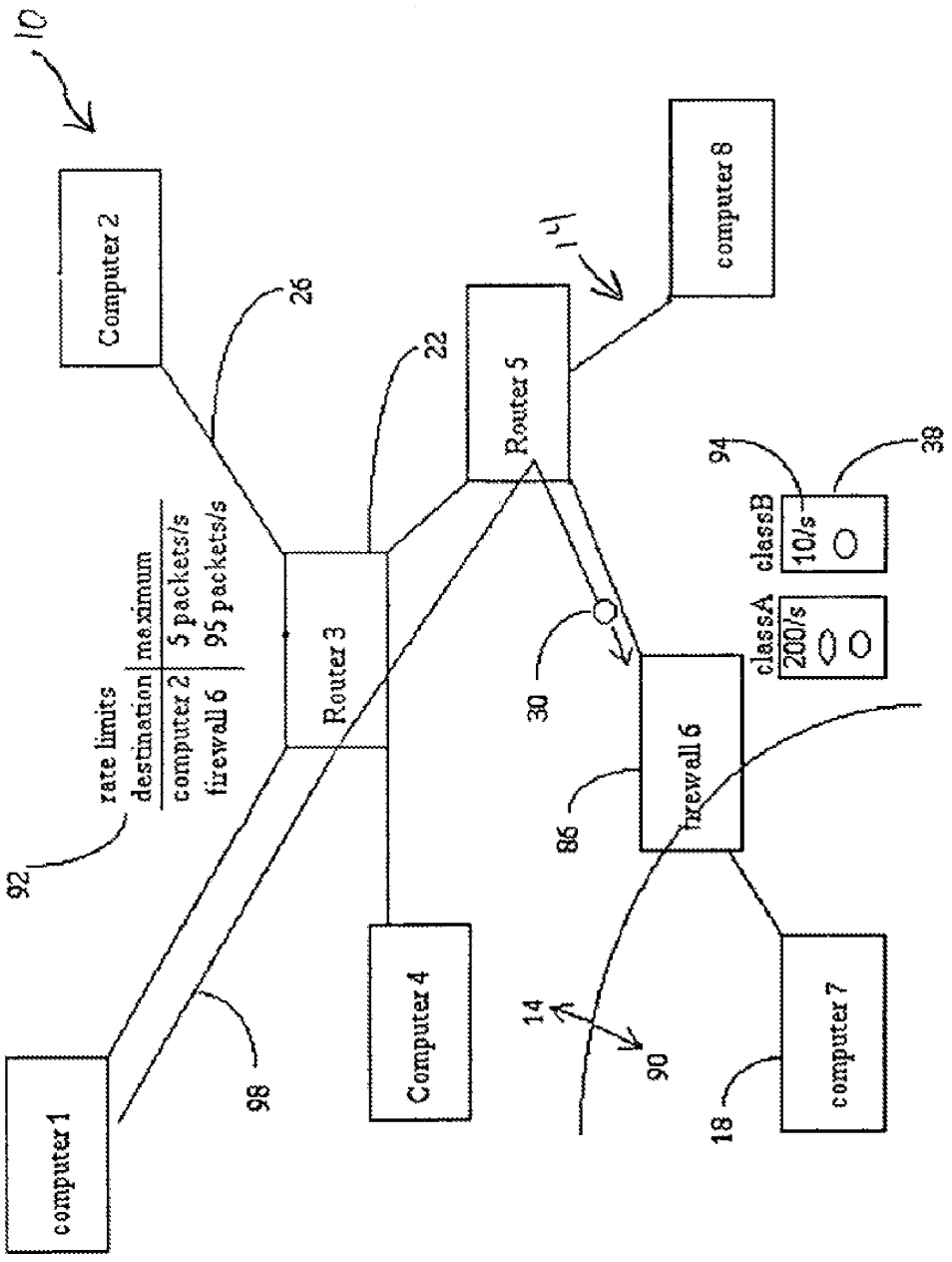

10
Computer 2
26
22
Router 5
14
computer 8
94
38
classB
10/s
classA
200/s
rate limits
destination | maximum
computer 2 | 5 packets/s
firewall 6 | 95 packets/s
92
Router 3
30
86
firewall 6
98
Computer 4
14
90
18
computer 7
computer 1

Figure 8

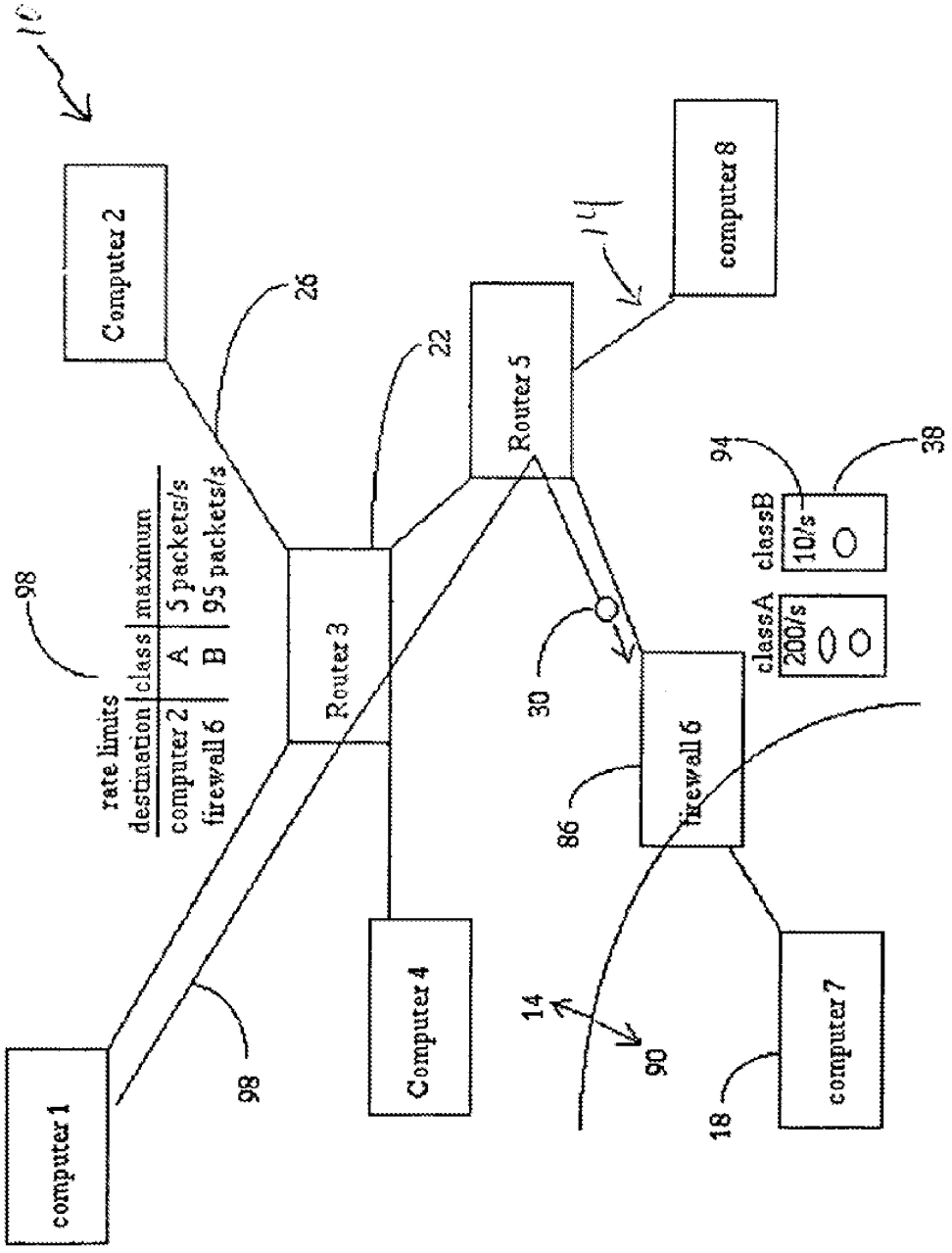

computer 1
Computer 2
Computer 4
computer 7
computer 8
Router 3
Router 5
firewall 6
rate limits
destination | class | maximum
computer 2 | A | 5 packets/s
firewall 6 | B | 95 packets/s
classA
200/s
classB
10/s
98
26
22
14
30
86
90
94
38
18

Figure 9

PACKET FLOODING DEFENSE SYSTEM

CROSS REFERENCE TO RELATED APPLICATIONS

This Application is a continuation of U.S. patent application Ser. No. 09/715,813, filed 11/16/2000 now U.S. Pat. No. 6,789,190.

FIELD OF INVENTION

The invention pertains to network data transmission controls. More particularly, the invention relates to systems for minimizing the effects of packet flooding attacks directed against computers or routers connected to a network.

BACKGROUND OF THE INVENTION

Various types of systems have been developed for handling unwanted network data transmission incorporating a number of different technologies. U.S. Pat. No. 5,581,559 issued to Crayford et al. discloses a method that verifies the integrity of data transmitted over a network by comparing the destination address for a data packet with end station addresses stored on network repeaters. Where the destination address fails to match the stored end station addresses, the data packet will be disrupted.

U.S. Pat. No. 6,044,402 issued to Jacobson et al., describes a system in which the only data packets that are transmitted between source and destination network addresses are those that satisfy the blocking policies stored by the blocking data structure. Thus only, "pre-approved" data can flow through such a control mechanism. U.S. Pat. No. 5,455,865, issued to Perlman discloses a system that relies upon a stored list of acceptable packet identifiers at each node in the network. U.S. Pat. No. 5,353,353 issued to Vijeh et al. describes a system that determines the acceptability of data packets based upon a destination address/source address match and will disrupt any packet not satisfying these criteria. U.S. Pat. No. 5,850,515 issued to Lo et al. discloses a system that uses 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. It also employs a system where an end station can be disabled by a program that determines that a certain number of unauthorized packets have been detected. While other variations exist, the above-described designs for handling unwanted network data transmissions are typical of those encountered in the prior art.

U.S. Pat. No. 5,367,523 to Chang et al. discloses an end-to-end, closed loop flow and congestion control system for packet communications networks which 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. Requests and responses are piggy-backed on data packets and result in changes in the input data rate in a direction to optimize data throughput. GREEN, YELLOW and RED operating modes are defined to increase data input, reduce data input and reduce data input drastically, respectively. Incremental changes in data input are altered non-linearly to change more quickly when further away from the optimum operating point than when closer to the optimum operating point. Chang, et al, is intended for end-to-end congestion control. Congestion control assumes cooperation between sender and receiver in solving the problem. In a packet flooding defense, the sender, who is the attacker, will never cooperate with the receiver, his victim. In Chang, et al, the information used is the source/destination address pairs in the packet. Chang, et al, 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 primary objective of the present invention is to defend against "packet flooding attacks" in which an attacker tries to use up all the bandwidth to the victim by sending data of little or no value (at least to the victim), thereby making more valuable communication with the victim slow or unreliable. A secondary objective is to defend against a related class of attacks in which the attacker tries to use up some other resource by sending more requests of some particular type to the victim than the victim can handle.

One way to view all these attacks is that a resource is being allocated in an unfair way. Well-behaved users request reasonable amounts, while attackers request unreasonable amounts. The most straight-forward allocation mechanism, which might be called "first come first served", ends up allocating almost all of the resource to the attackers. A more "fair" allocation would reduce the impact of an attacker to that of a normal user.

There are two obvious impediments to the "fair service" goal above. One is lack of a reliable way to associate incoming packets with those users among whom bandwidth should be fairly allocated. The other is lack of control over what packets arrive. The solution described here to both of these problems requires help from the routers that forward packets to the victim.

The defense is distributed among cooperating sites and routers. A set of transitively connected cooperating machines is called a "cooperating neighborhood". The quality of the defense is related to the size of the cooperating neighborhood, a larger neighborhood providing better defense. Within the neighborhood it is possible to trace the forwarding path of packets. The association of packets with the "users" is approximated by associating packets with "places" in the cooperating neighborhood from which those packets are forwarded. That is, service will be allocated in a fair (or otherwise reasonable) manner among these places. A "place" in this sense is typically a particular interface from which a packet arrived at a cooperating router.

One such place is likely to be shared by many actual users. An attack will deny service to those users sharing the same place. The advantage of a large number of such places is that each place is shared by fewer users, so an attack will deny service to fewer users. It is advantageous to a user who wants to communicate with a particular machine, to be in the cooperating neighborhood of that machine, since no attacker from another machine can deny him service. Conversely, an attacker wishing to deny service to as many users as possible prefers to share an entry point into the cooperating neighborhood with as many users as possible.

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 may not be the case, however, if routers are unable to forward all the packets they receive. To some extent fair service is limited by network topology, i.e., too many legitimate users trying to share parts of the same path will inevitably suffer relative to users of uncrowded paths. However another potential cause for this problem is a flooding attack against a router. That problem is solved by letting routers allocate their services in a similar way to that described above for sites. That is, they allocate the limited

resource of forwarding bandwidth along any given output in a reasonable way among some set of places in the cooperating neighborhood.

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.

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).

SUMMARY OF THE INVENTION

The present invention addresses many of the deficiencies of prior network defense systems and satisfies all of the objectives described above.

A packet flooding defense system for a network providing the desired features may be constructed from the following components. The network includes a plurality of host computers, routers, communication lines and transmitted data packets. Means are provided 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.

In another variant, a packet flooding defense system for a network including a plurality of host computers, routers, communication lines and transmitted data packets includes means for classifying data packets received at a host computer and means for associating a maximum acceptable processing rate with each class of data packet received at the computer. Means are provided for the computer to determine the rate at which data packets of each class are transmitted from a router to the computer as are means for the router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to the computer. Means are provided for the router to control the rate of transmission of data packets from the router to the computer. Thus, the rate of data packet transmissions received at the computer is kept below the maximum acceptable processing rate for each data packet class by the control of the rate of transmission of data packets from the router, thereby freeing a portion of the network providing data packet transmission to the computer.

In this invention a path (which is not controlled by the attacker) is used to determine the actual direction of the packet flow towards the victim. Bandwidth is allocated based upon path (which is done via packet marks provided by routers leading up to the victim). In other words this invention uses attacker-independent information about the path a packet takes to allocate forwarding bandwidth in a router. The part that makes this invention completely different from Chang, et al. is that the information has to be attacker-independent (i.e., sender-independent) in order to work as a defense.

In yet another variant, the router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to the computer and the router is capable of controlling the rate of transmission of each class of data packets to the computer.

In still another variant, a packet flooding defense system for a network including a plurality of host computers, routers, communication lines and transmitted data packets includes means for classifying data packets received at a router and means for associating a maximum acceptable transmission rate with each class of data packet received at the router. Means are provided for the router to find information for packets it receives regarding the path by which the packets came to the router. Thus, the router can use the information to allocate the transmission rate for each class in a desired way.

In a further variant of the invention, a packet flooding defense system for a network including a plurality of host computers, routers, communication lines and transmitted data packets includes means for classifying data packets received at a first router and means for associating a maximum acceptable transmission rate with each class of data packet received at the first router. Means are provided for the first router to determine the rate at which data packets of each class are transmitted from a second router to the first router as are means for the second router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to the first router. Means are provided for the second router to control the rate of transmission of data packets from the second router to the first router. Thus, the rate of data packet transmissions received at the first router is kept below the maximum acceptable transmission rate for each data packet class by the control of the rate of transmission of data packets from the second router, thereby freeing a portion of the network providing data packet transmission to the first router.

In yet a further variant, the second router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to the first router and the second router is capable of controlling the rate of transmission of each class of data packets to the first router.

In another variant, a packet flooding defense system for a network including a plurality of host computers, routers, communication lines and transmitted data packets includes at least one firewall. The firewall includes hardware and software serving to control packet transmission between the network and a host computer connected to an internal network. Means are provided for classifying data packets received at the firewall as are means for associating a maximum acceptable transmission rate with each class of data packet received at the firewall. Means are provided for the firewall to find information for packets it receives regarding the path by which the packets came to the firewall. Thus, the firewall can use the information to allocate the transmission rate for each class in a desired way.

In still another variant of the invention, a packet flooding defense system for a network including a plurality of host computers, routers, communication lines and transmitted data packets includes at least one firewall. The firewall includes hardware and software serving to control packet transmission between the network and a host computer connected to an internal network and means for classifying data

packets received at the firewall. Means are provided for associating a maximum acceptable transmission rate with each class of data packet received at the firewall as are means for the firewall to determine the rate at which data packets of each class are transmitted from a router to the firewall. Means are provided for the router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to the firewall as are means for the router to control the rate of transmission of date packets from the router to the firewall. Thus, the rate of data packet transmissions received at the firewall is kept below the maximum acceptable transmission rate for each data packet class by the control of the rate of transmission of data packets from the router, thereby freeing a portion of the network providing data packet transmission to the firewall.

In a final variant of the invention, the router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to the firewall and the router is capable of controlling the rate of transmission of each class of data packets to the firewall.

An appreciation of the other aims and objectives of the present invention and an understanding of it may be achieved by referring to the accompanying drawings and the detailed description of a preferred embodiment.

DESCRIPTION OF THE DRAWINGS

FIG. **1** is a schematic view of a first embodiment of the invention illustrating the association of maximum acceptable processing rates for each class of packet received at a computer and a path by which the packets came to the computer;

FIG. **2** is a schematic view of a second embodiment illustrating the association of maximum acceptable processing rates for each class of packet received at a computer, a path by which the packets came to the computer and illustrating information received at a router regarding maximum acceptable transmission rate for data packets being transmitted to the computer;

FIG. **3** is a schematic view of a third embodiment illustrating information received at a router regarding maximum acceptable transmission rate for each class of data packets being transmitted to the computer;

FIG. **4** is a schematic view of a fourth embodiment illustrating association of maximum acceptable transmission rates for each class of packet received at a router and a path by which the packets came to the router;

FIG. **5** is a schematic view of a fifth embodiment illustrating the association of maximum acceptable transmission rates for each class of packet received at a first router, a path by which the packets came to the first router and illustrating information received at a second router regarding maximum acceptable transmission rate for data packets being transmitted to the first router;

FIG. **6** is a schematic view of a sixth embodiment illustrating information received at the second router regarding maximum acceptable transmission rate for each class of data packets being transmitted to the first router;

FIG. **7** is a schematic view of a seventh embodiment of the invention illustrating the association of maximum acceptable transmission rates for each class of packet received at a firewall and a path by which the packets came to the firewall;

FIG. **8** is a schematic view of an eighth embodiment illustrating the association of maximum acceptable transmission rates for each class of packet received at the firewall, a path by which the packets came to the firewall and illustrating information received at a router regarding maximum acceptable transmission rate for data packets being transmitted to the firewall; and

FIG. **9** is a schematic view of a ninth embodiment illustrating information received at a router regarding maximum acceptable transmission rate for each class of data packets being transmitted to the firewall.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** illustrates a packet flooding defense system **10** for a network **14** providing the desired features that may be constructed from the following components. The network **14** includes a plurality of host computers **18**, routers **22**, communication lines **26** and transmitted data packets **30**. Means are provided for classifying data packets **30** received at a host computer **18** as are means for associating a maximum acceptable processing rate **34** with each class **38** of data packet **30** received at the computer **18**. Means are also provided for the computer **18** to find information for packets **30** it receives regarding the path **46** by which the packets **30** came to the computer **18**. Thus, the computer **18** can use the information to allocate the processing rate for each class **38** in a desired way among the places from which packets **30** are transmitted.

In another variant, as illustrated in FIG. **2**, a packet flooding defense system **10** for a network **14** including a plurality of host computers **18**, routers **22**, communication lines **26** and transmitted data packets **30** includes means for classifying data packets **30** received at a host computer **18** and means for associating a maximum acceptable processing rate **34** with each class **38** of data packet **30** received at the computer **18**. Means are provided for the computer **18** to determine the rate at which data packets **30** of each class **38** are transmitted from a router **22** to the computer **18** as are means for the router **22** to receive information regarding maximum acceptable transmission rate **70** for data packets **30** being transmitted to the computer **18**. Means are provided for the router **22** to control the rate of transmission of data packets **30** from the router **22** to the computer **18**. Thus, the rate of data packet transmissions received at the computer **18** is kept below the maximum acceptable processing rate **34** for each data packet class **38** by the control of the rate of transmission of data packets **30** from the router **22**, thereby freeing a portion of the network **14** providing data packet transmission to the computer **18**.

In yet another variant, as illustrated in FIG. **3**, the router **22** is capable of receiving information regarding maximum acceptable transmission rate **70** for each class **38** of data packet **30** being transmitted to the computer **18** and the router **22** is capable of controlling the rate of transmission of each class **38** of data packets **30** to the computer **18**.

In still another variant, as illustrated in FIG. **4**, a packet flooding defense system **10** for a network **14** including a plurality of host computers **18**, routers **22**, communication lines **26** and transmitted data packets **30**, includes means for classifying data packets **30** received at a router **22** and means for associating a maximum acceptable transmission rate **74** with each class **38** of data packet **30** received at the router **22**. Means are provided 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**. Thus, the router **22** can use the information to allocate the transmission rate for each class **38** in a desired way.

In a further variant of the invention, as illustrated in FIG. **5**, a packet flooding defense system **10** for a network **14** including a plurality of host computers **18**, routers **22**, communication lines **26** and transmitted data packets **30** includes means

for classifying data packets **30** received at a first router **54** and means for associating a maximum acceptable transmission rate **78** with each class **38** of data packet **30** received at the first router **54**. Means are provided for the first router **54** to determine the rate at which data packets **30** of each class **38** are transmitted from a second router **58** to the first router **54** as are means for the second router **58** to receive information regarding maximum acceptable transmission rate **82** for data packets **30** being transmitted to the first router **54**. Means are provided for the second router **58** to control the rate of transmission of data packets **30** from the second router **58** to the first router **54**. Thus, the rate of data packet transmissions received at the first router **54** is kept below the maximum acceptable transmission rate **78** for each data packet class **38** by the control of the rate of transmission of data packets **30** from the second router **58**, thereby freeing a portion of the network **14** providing data packet transmission to the first router **54**.

In yet a further variant, as illustrated in FIG. **6**, the second router **58** is capable of receiving information regarding maximum acceptable transmission rate **84** for each class **38** of data packet **30** being transmitted to the first router **54** and the second router **58** is capable of controlling the rate of transmission of each class **38** of data packets **30** to the first router **54**.

In another variant, as illustrated in FIG. **7**, a packet flooding defense system **10** for a network **14** including a plurality of host computers **18**, routers **22**, communication lines **26** and transmitted data packets **30** includes at least one firewall **86**. The firewall **86** includes hardware and software serving to control packet transmission between the network **14** and a host computer **18** connected to an internal network **90**. Means are provided for classifying data packets **30** received at the firewall **86** as are means for associating a maximum acceptable transmission rate **94** with each class **38** of data packet **30** received at the firewall **86**. Means are provided for the firewall **86** to find information for packets **30** it receives regarding the path **98** by which the packets **30** came to the firewall **86**. Thus, the firewall **86** can use the information to allocate the transmission rate for each class **38** in a desired way.

In still another variant of the invention, as illustrated in FIG. **8**, a packet flooding defense system **10** for a network **14** including a plurality of host computers **18**, routers **22**, communication lines **26** and transmitted data packets **30** includes at least one firewall **86**. The firewall **86** includes hardware and software serving to control packet transmission between the network **14** and a host computer **18** connected to an internal network **90** and means for classifying data packets **30** received at the firewall **86**. Means are provided for associating a maximum acceptable transmission rate **94** with each class **38** of data packet **30** received at the firewall **86** as are means for the firewall **86** to determine the rate at which data packets **30** of each class **38** are transmitted from a router **22** to the firewall **86**. Means are provided for the router **22** to receive information regarding maximum acceptable transmission rate **92** for data packets **30** being transmitted to the firewall **86** as are means for the router **22** to control the rate of transmission of data packets **30** from the router **22** to the firewall **86**. Thus, the rate of data packet transmissions received at the firewall **86** is kept below the maximum acceptable transmission rate **94** for each data packet class **38** by the control of the rate of transmission of data packets **30** from the router **22**, thereby freeing a portion of the network **14** providing data packet transmission to the firewall **86**.

In a final variant of the invention, as illustrated in FIG. **9**, the router **22** is capable of receiving information regarding maximum acceptable transmission rate **98** for each class **38** of data packet **30** being transmitted to the firewall **86** and the router **22** is capable of controlling the rate of transmission of each class **38** of data packets **30** to the firewall **86**.

The packet flooding defense system **10** has been described with reference to particular embodiments. Other modifications and enhancements can be made without departing from the spirit and scope of the claims that follow.

The invention claimed is:

1. 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.

2. 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; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer;

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

means for said computer to determine the rate at which data packets of each class are transmitted from a router to said computer;

means for said router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said computer;

means for said router to control the rate of transmission of data packets from said router to said computer; and

means in said computer for keeping the rate of data packet transmissions received at said computer below the maximum acceptable processing rate for each data packet class by said control of the rate of transmission of data packets from said router, and freeing a portion of the network providing data packet transmission to said computer.

3. A packet flooding defense system as described in claim **2**, wherein:

said router receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and said router controls the rate of transmission of each class of data packet to said computer.

4. 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 router into wanted data packets and unwanted data packets;

means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

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

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.

5. 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 first router into wanted data packets and unwanted data packets; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer;

means for associating a maximum acceptable transmission rate with each class of data packet received at said first router;

means for said first router to determine the rate at which data packets of each class are transmitted from a second router to said first router;

means for said second router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said first router;

means for said second router to control the rate of transmission of data packets from said second router to said first router; and

means in said first router for keeping the rate of data packet transmissions received at said first router below the maximum acceptable transmission rate for unwanted data packets by said control of the rate of transmission of data packets from said second router, and freeing a portion of the network providing data packet transmission to said first router.

6. A packet flooding defense system as described in claim 5, wherein:

said second router receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router controls the rate of transmission of each class of data packet to said first router.

7. 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; 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.

8. 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:

classifying data packets received at a host computer into wanted data packets and unwanted data packets; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer;

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

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

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

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

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

9. A method as described in claim 8, in which:

said router receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said 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, 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; said path comprising all routers in said network via which said packets are routed to said computer;

classifying data packets received at 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 unwanted data packets.

11. 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:

classifying data packets received at a first router into wanted data packets and unwanted data packets; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer;

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

determining by said first router of the rate at which data packets of each class are transmitted from a second router to said first router;

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

controlling by said second router of the rate of transmission of data packets from said second router to said first router so that said rate of transmission is below the maximum acceptable transmission rate for each data packet class; and

freeing a portion of the 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 maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router controls the rate of transmission of each class of data packets to said first router.

13. 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 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.

14. 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; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer;

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

means for said computer to determine the rate at which data packets of each class are transmitted from a router to said computer;

means for said router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said computer; and

means for said router to control the rate of transmission of data packets from said router to said computer so that the rate of data packet transmissions received at said computer is kept below the maximum acceptable processing rate for each data packet class; and

freeing a portion of 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 regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router controls the rate of transmission of each class of data packet to said computer.

16. 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 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;

means for classifying data packets received at said router into wanted data packets and unwanted data packets by path;

means for associating a maximum acceptable transmission rate with each class of data packet received at said router; and

means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate.

17. 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 first router into wanted data packets and unwanted data packets; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer;

means for associating a maximum acceptable transmission rate with each class of data packet received at said first router;

means for said first router to determine the rate at which data packets of each class are transmitted from a second router to said first router;

means for said second router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said first router; and

means for said second router to control the rate of transmission of data packets from said second router to said first router so that the rate of data packet transmission received at said first router is kept below the maximum acceptable transmission rate for each data packet class; 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 information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router controls the rate of transmission of each class of data packet to said first router.

* * * * *

Exhibit 1002

Prosecution History of U.S. Patent 7,523,497 ("'497 FH")

Customer No.: 000027683

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651.5000
Fax [214] 200.0853

14230 U.S. PTO 050704

PTO/SB/05 (08-03)
Approved for use through 07/31/2006. OMB 0651-0032
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.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	04-165-B
First Inventor	Donald N. Cohen
Title	PACKET FLOODING DEFENSE..
Express Mail Label No.	EV383355458US

17497 U.S. PTO 10/841064 050704

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450

1. ☑ Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original and a duplicate for fee processing)*
2. ☑ Applicant claims small entity status. See 37 CFR 1.27.
3. ☑ Specification [*Total Pages* 28]
   (preferred arrangement set forth below)
   - Descriptive title of the invention
   - Cross Reference to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the invention
   - Brief Summary of the invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. ☑ Drawing(s) (*35 U.S.C. 113*) [*Total Sheets* 9]
5. Oath or Declaration [*Total Sheets* 2]
   a. ☐ Newly executed (original or copy)
   b. ☑ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional with Box 18 completed)*
      i. ☐ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☐ Application Data Sheet. See 37 CFR 1.76
7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. ☐ Assignment Papers (cover sheet & document(s))
10. ☐ 37 CFR 3.73(b) Statement *(when there is an assignee)* ☑ Power of Attorney
11. ☐ English Translation Document *(if applicable)*
12. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☑ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. ☐ Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. ☑ Other: Credit Card Payment Form

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

☑ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: 09/715,813

Prior application information: *Examiner* Baum, Ronald *Art Unit:* 2135

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

☑ Customer Number: 31718 *OR* ☐ Correspondence address below

Name					
Address					
City		*State*		*Zip Code*	
Country		*Telephone*		*Fax*	

Name (Print/Type)	David A. Belasco	*Registration No. (Attorney/Agent)*	41,609
Signature		*Date*	May 6, 2004

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 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 Patent Application, 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.

14230 U.S. PTO
050704

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
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.

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 772.00

Complete if Known	
Application Number	Not yet Assigned
Filing Date	
First Named Inventor	Donald N. Cohen
Examiner Name	Not yet Assigned
Art Unit	Not yet Assigned
Attorney Docket No.	04-165-B

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☑ Credit card ☐ Money Order ☐ Other ☐ None

☐ Deposit Account:

Deposit Account Number

Deposit Account Name

The Director is authorized to: *(check all that apply)*

☑ Charge fee(s) indicated below ☑ Credit any overpayments

☐ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	385
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 385.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

			Extra Claims		Fee from below		Fee Paid
Total Claims	18	-20** =	0	X	9	=	0
Independent Claims	12	-3** =	9	X	43	=	387
Multiple Dependent					145	=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 387.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 0

SUBMITTED BY

(Complete *(if applicable)*)

Name (Print/Type)	David A. Belasco	Registration No. (Attorney/Agent)	41,609	Telephone	310-743-1188
Signature				Date	May 6, 2004

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.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 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: 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.

Applicant: Donald N. Cohen
Docket: 04-165-B

EXPRESS MAIL MAILING CERTIFICATE

"Express Mail" mailing label No. EV 383355458 US

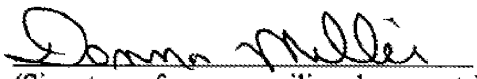
Date of Deposit: May 6, 2004

I hereby certify that the following documents:

1. Utility Patent Application Transmittal
2. Fee Transmittal
3. Credit Card Payment Form in the amount of $772.00
4. Specification Consisting of 28 pages
5. 9 Sheets of Drawings
6. Copy of Declaration
7. Copy of Power of Attorney
8. Return Receipt Postcard

are being deposited in a single envelope with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and such envelope is addressed to Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Donna Miller
(Name of person mailing documents)


(Signature of person mailing documents)

14230 U.S. PTO 050704

PTO/SB/05 (08-03)
Approved for use through 07/31/2006. OMB 0651-0032
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.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	04-165-B
First Inventor	Donald N. Cohen
Title	PACKET FLOODING DEFENSE..
Express Mail Label No.	EV383355458US

17497 U.S. PTO 10/841064 050704

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450

1. ☑ Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original and a duplicate for fee processing)*
2. ☑ Applicant claims small entity status. See 37 CFR 1.27.
3. ☑ Specification [*Total Pages* 28]
   (preferred arrangement set forth below)
   - Descriptive title of the invention
   - Cross Reference to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. ☑ Drawing(s) (*35 U.S.C. 113*) [*Total Sheets* 9]
5. Oath or Declaration [*Total Sheets* 2]
   a. ☐ Newly executed (original or copy)
   b. ☑ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional with Box 18 completed)*
      i. ☐ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☐ Application Data Sheet. See 37 CFR 1.76
7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. ☐ Assignment Papers (cover sheet & document(s))
10. ☐ 37 CFR 3.73(b) Statement *(when there is an assignee)* ☑ Power of Attorney
11. ☐ English Translation Document *(if applicable)*
12. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☑ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. ☐ Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. ☑ Other: Credit Card Payment Form

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

☑ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: 09/715,813

Prior application information: *Examiner* Baum, Ronald *Art Unit:* 2135

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

☑ Customer Number: 31718 *OR* ☐ Correspondence address below

Name					
Address					
City		*State*		*Zip Code*	
Country		*Telephone*		*Fax*	

Name (Print/Type)	David A. Belasco	*Registration No. (Attorney/Agent)*	41,609
Signature		*Date*	May 6, 2004

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 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 Patent Application, 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.

14230 U.S. PTO
050704

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
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.

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 772.00

Complete if Known	
Application Number	Not yet Assigned
Filing Date	
First Named Inventor	Donald N. Cohen
Examiner Name	Not yet Assigned
Art Unit	Not yet Assigned
Attorney Docket No.	04-165-B

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☑ Credit card ☐ Money Order ☐ Other ☐ None

☐ Deposit Account:

Deposit Account Number

Deposit Account Name

The Director is authorized to: *(check all that apply)*

☑ Charge fee(s) indicated below ☑ Credit any overpayments

☐ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	385
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 385.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

			Extra Claims		Fee from below		Fee Paid
Total Claims	18	-20** =	0	X	9	=	0
Independent Claims	12	-3** =	9	X	43	=	387
Multiple Dependent					145	=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 387.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	
				Other fee (specify)	

*Reduced by Basic Filing Fee Paid **SUBTOTAL (3)** ($) 0

SUBMITTED BY				(Complete *(if applicable)*)	
Name (Print/Type)	David A. Belasco	*Registration No. (Attorney/Agent)*	41,609	*Telephone*	310-743-1188
Signature				*Date*	May 6, 2004

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.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 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: 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.

Applicant: Donald N. Cohen
Docket: 04-165-B

EXPRESS MAIL MAILING CERTIFICATE

"Express Mail" mailing label No. EV 383355458 US

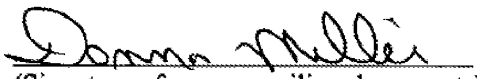
Date of Deposit: May 6, 2004

I hereby certify that the following documents:

1. Utility Patent Application Transmittal
2. Fee Transmittal
3. Credit Card Payment Form in the amount of $772.00
4. Specification Consisting of 28 pages
5. 9 Sheets of Drawings
6. Copy of Declaration
7. Copy of Power of Attorney
8. Return Receipt Postcard

are being deposited in a single envelope with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and such envelope is addressed to Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Donna Miller
(Name of person mailing documents)


(Signature of person mailing documents)

Express Mail Label No. EV 383355458US
Date of Deposit May 6, 2004
Docket No. 04-165-B

Packet Flooding Defense System

Cross Reference to Related Applications

This Application is a continuation of US Patent Application Serial No. 09/715,813, filed 11/16/2000.

Field of Invention

The invention pertains to network data transmission controls. More particularly, the invention relates to systems for minimizing the effects of packet flooding attacks directed against computers or routers connected to a network.

Background of the Invention

Various types of systems have been developed for handling unwanted network data transmission incorporating a number of different technologies. U.S. Patent No. 5,581,559 issued to *Crayford et al.* discloses a method that verifies the integrity of data transmitted over a network by comparing the destination address for a data packet with end station addresses stored on network repeaters. Where the destination address fails to match the stored end station addresses, the data packet will be disrupted.

U.S. Patent No. 6,044,402 issued to *Jacobson et al.*, describes a system in which the only data packets that are transmitted between source and destination network addresses are those that satisfy the blocking policies stored by the blocking data structure. Thus only, "pre-approved" data can flow through such a control mechanism. U.S. Patent No. 5,455,865, issued to *Perlman* discloses a system that relies upon a stored list of acceptable packet identifiers at each node in the network. U.S. Patent No. 5,353,353 issued to *Vijeh et al.* describes a system that determines the acceptability of data packets based upon a destination address/source address match and will disrupt any packet not satisfying these criteria. U.S. Patent No. 5,850,515 issued to *Lo et al.* discloses a system that uses 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. It also employs a system where an end station can be disabled by a program that determines that a certain number of unauthorized packets have been detected. While other variations exist, the above-described designs for handling unwanted network data transmissions are typical of those encountered in the prior art.

US Patent No. 5,367,523 to Chang et al. discloses an end-to-end, closed loop flow and congestion control system for packet communications networks which 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. Requests and responses are piggy-backed on data packets and result in changes in the input data rate in a direction to

optimize data throughput. GREEN, YELLOW and RED operating modes are defined to increase data input, reduce data input and reduce data input drastically, respectively. Incremental changes in data input are altered non-linearly to change more quickly when further away from the optimum operating point than when closer to the optimum operating point. Chang, et al, is intended for end-to-end congestion control. Congestion control assumes cooperation between sender and receiver in solving the problem. In a packet flooding defense, the sender, who is the attacker, will never cooperate with the receiver, his victim. In Chang, et al, the information used is the source/destination address pairs in the packet. Chang, et al, 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 primary objective of the present invention is to defend against "packet flooding attacks" in which an attacker tries to use up all the bandwidth to the victim by sending data of little or no value (at least to the victim), thereby making more valuable communication with the victim slow or unreliable. A secondary objective is to defend against a related class of attacks in which the attacker tries to use up some other resource by sending more requests of some particular type to the victim than the victim can handle.

One way to view all these attacks is that a resource is being allocated in an unfair way. Well-behaved users request reasonable amounts, while attackers request unreasonable amounts. The most straight-forward allocation mechanism, which might be called "first come

first served", ends up allocating almost all of the resource to the attackers. A more "fair" allocation would reduce the impact of an attacker to that of a normal user.

There are two obvious impediments to the "fair service" goal above. One is lack of a reliable way to associate incoming packets with those users among whom bandwidth should be fairly allocated. The other is lack of control over what packets arrive. The solution described here to both of these problems requires help from the routers that forward packets to the victim.

The defense is distributed among cooperating sites and routers. A set of transitively connected cooperating machines is called a "cooperating neighborhood". The quality of the defense is related to the size of the cooperating neighborhood, a larger neighborhood providing better defense. Within the neighborhood it is possible to trace the forwarding path of packets. The association of packets with the "users" is approximated by associating packets with "places" in the cooperating neighborhood from which those packets are forwarded. That is, service will be allocated in a fair (or otherwise reasonable) manner among these places. A "place" in this sense is typically a particular interface from which a packet arrived at a cooperating router.

One such place is likely to be shared by many actual users. An attack will deny service to those users sharing the same place. The advantage of a large number of such places is that each place is shared by fewer users, so an attack will deny service to fewer users. It is advantageous to a user who wants to communicate with a particular machine, to be in the

cooperating neighborhood of that machine, since no attacker from another machine can deny him service. Conversely, an attacker wishing to deny service to as many users as possible prefers to share an entry point into the cooperating neighborhood with as many users as possible.

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 may not be the case, however, if routers are unable to forward all the packets they receive. To some extent fair service is limited by network topology, i.e., too many legitimate users trying to share parts of the same path will inevitably suffer relative to users of uncrowded paths. However another potential cause for this problem is a flooding attack against a router. That problem is solved by letting routers allocate their services in a similar way to that described above for sites. That is, they allocate the limited resource of forwarding bandwidth along any given output in a reasonable way among some set of places in the cooperating neighborhood.

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.

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).

Summary of the Invention

The present invention addresses many of the deficiencies of prior network defense systems and satisfies all of the objectives described above.

A packet flooding defense system for a network providing the desired features may be constructed from the following components. The network includes a plurality of host computers, routers, communication lines and transmitted data packets. Means are provided 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.

In another variant, a packet flooding defense system for a network including a plurality of host computers, routers, communication lines and transmitted data packets includes means for classifying data packets received at a host computer and means for associating a maximum acceptable processing rate with each class of data packet received at the computer. Means are provided for the computer to determine the rate at which data packets of each class are transmitted from a router to the computer as are means for the router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to the computer. Means are provided for the router to control the rate of transmission of data packets from the router to the computer. Thus, the rate of data packet transmissions received at the computer is kept below the maximum acceptable processing rate for each data packet class by the control of the rate of transmission of data packets from the router, thereby freeing a portion of the network providing data packet transmission to the computer.

In this invention a path (which is not controlled by the attacker) is used to determine the actual direction of the packet flow towards the victim. Bandwidth is allocated based upon path (which is done via packet marks provided by routers leading up to the victim). In other words this invention uses attacker-independent information about the path a packet takes to allocate forwarding bandwidth in a router. The part that makes this invention completely different from Chang, et al, is that the information has to be attacker-independent (i.e., sender-independent) in order to work as a defense.

In yet another variant, the router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to the computer and the router is capable of controlling the rate of transmission of each class of data packets to the computer.

In still another variant, a packet flooding defense system for a network including a plurality of host computers, routers, communication lines and transmitted data packets includes means for classifying data packets received at a router and means for associating a maximum acceptable transmission rate with each class of data packet received at the router. Means are provided for the router to find information for packets it receives regarding the path by which the packets came to the router. Thus, the router can use the information to allocate the transmission rate for each class in a desired way.

In a further variant of the invention, a packet flooding defense system for a network including a plurality of host computers, routers, communication lines and transmitted data packets includes means for classifying data packets received at a first router and means for associating a maximum acceptable transmission rate with each class of data packet received at the first router. Means are provided for the first router to determine the rate at which data packets of each class are transmitted from a second router to the first router as are means for the second router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to the first router. Means are provided for the second router to control the rate of transmission of data packets from the second router to the first router. Thus, the rate of data packet transmissions received at the first router is kept below the

maximum acceptable transmission rate for each data packet class by the control of the rate of transmission of data packets from the second router, thereby freeing a portion of the network providing data packet transmission to the first router.

In yet a further variant, the second router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to the first router and the second router is capable of controlling the rate of transmission of each class of data packets to the first router.

In another variant, a packet flooding defense system for a network including a plurality of host computers, routers, communication lines and transmitted data packets includes at least one firewall. The firewall includes hardware and software serving to control packet transmission between the network and a host computer connected to an internal network. Means are provided for classifying data packets received at the firewall as are means for associating a maximum acceptable transmission rate with each class of data packet received at the firewall. Means are provided for the firewall to find information for packets it receives regarding the path by which the packets came to the firewall. Thus, the firewall can use the information to allocate the transmission rate for each class in a desired way.

In still another variant of the invention, a packet flooding defense system for a network including a plurality of host computers, routers, communication lines and transmitted data packets includes at least one firewall. The firewall includes hardware and software serving to control packet transmission between the network and a host computer connected to an internal

network and means for classifying data packets received at the firewall. Means are provided for associating a maximum acceptable transmission rate with each class of data packet received at the firewall as are means for the firewall to determine the rate at which data packets of each class are transmitted from a router to the firewall. Means are provided for the router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to the firewall as are means for the router to control the rate of transmission of data packets from the router to the firewall. Thus, the rate of data packet transmissions received at the firewall is kept below the maximum acceptable transmission rate for each data packet class by the control of the rate of transmission of data packets from the router, thereby freeing a portion of the network providing data packet transmission to the firewall.

In a final variant of the invention, the router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to the firewall and the router is capable of controlling the rate of transmission of each class of data packets to the firewall.

An appreciation of the other aims and objectives of the present invention and an understanding of it may be achieved by referring to the accompanying drawings and the detailed description of a preferred embodiment.

Description of the Drawings

Figure 1 is a schematic view of a first embodiment of the invention illustrating the association of maximum acceptable processing rates for each class of packet received at a computer and a path by which the packets came to the computer;

Figure 2 is a schematic view of a second embodiment illustrating the association of maximum acceptable processing rates for each class of packet received at a computer, a path by which the packets came to the computer and illustrating information received at a router regarding maximum acceptable transmission rate for data packets being transmitted to the computer;

Figure 3 is a schematic view of a third embodiment illustrating information received at a router regarding maximum acceptable transmission rate for each class of data packets being transmitted to the computer;

Figure 4 is a schematic view of a fourth embodiment illustrating association of maximum acceptable transmission rates for each class of packet received at a router and a path by which the packets came to the router;

Figure 5 is a schematic view of a fifth embodiment illustrating the association of maximum acceptable transmission rates for each class of packet received at a first router, a path by which the packets came to the first router and illustrating information received at a second router regarding maximum acceptable transmission rate for data packets being transmitted to the first router;

Figure 6 is a schematic view of a sixth embodiment illustrating information received at the second router regarding maximum acceptable transmission rate for each class of data packets being transmitted to the first router;

Figure 7 is a schematic view of a seventh embodiment of the invention illustrating the association of maximum acceptable transmission rates for each class of packet received at a firewall and a path by which the packets came to the firewall;

Figure 8 is a schematic view of an eighth embodiment illustrating the association of maximum acceptable transmission rates for each class of packet received at the firewall, a path by which the packets came to the firewall and illustrating information received at a router regarding maximum acceptable transmission rate for data packets being transmitted to the firewall; and

Figure 9 is a schematic view of a ninth embodiment illustrating information received at a router regarding maximum acceptable transmission rate for each class of data packets being transmitted to the firewall.

Detailed Description of the Preferred Embodiment

Figure 1 illustrates a packet flooding defense system **10** for a network **14** providing the desired features that may be constructed from the following components. The network **14** includes a plurality of host computers **18**, routers **22**, communication lines **26** and transmitted

data packets **30**. Means are provided for classifying data packets **30** received at a host computer **18** as are means for associating a maximum acceptable processing rate **34** with each class **38** of data packet **30** received at the computer **18**. Means are also provided for the computer **18** to find information for packets **30** it receives regarding the path **46** by which the packets **30** came to the computer **18**. Thus, the computer **18** can use the information to allocate the processing rate for each class **38** in a desired way among the places from which packets **30** are transmitted.

In another variant, as illustrated in **Figure 2**, a packet flooding defense system **10** for a network **14** including a plurality of host computers **18**, routers **22**, communication lines **26** and transmitted data packets **30** includes means for classifying data packets **30** received at a host computer **18** and means for associating a maximum acceptable processing rate **34** with each class **38** of data packet **30** received at the computer **18**. Means are provided for the computer **18** to determine the rate at which data packets **30** of each class **38** are transmitted from a router **22** to the computer **18** as are means for the router **22** to receive information regarding maximum acceptable transmission rate **70** for data packets **30** being transmitted to the computer **18**. Means are provided for the router **22** to control the rate of transmission of data packets **30** from the router **22** to the computer **18**. Thus, the rate of data packet transmissions received at the computer **18** is kept below the maximum acceptable processing rate **34** for each data packet class **38** by the control of the rate of transmission of data packets **30** from the router **22**, thereby freeing a portion of the network **14** providing data packet transmission to the computer **18**.

In yet another variant, as illustrated in **Figure 3**, the router **22** is capable of receiving information regarding maximum acceptable transmission rate **70** for each class **38** of data packet **30** being transmitted to the computer **18** and the router **22** is capable of controlling the rate of transmission of each class **38** of data packets **30** to the computer **18**.

In still another variant, as illustrated in **Figure 4**, a packet flooding defense system **10** for a network **14** including a plurality of host computers **18**, routers **22**, communication lines **26** and transmitted data packets **30**, includes means for classifying data packets **30** received at a router **22** and means for associating a maximum acceptable transmission rate **74** with each class **38** of data packet **30** received at the router **22**. Means are provided 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**. Thus, the router **22** can use the information to allocate the transmission rate for each class **38** in a desired way.

In a further variant of the invention, as illustrated in **Figure 5**, a packet flooding defense system **10** for a network **14** including a plurality of host computers **18**, routers **22**, communication lines **26** and transmitted data packets **30** includes means for classifying data packets **30** received at a first router **54** and means for associating a maximum acceptable transmission rate **78** with each class **38** of data packet **30** received at the first router **54**. Means are provided for the first router **54** to determine the rate at which data packets **30** of each class **38** are transmitted from a second router **58** to the first router **54** as are means for the second router **58** to receive information regarding maximum acceptable transmission rate **82** for data packets **30** being transmitted to the first router **54**. Means are provided for the second router

58 to control the rate of transmission of data packets 30 from the second router 58 to the first router 54. Thus, the rate of data packet transmissions received at the first router 54 is kept below the maximum acceptable transmission rate 78 for each data packet class 38 by the control of the rate of transmission of data packets 30 from the second router 58 , thereby freeing a portion of the network 14 providing data packet transmission to the first router 54.

In yet a further variant, as illustrated in **Figure 6**, the second router 58 is capable of receiving information regarding maximum acceptable transmission rate 84 for each class 38 of data packet 30 being transmitted to the first router 54 and the second router 58 is capable of controlling the rate of transmission of each class 38 of data packets 30 to the first router 54.

In another variant, as illustrated in **Figure 7**, a packet flooding defense system 10 for a network 14 including a plurality of host computers 18, routers 22, communication lines 26 and transmitted data packets 30 includes at least one firewall 86. The firewall 86 includes hardware and software serving to control packet transmission between the network 14 and a host computer 18 connected to an internal network 90. Means are provided for classifying data packets 30 received at the firewall 86 as are means for associating a maximum acceptable transmission rate 94 with each class 38 of data packet 30 received at the firewall 86. Means are provided for the firewall 86 to find information for packets 30 it receives regarding the path 98 by which the packets 30 came to the firewall 86. Thus, the firewall 86 can use the information to allocate the transmission rate for each class 38 in a desired way.

In still another variant of the invention, as illustrated in **Figure 8**, a packet flooding defense system **10** for a network **14** including a plurality of host computers **18**, routers **22**, communication lines **26** and transmitted data packets **30** includes at least one firewall **86**. The firewall **86** includes hardware and software serving to control packet transmission between the network **14** and a host computer **18** connected to an internal network **90** and means for classifying data packets **30** received at the firewall **86**. Means are provided for associating a maximum acceptable transmission rate **94** with each class **38** of data packet **30** received at the firewall **86** as are means for the firewall **86** to determine the rate at which data packets **30** of each class **38** are transmitted from a router **22** to the firewall **86**. Means are provided for the router **22** to receive information regarding maximum acceptable transmission rate **92** for data packets **30** being transmitted to the firewall **86** as are means for the router **22** to control the rate of transmission of data packets **30** from the router **22** to the firewall **86**. Thus, the rate of data packet transmissions received at the firewall **86** is kept below the maximum acceptable transmission rate **94** for each data packet class **38** by the control of the rate of transmission of data packets **30** from the router **22**, thereby freeing a portion of the network **14** providing data packet transmission to the firewall **86**.

In a final variant of the invention, as illustrated in **Figure 9**, the router **22** is capable of receiving information regarding maximum acceptable transmission rate **98** for each class **38** of data packet **30** being transmitted to the firewall **86** and the router **22** is capable of controlling the rate of transmission of each class **38** of data packets **30** to the firewall **86**.

The packet flooding defense system **10** has been described with reference to particular embodiments. Other modifications and enhancements can be made without departing from the spirit and scope of the claims that follow.

CLAIMS

1. 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;

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; and

whereby, said computer can use said information to allocate the processing rate available for packets of each class in a desired way.

2. 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;

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

means for said computer to determine the rate at which data packets of each class are transmitted from a router to said computer;

means for said router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said computer;

means for said router to control the rate of transmission of data packets from said router to said computer; and

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

3. A packet flooding defense system as described in Claim 2, wherein:

said router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router is capable of control

ling the rate of transmission of each class of data packets to said computer.

4. 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 router;

means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

means for said router to find information for packets it receives regarding the path by which said packets came to said router; and

whereby, said router can use said information to allocate the transmission rate for each class in a desired way.

5. 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 first router;

means for associating a maximum acceptable transmission rate with each class of data packet received at said first router;

means for said first router to determine the rate at which data packets of each class are transmitted from a second router to said first router;

means for said second router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said first router;

means for said second router to control the rate of transmission of data packets from said second router to said first router; and

whereby, the rate of data packet transmissions received at said first router is kept below the maximum acceptable transmission rate for each data packet class by said control of the rate of transmission of data packets from said second router, thereby freeing a portion of the network providing data packet transmission to said first router.

6. A packet flooding defense system as described in Claim 5, wherein:

said second router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router is capable of controlling the rate of transmission of each class of data packets to said first router.

7. 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;

classifying data packets received at a host computer 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 packets of each class in a desired way.

8. 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:

classifying data packets received at a host computer;

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

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

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

controlling the rate of transmission of data packets from said router to said computer by said router so that data packet transmissions received at said computer are kept below the maximum acceptable processing rate for each data packet class;

thereby freeing a portion of the network providing data packet transmission to said computer.

9. A method as described in Claim 8, in which:

said router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router is capable of controlling the rate of transmission of each class of data packets to said computer.

10. 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;

classifying data packets received at a router 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 in a desired way.

11. 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:

classifying data packets received at a first router;

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

determining by said first router of the rate at which data packets of each class are transmitted from a second router to said first router;

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

controlling by said second router of the rate of transmission of data packets from said second router to said first router so that said rate of transmission is below the maximum acceptable transmission rate for each data packet class;

thereby freeing a portion of the network providing data packet transmission to said first router.

12. A method as described in Claim 11, in which:

said second router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router is capable of controlling the rate of transmission of each class of data packets to said first router.

13. 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 determining a path by which data packets arrive at a host computer;

means for classifying data packets received at said host computer 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 each class of data packet.

14. 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;

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

means for said computer to determine the rate at which data packets of each class are transmitted from a router to said computer;

means for said router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said computer; and

means for said router to control the rate of transmission of data packets from said router to said computer so that the rate of data packet transmissions received at said computer is kept below the maximum acceptable processing rate for each data packet class;

thereby freeing a portion of the network providing data packet transmission to said computer.

15. A packet flooding defense system as described in Claim 14, in which:

said router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router is capable of controlling the rate of transmission of each class of data packet to said computer.

16. 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 a router to determine a path by which said packets came to said router;

means for classifying data packets received at a router by path;

means for associating a maximum acceptable transmission rate with each class of data packet received at said router; and

means for said router to allocate the transmission rate for each class in a desired way.

17. 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 first router;

means for associating a maximum acceptable transmission rate with each class of data packet received at said first router;

means for said first router to determine the rate at which data packets of each class are transmitted from a second router to said first router;

means for said second router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said first router; and

means for said second router to control the rate of transmission of data packets from said second router to said first router so that the rate of data packet transmission received at said first router is kept below the maximum acceptable transmission rate for each data packet class;

thereby 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 is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router is capable of controlling the rate of transmission of each class of data packets to said first router.

ABSTRACT

The invention prevents "packet flooding", where an attacker uses up all available bandwidth to a victim with useless data. It can also be used to prevent some other related denial of service attacks. The defense is distributed among cooperating sites and routers. The sites identify data they don't want. The routers help sites to determine which routers forward that data. The sites then ask these routers to reduce the rate at which such data is forwarded. Variations of the defense protect against packet flooding attacks on routers and attacks in which an attacker tries to use up some service offered by a site.

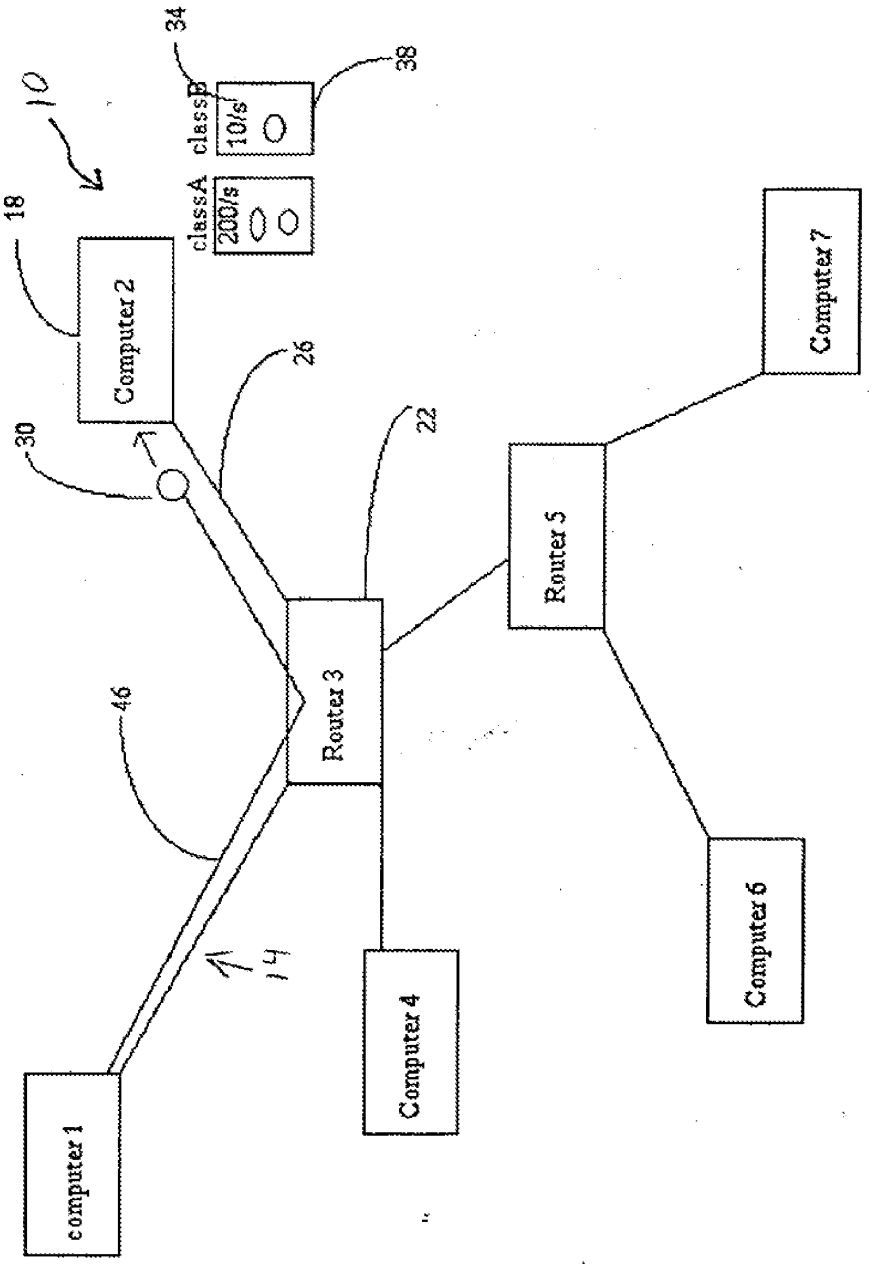

10
34
38
classB
10/s
classA
200/s
18
Computer 2
26
30
22
Router 5
Computer 7
Router 3
46
14
Computer 4
Computer 6
computer 1

Figure 1

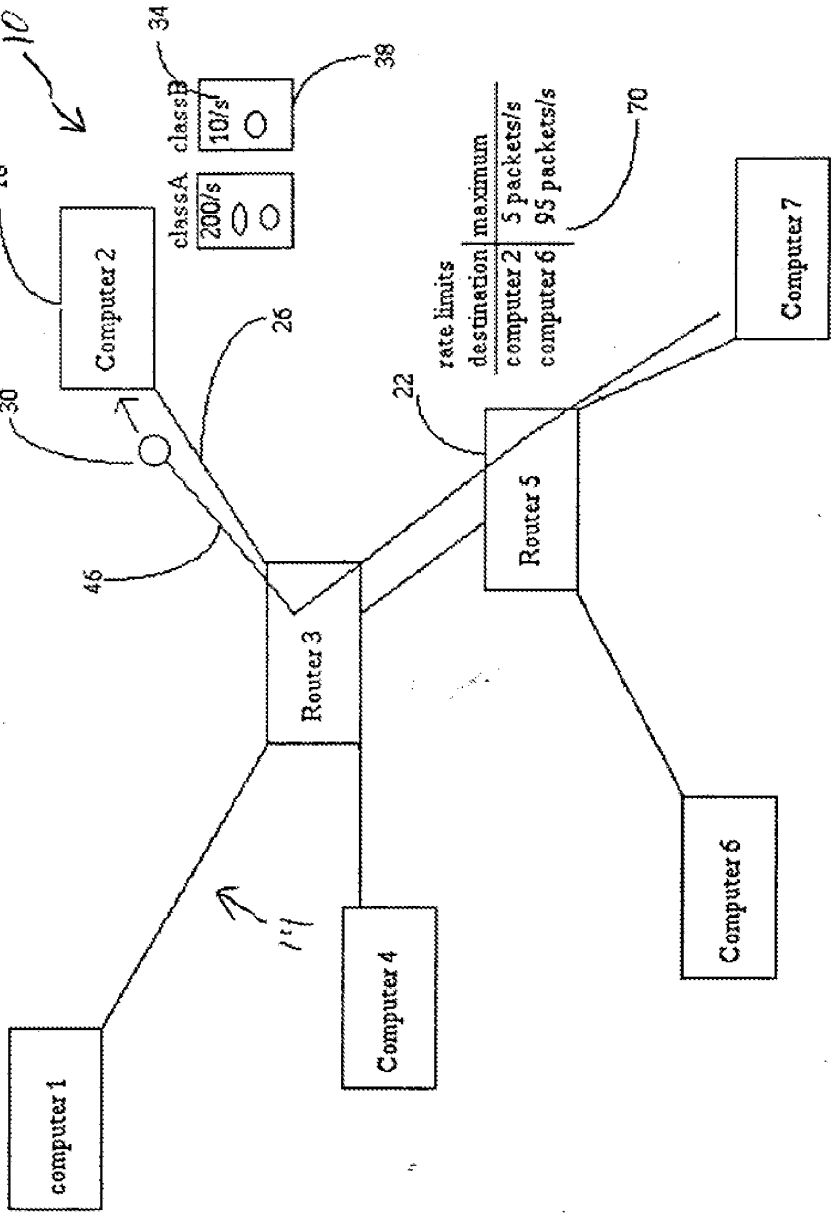

10
34
classB
10/s
38
classA
200/s
18
Computer 2
26
30
46
rate limits
destination | maximum
computer 2 | 5 packets/s
computer 6 | 95 packets/s
70
22
Router 5
Computer 7
Router 3
14
Computer 4
Computer 6
computer 1

Figure 2

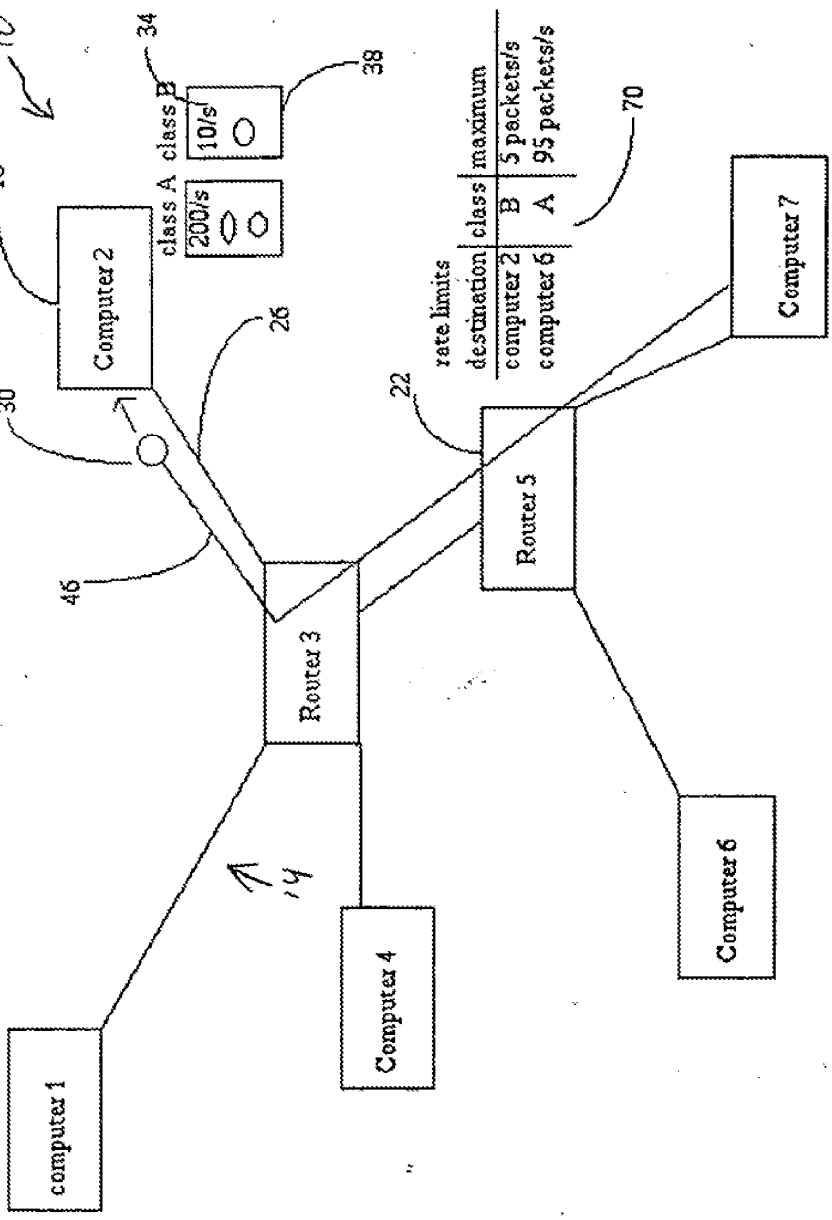

10
18
Computer 2
34
class B
10/s
38
class A
200/s
26
30
46
rate limits
destination | class | maximum
computer 2 | B | 5 packets/s
computer 6 | A | 95 packets/s
70
22
Router 5
Computer 7
Router 3
14
Computer 4
Computer 6
computer 1

Figure 3

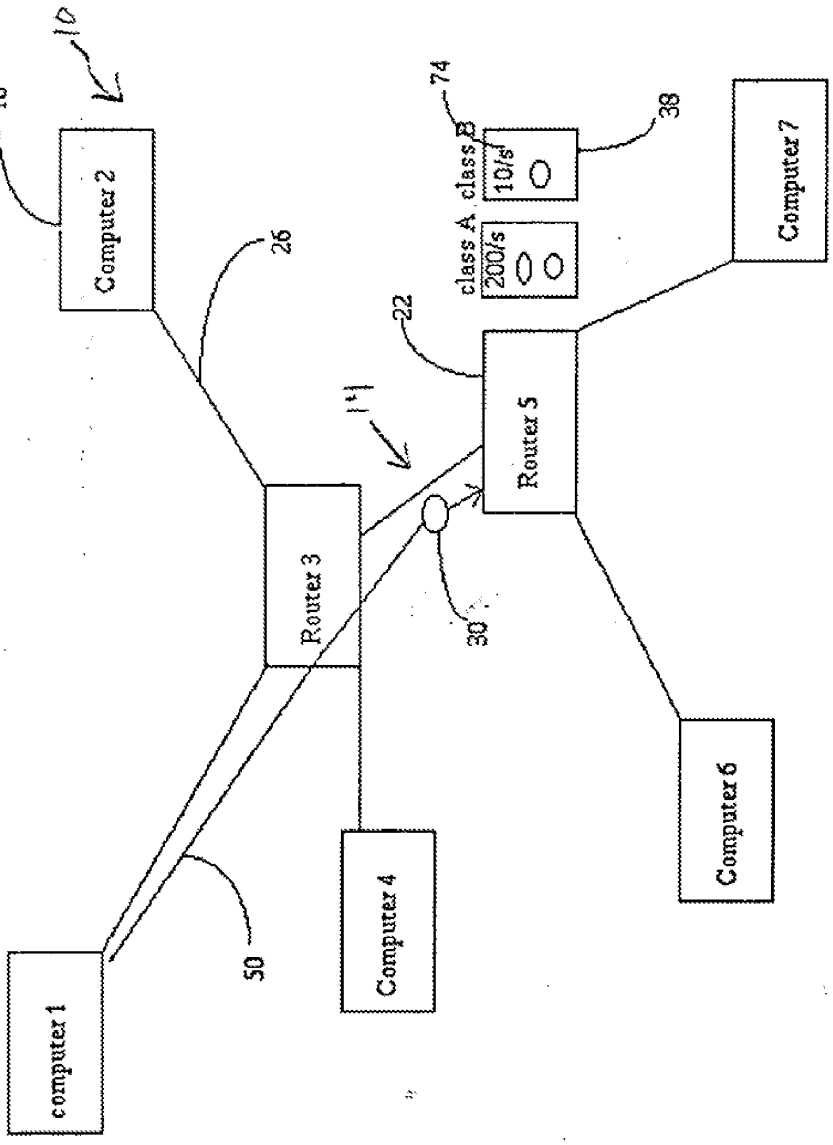
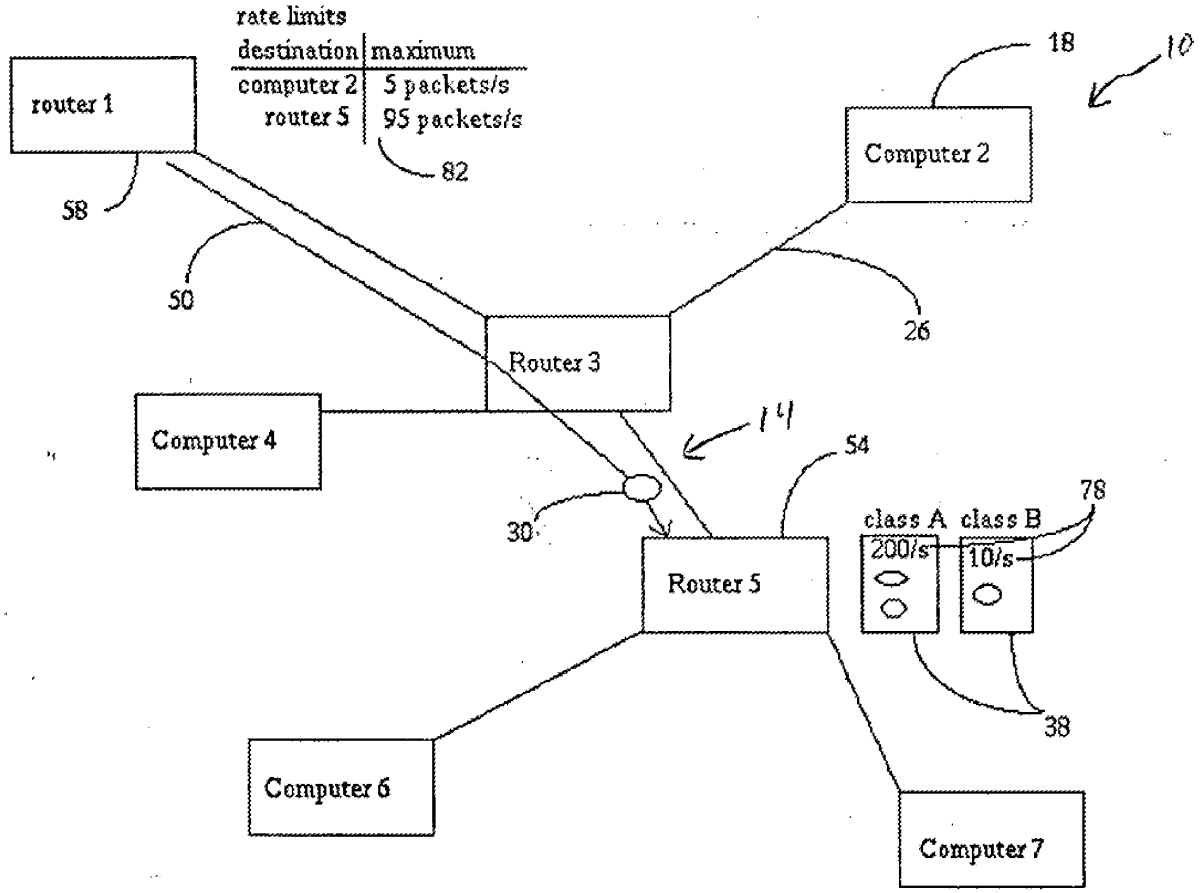

10
18
Computer 2
26
74
class B
10/s
38
class A
200/s
Computer 7
22
Router 5
14
Router 3
30
Computer 6
Computer 4
50
computer 1

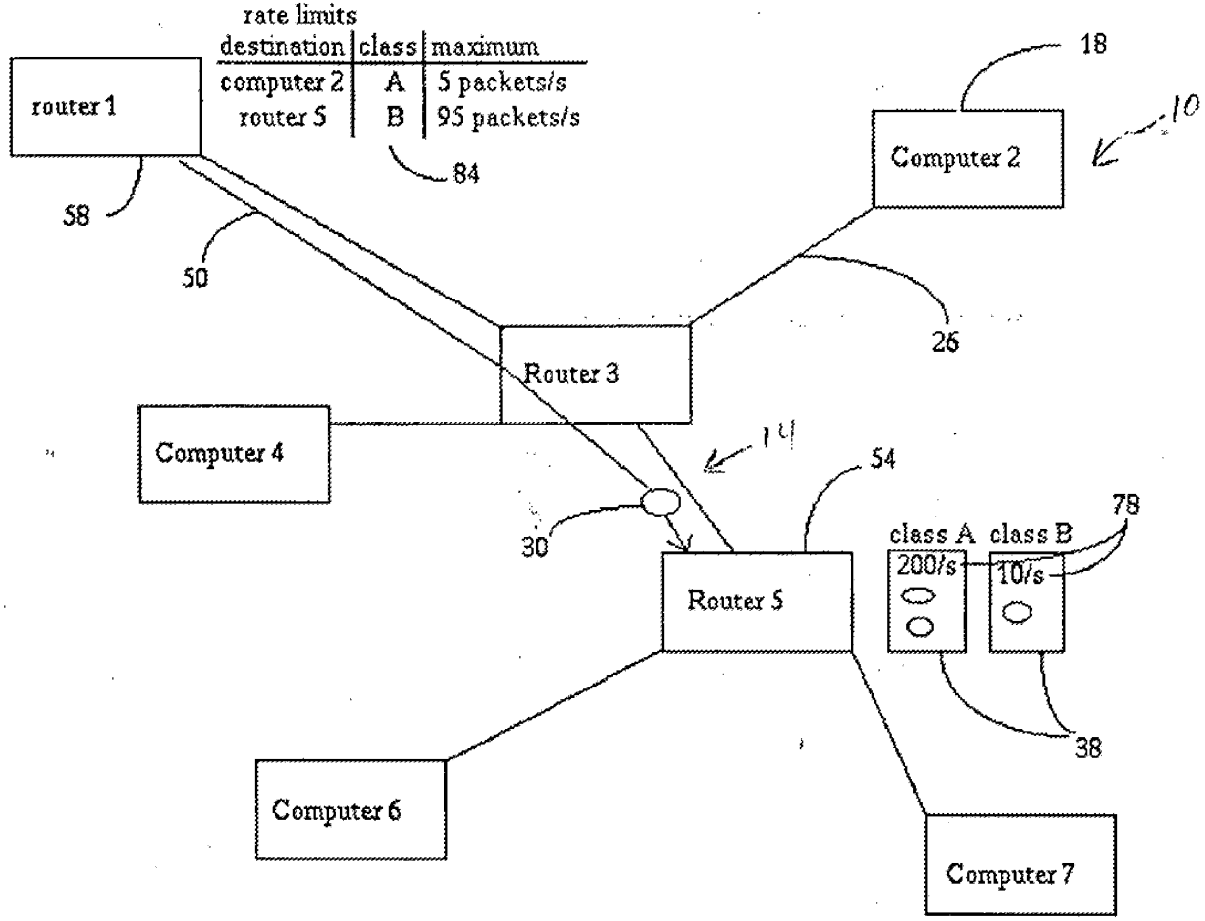
Figure 4

Figure 5



Cloudflare, Inc. Exhibit 1003 Page 545

Figure 6



Cloudflare, Inc. Exhibit 1003 Page 546

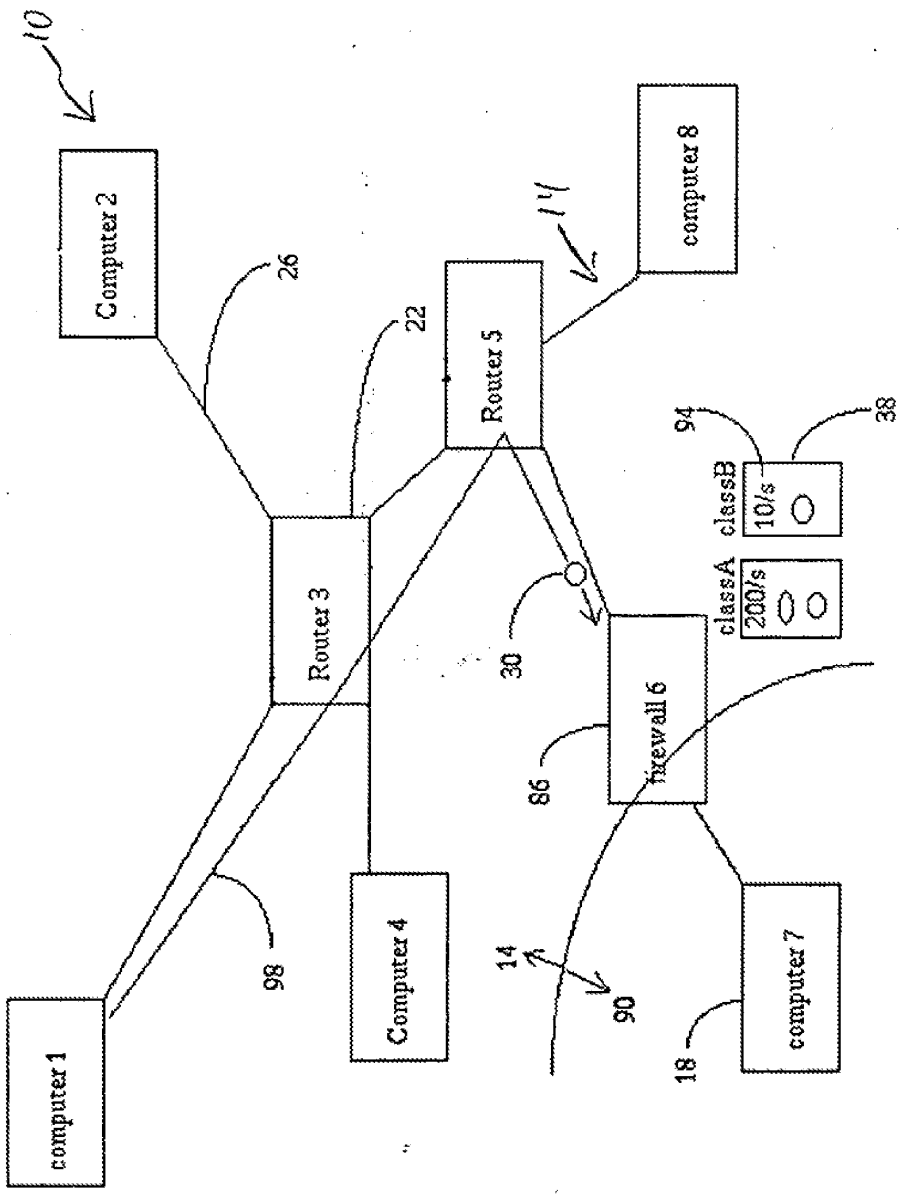

10
Computer 2
26
22
Router 5
11
computer 8
94
38
classB
10/s
classA
200/s
Router 3
30
firewall 6
86
98
Computer 4
14
90
18
computer 7
computer 1

Figure 7

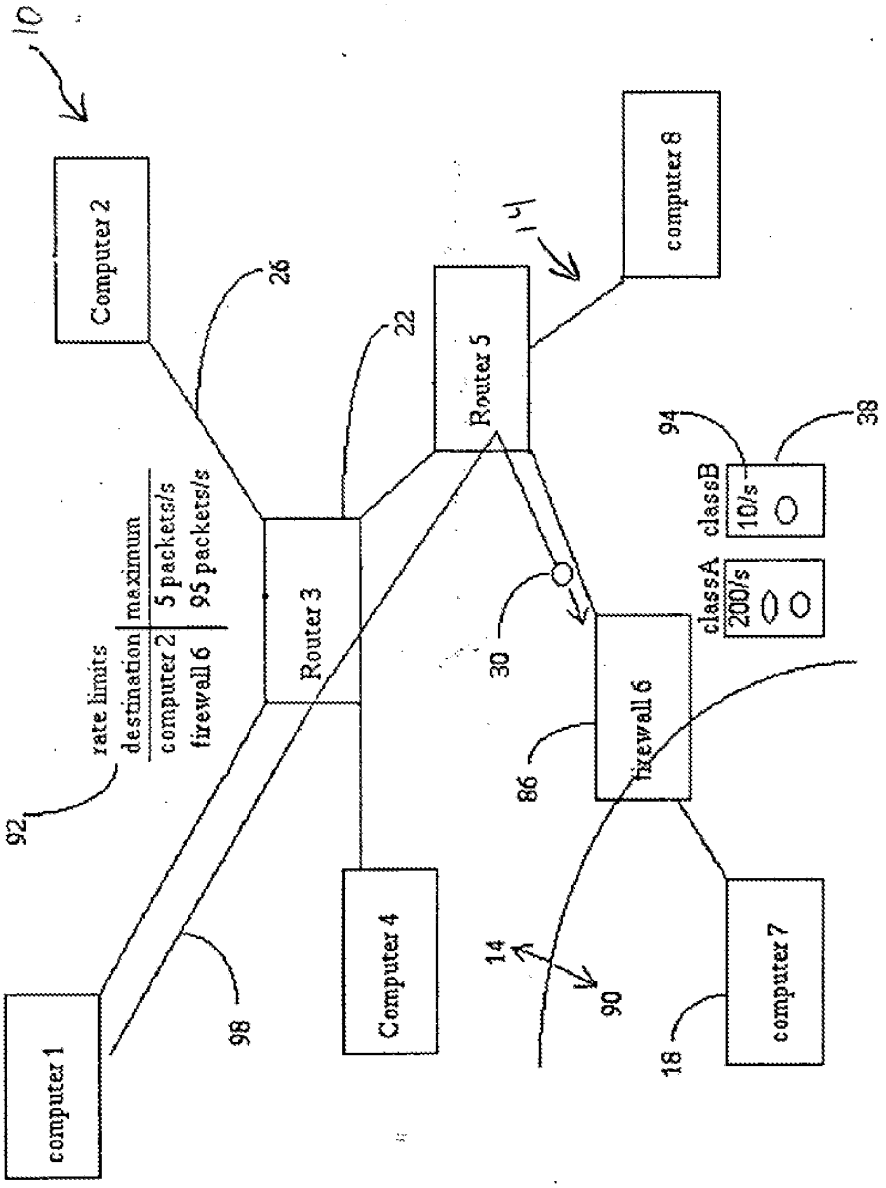

10
Computer 2
26
22
Router 5
14
computer 8
94
38
classB
10/s
classA
200/s
30
Router 3
rate limits
destination | maximum
computer 2 | 5 packets/s
firewall 6 | 95 packets/s
92
86
firewall 6
98
Computer 4
14
90
18
computer 7
computer 1

Figure 8

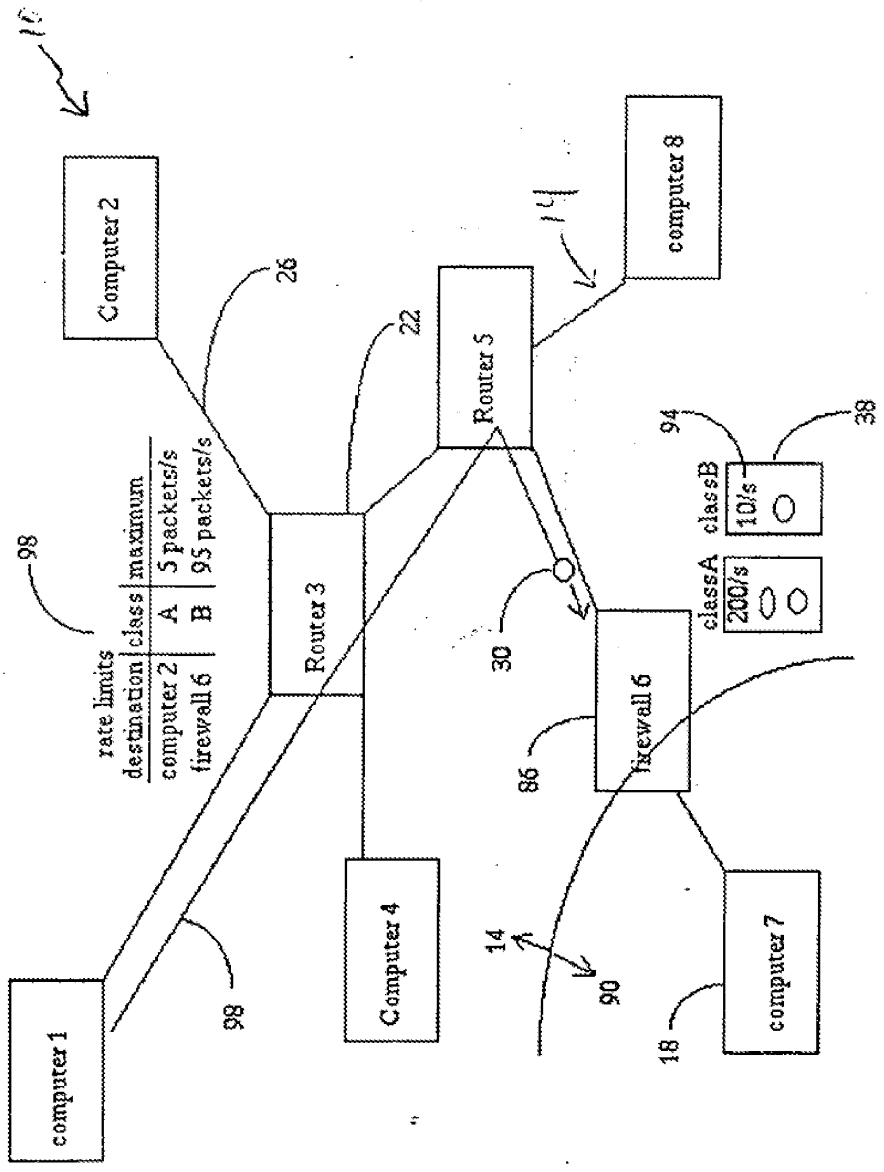

10
Computer 2
26
22
Router 5
14
computer 8
94
38
classB
10/s
98
rate limits
destination | class | maximum
computer 2 | A | 5 packets/s
firewall 6 | B | 95 packets/s
Router 3
30
classA
200/s
86
firewall 6
Computer 4
14
90
18
computer 7
98
computer 1

Figure 9

Please type a plus sign (+) inside this box → [+]

PTO/SB/81 (08-01)
Approved for use through 10/31/2002. OMB 0651-0035
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.

POWER OF ATTORNEY OR AUTHORIZATION OF AGENT

Application Number	09/715,813
Filing Date	11/16/2000
First Named Inventor	Cohen
Title	Packet Flooding Defense
Group Art Unit	2131
Examiner Name	Not Assigned
Attorney Docket Number	02-322-B (old Q982-08)

I hereby appoint:

[X] Practitioners at Customer Number 31718 → (31718)

OR

[ ] Practitioner(s) named below:

Name	Registration Number

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

[X] The above-mentioned Customer Number.

OR

[ ] Practitioners at Customer Number [ ] → *Place Customer Number Bar Code Label here*

OR

[ ] Firm or Individual Name					
Address					
Address					
City		State		Zip	
Country					
Telephone		Fax			

I am the:

[ ] Applicant/Inventor.

[X] Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

SIGNATURE of Applicant or Assignee of Record

Name	Deborah A. Taylor, President, Computing Services Support Solutions, Inc.
Signature	Deborah A. Taylor
Date	09 December 2002

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

[X] *Total of 1 forms are submitted.

Burden Hour Statement: This form is estimated to take 3 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

BEST AVAILABLE COPY

Docket No.
Q982-P

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

PACKET FLOODING DEFENSE SYSTEM

the specification of which

(check one)

☒ is attached hereto.

☐ was filed on _____ as United States Application No. or PCT International Application Number _____

and was amended on _____ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Not Claimed
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional

(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

William H. Pavitt, Jr.	**Registration No. 16,290;**
Natan Epstein	**Registration No. 28,997;**
Robert Jacobs	**Registration No. 33,403;**
David A. Belasco	**Registration No. 41,609;**
Todd B. Serota	**Registration No. 31,421**

Send Correspondence to: **David A. Belasco, Esq.**
BEEHLER & PAVITT
100 Corporate Pointe, Suite 330
Culver City, California 90230

Direct Telephone Calls to: *(name and telephone number)*
David A. Belasco, Esq. (310) 215-3183

Full name of sole or first inventor
Donald N. Cohen

Sole or first inventor's signature — Date

Residence
2815 Haddington Drive Los Angeles, California 90064

Citizenship
U.S.A.

Post Office Address
Same as above

Full name of second inventor, if any

Second inventor's signature — Date

Residence

Citizenship

Post Office Address

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

05/11/2004 GWDRBDF1 00000040 10841064

01 FC:2091 385.00 DP
02 FC:2201 387.00 DP

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002 — 489-267/69033

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2003

Application or Docket Number: 10/841,064

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS 18		
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	18 minus 20=	* 0
INDEPENDENT CLAIMS	12 minus 3 =	* 9
MULTIPLE DEPENDENT CLAIM PRESENT		☐

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY TYPE ☐		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
BASIC FEE	385.00	OR	BASIC FEE	770.00
XS 9=		OR	X$18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL	772	OR	TOTAL	

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐				

1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐				

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM ☐				

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	32	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:55
L2	444	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (router and denial adj1 service and bandwidth) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:56
L3	34	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (router and denial adj1 service and bandwidth) and firewall$ and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:58
L4	414	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (packet with flow adj2 (control or allocat$ or congest$ or ((high or large) adj1 (traffic or through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 16:02
L5	140	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (packet adj3 flow adj2 (control or allocat$ or congest$ or ((high or large) adj1 (traffic or through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 16:02
S1	2070	713/201.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:35
S2	3	713/201.ccls. and packet with flooding and router	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:56
S3	3	713/201.ccls. and packet with flooding and router	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:56

EAST Search History

S4	94	packet with flooding and router	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 16:03
S5	5	packet with flooding and router and denial and bandwidth	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:57
S6	495	router and denial and bandwidth	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:59
S7	471	router and denial adj1 service	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:59
S8	329	router and denial adj1 service and bandwidth	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 16:06
S9	64	router and denial and bandwidth and transmi$ adj1 rate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:00
S10	8	router and denial and bandwidth and send$ adj1 rate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:00
S11	982	network same router and flood$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:01
S12	118	network same router and flood$ and defen$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:01
S13	130	router and flood$ and defen$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:01

EAST Search History

S14	91	ddos	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:02
S15	30	packet adj1 class$ and denial adj1 service	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:02
S16	6	throttl$ with bandwidth and denial	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:03
S17	8	709/238-244.ccls. and denial and allocate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:05
S18	4	709/238-244.ccls. and flood$ with rate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:07
S19	241	709/238-244.ccls. and transmi$ with rate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:07
S20	126	router with flow adj1 control	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:08
S21	7	packet adj1 flood$ and defense	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:08
S22	446	packet with overload$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:16
S23	50	packet adj2 overload$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:17

EAST Search History

S24	96	packet adj1 flood$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:33
S25	568	packet with flow adj2 (control or allocat$) and router$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:34
S26	67	packet with flow adj2 (control or allocat$) and router$ and (defense or denial)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:50
S27	25	router with flow adj2 (control or allocat$) and (defense or denial)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:36
S28	2	"5367523".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:06
S29	2	"5007052".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:09
S30	2	"5699513".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:12
S31	2	"6412000".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:15
S32	2	"5434860".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:17
S33	2	"20020032871".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:19

Cloudflare, Inc. Exhibit 1003 Page 559

EAST Search History

S34	2	"4817080".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:21
S35	2	"6088804".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:21
S36	10	"5581559".pn. or "6044402".pn. or "5455865".pn. or "5353353".pn. or "5850515".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 15:51
S37	1	("5581559".pn. or "6044402".pn. or "5455865".pn. or "5353353".pn. or "5850515".pn.) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 15:51
S38	4	370/229-240.ccls. and packet with flooding and router	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 16:04
S39	17	370/229-240.ccls. and router and denial adj1 service and bandwidth	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:37
S40	5	370/229-240.ccls. and router and denial adj1 service and bandwidth and firewall	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 16:10
S41	7	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:57
S42	82	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router and denial adj1 service and bandwidth)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:57
S43	0	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial)) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:56

Cloudflare, Inc. Exhibit 1003 Page 560

EAST Search History

S44	54	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router and denial adj1 service and bandwidth) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:55
S45	1	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router and denial adj1 service and bandwidth) with firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:55
S46	2	(713/201,160.ccls. or 709/238-244. ccls. or 370/229-240.ccls.) and (router and denial adj1 service and bandwidth) with firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:55
S47	0	(713/201,160.ccls. or 709/238-244. ccls. or 370/229-240.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial)) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:56
S48	7	(713/201,160.ccls. or 709/238-244. ccls. or 370/229-240.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:53

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.
10/841,064	05/07/2004	Donald N. Cohen	04-165-B	9716

31718 7590 10/01/2007
BELASCO, JACOBS & TOWNSLEY LLP
HOWARD HUGHES CENTER
6100 CENTER DRIVE
SUITE 630
LOS ANGELES, CA 90045

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
10/01/2007	ELECTRONIC

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.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patmail@bjtlaw.com
donna@bjtlaw.com
denise@bjtlaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/841,064	COHEN, DONALD N.	
	Examiner	Art Unit	
	Ronald Baum	2136	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance 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.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 May 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 07 May 2004.

2. Claims 1-18 are pending for examination.

3. Claims 1-18 are rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-6, 8, 9, 11, 12, 14, 15, 17 and 18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 1, 4, the phrase "can use" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention (See MPEP § 2173.05(d)), insofar as "can use" is not a positive limitation but only requires the ability to so perform. It does not constitute a limitation in the patentable sense. *In re Hutchison*, 69 USPQ 138.

Regarding claims 3, 6, 9, 12, 15 and 18, the phrase "is capable" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention (See MPEP § 2173.05(d)), insofar as "is capable" is not a positive limitation but only requires the ability to so perform. It does not constitute a limitation in the patentable sense. *In re Hutchison*, 69 USPQ 138.

Regarding claims 1, 2, 4, 5, 8, 11, 14 and 17 the phrase "thereby" and "whereby" renders the claim indefinite because it has been held that the functional "whereby", "thereby" statement(s) do not define any structure and accordingly can not serve to distinguish. *In re Mason*, 114 USPQ 127, 44 CCPA 937 (1957).

Claim Rejections - 35 USC § 102

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

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Chang et al, U.S. Patent 5,367,523.

6. As per claim 1; "A packet flooding defense system *[col. 1, lines 7-11,col. 2, lines 53-col. 3, line 11, whereas flow and congestion control in packet networks corresponds to a packet flooding defense, and whereas senders, receivers, and intermediate nodes in a packet communications network correspond to network computers per se as well as typically computers configured as gateways, routers, and firewalls (i.e., col. 1, lines 27-col. 2, line 8)]* for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets *[figure 1 as applied to appropriate figures 2-9 and accompanying descriptions], said system comprising: means for classifying data packets received at a host computer; means for associating a maximum acceptable processing rate with each class of data packet received at said computer [col. 3, lines 12-46, col. 10, lines 8-col. 11, line 10, whereas the color coded*

green, yellow, etc., packet characterizations constitute classification, upon which rate criteria is established, which in itself is control of processing rate resources.], said system comprising:

means for classifying data packets received at a host computer;

means for associating a maximum acceptable processing rate with each class of data packet received at said computer *[col. 3, lines 12-46, col. 10, lines 8-col. 11, line 10, whereas the color coded green, yellow, etc., packet characterizations constitute classification, upon which rate criteria is established, which in itself is control of processing rate resources.]*;

means for said computer to find information for packets it receives regarding the path by which said packets came to said computer *[col. 5, lines 50-col. 6, line 9, col. 6, lines 21-48]*; and

whereby, said computer can use said information to allocate the processing rate available for packets of each class in a desired way *[figures 5-9 and accompanying descriptions]*.".

As per claim 7, this claim is the method claim for the means plus function claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "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;

classifying data packets received at a host computer 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 packets of each class in a desired way.".

As per claim 4, this claim is a narrower router versus a host receiving, and transmission versus processing rate variation of claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection (i.e., the packet communications network includes intermediate congestion control on a "hop by hop" (col. 1, lines 27-40) basis which broadly defined clearly encompasses network routers. Further, (col. 6, lines 2-4, "Such routing decisions...response to information in the header of the data packet.") determining the path by which the data arrives at the receiver is suggested by the fact that the header contains source / destination (IP) network addressing information which clearly constitutes routing (path) information (a router implemented function)); "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 router;

means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

means for said router to find information for packets it receives regarding the path by which said packets came to said router; and

whereby, said router can use said information to allocate the transmission rate for each class in a desired way.".

As per claim 10, this claim is the method claim for the means plus function claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection; "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;

classifying data packets received at a router 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 in a desired way.".

As per claim 13, this claim is a variation on claim 1 above, whereas the received packet path classification of, or information pertaining to, is used relative to a given limited (i.e., maximum) processing rate to allocate effective processing rate, and is rejected for the same reasons provided for the claim 1 rejection; "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 determining a path by which data packets arrive at a host computer;

means for classifying data packets received at said host computer 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 each class of data packet.".

As per claim 16, this claim is a narrower router versus a host receiving, and transmission versus processing rate variation of claim 13 above, and is rejected for the same reasons provided for the claim 13 rejection (i.e., the packet communications network includes intermediate congestion control on a "hop by hop" (col. 1, lines 27-40) basis which broadly defined clearly encompasses network routers. Further, (col. 6, lines 2-4, "Such routing decisions...response to information in the header of the data packet.") determining the path by which the data arrives at the receiver is suggested by the fact that the header contains source / destination (IP) network addressing information which clearly constitutes routing (path) information (a router implemented function)); "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 a router to determine a path by which said packets came to said router;

means for classifying data packets received at a router by path;

means for associating a maximum acceptable transmission rate with each class of data packet received at said router; and

means for said router to allocate the transmission rate for each class in a desired way.".

7. As per claim 2; "A packet flooding defense system *[col. 1, lines 7-11,col. 2, lines 53-col. 3, line 11, whereas flow and congestion control in packet networks corresponds to a packet flooding defense, and whereas senders, receivers, and intermediate nodes in a packet communications network correspond to network computers per se as well as typically computers configured as gateways, routers, and firewalls (i.e., col. 1, lines 27-col. 2, line 8)]* for a network

comprising a plurality of host computers, routers, communication lines and transmitted data packets *[figure 1 as applied to appropriate figures 2-9 and accompanying descriptions]*, said system comprising:

means for classifying data packets received at a host computer;

means for associating a maximum acceptable processing rate with each class of data packet received at said computer *[col. 3, lines 12-46, col. 10, lines 8-col. 11, line 10, whereas the color coded green, yellow, etc., packet characterizations constitute classification, upon which rate criteria is established, which in itself is control of processing rate resources.]*;

means for said computer to determine the rate at which data packets of each class are transmitted from a router to said computer;

means for said router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said computer;

means for said router to control the rate of transmission of data packets from said router to said computer; and

whereby, the rate of data packet transmissions received at said computer is kept below the maximum acceptable processing rate for each data packet class by said control of the rate of transmission of data packets from said router,

thereby freeing a portion of the network providing data packet transmission to said computer *[figures 5-9 and accompanying descriptions]*.".

As per claim 8, this claim is the method claim for the means plus function claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection; "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:

classifying data packets received at a host computer;

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

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

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

controlling the rate of transmission of data packets from said router to said computer by said router so that data packet transmissions received at said computer are kept below the maximum acceptable processing rate for each data packet class;

thereby freeing a portion of the network providing data packet transmission to said computer.".

As per claim 14, this claim is a variation on claim 2 above, insofar as the '... so that the rate of data packet transmissions ... kept below the maximum ... rate for each data packet class' aspect is explicitly part of the 'means for said router to control the rate of transmission' limitation in claim 14, whereas it is a broader aspect of the entire claim in claim 2, and is rejected for the same reasons provided for the claim 2 rejection; "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;

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

means for said computer to determine the rate at which data packets of each class are transmitted from a router to said computer;

means for said router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said computer; and

means for said router to control the rate of transmission of data packets from said router to said computer so that the rate of data packet transmissions received at said computer is kept below the maximum acceptable processing rate for each data packet class;

thereby freeing a portion of the network providing data packet transmission to said computer.".

As per claim 5, this claim is a narrower router versus a host receiving, and transmission versus processing rate variation of claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection (i.e., the packet communications network includes intermediate congestion control on a "hop by hop" (col. 1, lines 27-40) basis which broadly defined clearly encompasses network routers. Further, (col. 6, lines 2-4, "Such routing decisions...response to information in the header of the data packet.") determining the path by which the data arrives at the receiver is suggested by the fact that the header contains source / destination (IP) network addressing information which clearly constitutes routing (path) information (a router implemented function)); "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 first router;

means for associating a maximum acceptable transmission rate with each class of data packet received at said first router;

means for said first router to determine the rate at which data packets of each class are transmitted from a second router to said first router;

means for said second router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said first router;

means for said second router to control the rate of transmission of data packets from said second router to said first router; and

whereby, the rate of data packet transmissions received at said first router is kept below the maximum acceptable transmission rate for each data packet class by said control of the rate of transmission of data packets from said second router,

thereby freeing a portion of the network providing data packet transmission to said first router.".

As per claim 11, this claim is the method claim for the means plus function claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection; "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:

classifying data packets received at a first router;

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

determining by said first router of the rate at which data packets of each class are transmitted from a second router to said first router;

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

controlling by said second router of the rate of transmission of data packets from said second router to said first router so that said rate of transmission is below the maximum acceptable transmission rate for each data packet class;

thereby freeing a portion of the network providing data packet transmission to said first router.".

As per claim 17, this claim is a variation on claim 5 above, insofar as the '... so that the rate of data packet transmissions ... kept below the maximum ... rate for each data packet class' aspect is explicitly part of the 'means for said router to control the rate of transmission' limitation in claim 17, whereas it is a broader aspect of the entire claim in claim 5, and is rejected for the same reasons provided for the claim 5 rejection; "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 first router;

means for associating a maximum acceptable transmission rate with each class of data packet received at said first router;

means for said first router to determine the rate at which data packets of each class are transmitted from a second router to said first router;

means for said second router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said first router; and

means for said second router to control the rate of transmission of data packets from said second router to said first router so that the rate of data packet transmission received at said first router is kept below the maximum acceptable transmission rate for each data packet class;

thereby freeing a portion of the network providing data packet transmission to said first router.".

8. Claim 3 ***additionally recites*** the limitations that; "A packet flooding defense system as described in claim 2, wherein:

said router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router is capable of control ling the rate of transmission of each class of data packets to said computer.".

The teachings of Chang et al (figures 5-9 and accompanying descriptions) suggest such limitations.

As per claim 9, this claim is the method claim for the means plus function claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection; "A method as described in claim 8, in which:

said router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router is capable of controlling the rate of transmission of each class of data packets to said computer.".

As per claim 15, this claim is a variation on claim 3 above, insofar as the '... so that the rate of data packet transmissions ... kept below the maximum ... rate for each data packet class' aspect is explicitly part of the 'means for said router to control the rate of transmission' limitation in claim 14, whereas it is a broader aspect of the entire claim in claim 3, and is rejected for the same reasons provided for the claim 3 rejection; "A packet flooding defense system as described in claim 14, in which:

said router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router is capable of controlling the rate of transmission of each class of data packet to said computer.".

As per claim 6, this claim is a narrower router versus a host receiving, and transmission versus processing rate variation of claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection (i.e., the packet communications network includes intermediate congestion control on a "hop by hop" (col. 1, lines 27-40) basis which broadly defined clearly encompasses network routers. Further, (col. 6, lines 2-4, "Such routing decisions...response to information in the header of the data packet.") determining the path by which the data arrives at

the receiver is suggested by the fact that the header contains source / destination (IP) network addressing information which clearly constitutes routing (path) information (a router implemented function)); "A packet flooding defense system as described in claim 5, wherein:

said second router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router is capable of controlling the rate of transmission of each class of data packets to said first router.".

The teachings of Chang et al (Abstract, figure 1 and associated description, col. 1,lines 22-col.

As per claim 12, this claim is the method claim for the means plus function claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection; "A method as described in claim 11, in which:

said second router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router is capable of controlling the rate of transmission of each class of data packets to said first router.".

As per claim 18, this claim is a variation on claim 6 above, insofar as the '... so that the rate of data packet transmissions ... kept below the maximum ... rate for each data packet class' aspect is explicitly part of the 'means for said router to control the rate of transmission' limitation in claim 18, whereas it is a broader aspect of the entire claim in claim 6, and is rejected

for the same reasons provided for the claim 6 rejection; "A packet flooding defense system as described in claim 17, wherein:

said second router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router is capable of controlling the rate of transmission of each class of data packets to said first router.".

Conclusion

9. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300.**

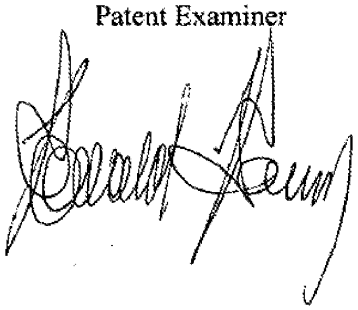
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through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

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

9/25/07



Notice of References Cited	Application/Control No. 10/841,064	Applicant(s)/Patent Under Reexamination COHEN, DONALD N.	
	Examiner Ronald Baum	Art Unit 2136	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,367,523	11-1994	Chang et al.	370/235
*	B	US-5,007,052	04-1991	Flammer, George	370/389
*	C	US-6,412,000	06-2002	Riddle et al.	709/224
*	D	US-5,434,860	07-1995	Riddle, Guy G.	370/232
*	E	US-2002/0032871	03-2002	Malan et al.	713/201
*	F	US-6,088,804	07-2000	Hill et al.	726/25
*	G	US-5,581,559	12-1996	Crayford et al.	370/392
*	H	US-6,044,402	03-2000	Jacobson et al.	709/225
*	I	US-5,455,865	10-1995	Perlman, Radia J.	713/153
*	J	US-5,353,353	10-1994	Vijeh et al.	380/29
*	K	US-5,850,515	12-1998	Lo et al.	714/43
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	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.

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. 9716

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/841,064	05/07/2004 RULE	713	2136	04-165-B

APPLICANTS
Donald N. Cohen, Los Angeles, CA;

**** CONTINUING DATA ***************************
This application is a CON of 09/715,813 11/16/2000 PAT 6,789,190

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY ****
07/12/2004

Foreign Priority claimed	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No ☐ Met after Allowance Verified and Acknowledged _____ Examiner's Signature _____ Initials	CA	9	18	12

ADDRESS

BELASCO, JACOBS & TOWNSLEY LLP
HOWARD HUGHES CENTER
6100 CENTER DRIVE
SUITE 630
LOS ANGELES, CA 90045
UNITED STATES

TITLE

Packet flooding defense system

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
772	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

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
10/841,064	COHEN, DONALD N.
Examiner	**Art Unit**
Ronald Baum	2136

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date								
Final	Original	9/25/07								
	1	√								
	2	√								
	3	√								
	4	√								
	5	√								
	6	√								
	7	√								
	8	√								
	9	√								
	10	√								
	11	√								
	12	√								
	13	√								
	14	√								
	15	√								
	16	√								
	17	√								
	18	√								
	19									
	20									
	21									
	22									
	23									
	24									
	25									
	26									
	27									
	28									
	29									
	30									
	31									
	32									
	33									
	34									
	35									
	36									
	37									
	38									
	39									
	40									
	41									
	42									
	43									
	44									
	45									
	46									
	47									
	48									
	49									
	50									

Claim		Date								
Final	Original									
	51									
	52									
	53									
	54									
	55									
	56									
	57									
	58									
	59									
	60									
	61									
	62									
	63									
	64									
	65									
	66									
	67									
	68									
	69									
	70									
	71									
	72									
	73									
	74									
	75									
	76									
	77									
	78									
	79									
	80									
	81									
	82									
	83									
	84									
	85									
	86									
	87									
	88									
	89									
	90									
	91									
	92									
	93									
	94									
	95									
	96									
	97									
	98									
	99									
	100									

Claim		Date								
Final	Original									
	101									
	102									
	103									
	104									
	105									
	106									
	107									
	108									
	109									
	110									
	111									
	112									
	113									
	114									
	115									
	116									
	117									
	118									
	119									
	120									
	121									
	122									
	123									
	124									
	125									
	126									
	127									
	128									
	129									
	130									
	131									
	132									
	133									
	134									
	135									
	136									
	137									
	138									
	139									
	140									
	141									
	142									
	143									
	144									
	145									
	146									
	147									
	148									
	149									
	150									

Search Notes

Application/Control No.	Applicant(s)/Patent under Reexamination	
10/841,064	COHEN, DONALD N.	
Examiner	**Art Unit**	
Ronald Baum	2136	

SEARCHED			
Class	Subclass	Date	Examiner
none	none	9/25/2007	RJB

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
inventor search	9/25/2007	RJB
Google(npl):packet flow control congestion traffic router denial service	9/25/2007	RJB
class 709,713,726,370,380 with text patent search: see attached EAST search history	9/25/2007	RJB

PATENT
Docket 04-165-B

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Cohen	Examiner:	Baum
Serial No.:	10/841,064	Group Art Unit:	2136
Filed:	05/07/2004	Confirmation No.:	9716
Title:	PACKET FLOODING DEFENSE SYSTEM		

AMENDMENT

In response to the Office action of October 1, 2007, please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 11 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

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; and

~~whereby, said computer can~~means in said computer for useing said information to allocate the processing rate available for unwanted data packets ~~of each class in a desired way~~to be less than or equal to said maximum acceptable processing rate.

2. (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 determine the rate at which data packets of each class are transmitted from a router to said computer;

means for said router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said computer;

means for said router to control the rate of transmission of data packets from said router to said computer; and

~~whereby,~~means in said computer for keeping the rate of data packet transmissions received at said computer ~~is kept~~ below the maximum acceptable processing rate for each data packet class by said control of the rate of transmission of data packets from said router, ~~thereby~~ and freeing a portion of the network providing data packet transmission to said computer.

3. (currently amended): A packet flooding defense system as described in Claim 2, wherein:

said router ~~is capable of~~ receive~~sing~~ information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router ~~is capable of controlling~~ controls the rate of transmission of each class of data packets to said computer.

4. (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 router into wanted data packets and unwanted data packets;

means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

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; and

~~whereby,~~ means in said router for said router ~~can~~ to use said information to allocate the transmission rate for ~~each class in a desired way~~unwanted data packets to be less than equal to said maximum acceptable transmission rate.

5. (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 first router into wanted data packets and unwanted data packets;

means for associating a maximum acceptable transmission rate with each class of data packet received at said first router;

means for said first router to determine the rate at which data packets of each class are transmitted from a second router to said first router;

means for said second router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said first router;

means for said second router to control the rate of transmission of data packets from said second router to said first router; and

~~whereby,~~means in said first router for keeping the rate of data packet transmissions received at said first router ~~is kept~~ below the maximum acceptable transmission rate for ~~each~~ unwanted data packets ~~class~~ by said control of the rate of transmission of data packets from said second router, ~~thereby~~ and freeing a portion of the network providing data packet transmission to said first router.

6. (currently amended): A packet flooding defense system as described in Claim 5, wherein:

said second router ~~is capable of receiving~~ receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router ~~is capable of~~ controlsling the rate of transmission of each class of data packets to said first router.

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~~.

8. (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:

classifying data packets received at a host computer into wanted data packets and unwanted data packets;

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

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

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

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

~~thereby~~ freeing a portion of the network providing data packet transmission to said computer.

9. (currently amended): A method as described in Claim 8, in which:

said router ~~is capable of receiving~~ receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router ~~is capable of controlling~~ controls the rate of transmission of each class of data packets to said computer.

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~~.

11. (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:

classifying data packets received at a first router into wanted data packets and unwanted data packets;

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

determining by said first router of the rate at which data packets of each class are transmitted from a second router to said first router;

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

controlling by said second router of the rate of transmission of data packets from said second router to said first router so that said rate of transmission is below the maximum acceptable transmission rate for each data packet class; and

~~thereby~~ freeing a portion of the network providing data packet transmission to said first router.

12. (currently amended): A method as described in Claim 11, in which:

said second router ~~is capable of~~ receive~~sing~~ information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router ~~is capable of controlling~~ controls the rate of transmission of each class of data packets to said first router.

13. (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 determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host 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 ~~each class of~~ said unwanted data packets.

14. (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 determine the rate at which data packets of each class are transmitted from a router to said computer;

means for said router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said computer; and

means for said router to control the rate of transmission of data packets from said router to said computer so that the rate of data packet transmissions received at said computer is kept below the maximum acceptable processing rate for each data packet class; and

~~thereby~~ freeing a portion of the network providing data packet transmission to said computer.

15. (currently amended): A packet flooding defense system as described in Claim 14, in which:

said router ~~is capable of receiving~~ receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router ~~is capable of controlling~~ controls the rate of transmission of each class of data packet to said computer.

16. (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 a router to determine a path by which said packets came to said router via packet marks provided by routers leading to said router;

means for classifying data packets received at ~~a~~ said router into wanted data packets and unwanted data packets by path;

means for associating a maximum acceptable transmission rate with each class of data packet received at said router; and

means for said router to allocate the transmission rate for ~~each class in a desired way~~unwanted data packets to be less than equal to said maximum acceptable processing rate.

17. (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 first router into wanted data packets and unwanted data packets;

means for associating a maximum acceptable transmission rate with each class of data packet received at said first router;

means for said first router to determine the rate at which data packets of each class are transmitted from a second router to said first router;

means for said second router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said first router; and

means for said second router to control the rate of transmission of data packets from said second router to said first router so that the rate of data packet transmission received at said first router is kept below the maximum acceptable transmission rate for each data packet class; and

~~thereby~~ freeing a portion of the network providing data packet transmission to said first router.

18. (currently amended): A packet flooding defense system as described in Claim 17, wherein:

said second router ~~is capable of receiving~~ receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router ~~is capable of controlling~~ controls the rate of transmission of each class of data packets to said first router.

REMARKS/ARGUMENTS

The Examiner rejected Claims 1-6, 8, 9, 11, 12, 14, 15, 17 and 18 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner stated the phrases "can use" and "is capable", and the words "thereby" and "whereby" render the claims in which they are used indefinite. In response the Applicant has reworded Claims 1-6, 8, 9, 11, 12, 14, 15, 17 and 18 to eliminate use of these phrases and words.

The Examiner rejected Claims 1-18 35 U.S.C. 102(b) as being anticipated by Chang et al., U.S.Patent No. 5,367,523.

> For a prior art reference to anticipate a claim, the reference must disclose each and every element of the claim with sufficient clarity to prove its existence in the prior art. *See In re Spada*, 911 F.2d 705, 708, 15 USPQ 2d 1655, 1657 (Fed. Cir. 1990) ("[T]he [prior art] reference must describe the applicant's claimed invention sufficiently to have placed a person of ordinary skill in the field of the invention in possession of it." (citations omitted)). Although this disclosure requirement presupposes the knowledge of one skilled in the art of the claimed invention, that presumed knowledge does not grant a license to read into the prior art reference teachings that are not there. ***Motorola, Inc. v. Interdigital Tech. Corp.***, 43 USPQ 2d 1481, 1490 (Fed. Cir. 1997)

Chang et al. disclose an end-to-end, closed loop flow and congestion control system for packet communications networks which exchanges rate request and rate response messages between data senders and receivers to allow the senders to adjust the data rate to avoid congestion and to control the data flow. Requests and responses are piggy-backed on data packets and result in changes in the input data rate in a direction to optimize data throughput. GREEN, YELLOW and RED operating modes are defined to increase data input, reduce data input and reduce data input drastically, respectively. Incremental changes in data input are altered non-linearly to change more quickly when further away from the optimum operating point than when closer to the optimum operating point. See Abstract and column 2, line 53 to column 4, line 25.

In contrast the instant invention is intended to prevent a packet flooding attack. See page 1, lines 10-12. In the instant invention there is no communication between the receiver and sender. Such communication would be pointless because the attacker intends to overwhelm the victim by

sending a multitude of data packets as rapidly as possible in an attempt to shut down the victim. See page 3, lines 12-16. Thus the attacker will never respond to any requests to reduce the inflow of data packets. As a consequence, the instant invention only detects the path from which the data packets come via packet marks and then sorts data packets into two classes, wanted and unwanted, based on the path from which the data packet come. See page 7, lines 15-21; page 5, lines 20-22; page 6, lines 6-9; and Figures 1-6.

The Applicant has amended claims 1-18 to include the facts 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. Support for these amendments can be found at page 7, lines 15-21; page 5, lines 20-22; page 6, lines 6-9; and Figures 1-6. No new matter has been added.

Chang et al. do not disclose each and every element in the instant claims, as amended. Specifically, Chang et al. do not disclose: detecting the path from which the data packets come; detecting packet marks; and sorting data packets into two classes, wanted and unwanted. Further, Chang et al. require feedback from the receiver to the sender, which is not found in the instant invention. Thus the instant claims, as amended, are patentably distinct from Chang et al.

An extension fee of $525 for a small entity is due because this Amendment is being submitted within the third extension month. This fee will be electronically paid on electronic filing of this amendment. Reconsideration of this application and its early allowance are respectfully requested in view of the above presented amendments and remarks.

Respectfully submitted,



David A. Belasco
Applicant's Attorney
Registration No. 41,609

BELASCO JACOBS & TOWNSLEY, LLP
6100 Center Drive, Suite 630
Los Angeles, CA 90045
Phone: (310) 743-1188
Fax: (310) 743-1189

Electronic Patent Application Fee Transmittal

Application Number:	10841064
Filing Date:	07-May-2004
Title of Invention:	Packet flooding defense system
First Named Inventor/Applicant Name:	Donald N. Cohen
Filer:	David Allen Belasco/Donna Miller
Attorney Docket Number:	04-165-B

Filed as Small Entity

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 3 months with $0 paid	2253	1	525	525

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	525

Electronic Acknowledgement Receipt

EFS ID:	2954438
Application Number:	10841064
International Application Number:	
Confirmation Number:	9716
Title of Invention:	Packet flooding defense system
First Named Inventor/Applicant Name:	Donald N. Cohen
Customer Number:	31718
Filer:	David Allen Belasco/Donna Miller
Filer Authorized By:	David Allen Belasco
Attorney Docket Number:	04-165-B
Receipt Date:	05-MAR-2008
Filing Date:	07-MAY-2004
Time Stamp:	16:44:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$525
RAM confirmation Number	1965
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)

1	Amendment - After Non-Final Rejection	Amendment.pdf	465939 132fbe19839ca8e3d2684e1ddc388a900d8179d4e	no	13
Warnings:					
Information:					
2	Fee Worksheet (PTO-06)	fee-info.pdf	8129 04e96a7112f0b0a722c7ce5f911176f9272b58268	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	474068		

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.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/841,064	05/07/2004	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	03/05/2008	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 18	Minus	** 20	= 0	X $25 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 12	Minus	***12	= 0	X $100 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/EVELYN G. NIMMONS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 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: 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.

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.
10/841,064	05/07/2004	Donald N. Cohen	04-165-B	9716

31718 7590 06/13/2008
BELASCO, JACOBS & TOWNSLEY LLP
HOWARD HUGHES CENTER
6100 CENTER DRIVE
SUITE 630
LOS ANGELES, CA 90045

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
06/13/2008	ELECTRONIC

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.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patmail@bjtlaw.com
donna@bjtlaw.com
denise@bjtlaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/841,064	COHEN, DONALD N.	
	Examiner	Art Unit	
	RONALD BAUM	2139	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance 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.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 05 March 2008.

2. Claims 1-18 are pending for examination.

3. Claims 1-18 are rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. The rejection under 35 U.S.C. 112, second paragraph, is withdrawn.

Claim Rejections - 35 USC § 102

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

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Chang et al, U.S. Patent 5,367,523.

6. As per claim 1; "A packet flooding defense system *[col. 1, lines 7-11,col. 2, lines 53-col. 3, line 11, whereas flow and congestion control in packet networks corresponds to a packet flooding defense, and whereas senders, receivers, and intermediate nodes in a packet communications network correspond to network computers per se as well as typically computers configured as gateways, routers, and firewalls (i.e., col. 1, lines 27-col. 2, line 8)]* for a network

comprising a plurality of host computers, routers, communication lines and transmitted data packets *[figure 1 as applied to appropriate figures 2-9 and accompanying descriptions]*, said system comprising:

means for

classifying data packets received at a host computer into

wanted data packets and

unwanted data packets *[col. 3, lines 12-46, col. 10, lines 8-col. 11, line 10, whereas the color coded green, yellow, etc., packet characterizations constitute classification, upon which flow and congestion 'control' in packet networks is in itself control of processing rate resources, which in such an environment would broadly constitute a classifying of said packets into wanted and unwanted, rendering that aspect of the claim limitation not patently distinct.]*;

means for

associating a maximum acceptable processing rate with

each class of data packet

received at said computer *[col. 3, lines 12-46, col. 10, lines 8-col. 11, line 10, whereas the color coded green, yellow, etc., packet characterizations constitute classification, upon which rate criteria is established, which in itself is control of processing rate resources.]*;

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 *[col. 5, lines 50-col. 6, line 9, col. 6, lines 21-48, whereas the inherent inclusion of a sending network node IP address (i.e., **the** router ' leading to said host computer ') in a given packets header as received by a given destination node (i.e., ' via packet marks provided by router ' associated with **the** 'said host computer '), which would broadly constitute ' [found] information ... regarding the path ', rendering that aspect of the claim limitation not patently distinct.]*; 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 *[figures 5-9 and accompanying descriptions, col. 3, lines 12-46, col. 10, lines 8-col. 11, line 10, whereas the color coded green, yellow, etc., packet characterizations constitute classification, upon which rate criteria is established, which in itself is control of processing rate resources (i.e., ' allocate the processing rate available ... less than or equal to ... said maximum acceptable processing rate [i.e., the*

whole point of the Chang et al reference congestion and flow control]'), and further, the inherent inclusion of a sending network node IP address in a given packets header as received by a given destination node (i.e., ' said information '), rendering that aspect of the claim limitation not patently distinct.].".

As per claim 7, this claim is the method claim for the means plus function claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

As per claim 4, this claim is a narrower router versus a host receiving, and transmission versus processing rate variation of claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection (i.e., the packet communications network includes intermediate congestion control on a "hop by hop" (col. 1, lines 27-40) basis which broadly defined clearly encompasses network routers. Further, (col. 6, lines 2-4, "Such routing decisions…response to information in the header of the data packet.") determining the path by which the data arrives at the receiver is suggested by the fact that the header contains source / destination (IP) network addressing information which clearly constitutes routing (path) information (a router implemented function)).

As per claim 10, this claim is the method claim for the means plus function claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection.

As per claim 13, this claim is a variation on claim 1 above, whereas the received packet path classification of, or information pertaining to, is used relative to a given limited (i.e., maximum) processing rate to allocate effective processing rate, and is rejected for the same reasons provided for the claim 1 rejection.

As per claim 16, this claim is a narrower router versus a host receiving, and transmission versus processing rate variation of claim 13 above, and is rejected for the same reasons provided for the claim 13 rejection (i.e., the packet communications network includes intermediate congestion control on a "hop by hop" (col. 1, lines 27-40) basis which broadly defined clearly encompasses network routers. Further, (col. 6, lines 2-4, "Such routing decisions…response to information in the header of the data packet.") determining the path by which the data arrives at the receiver is suggested by the fact that the header contains source / destination (IP) network addressing information which clearly constitutes routing (path) information (a router implemented function)).

7. As per claim 2; "A packet flooding defense system *[col. 1, lines 7-11,col. 2, lines 53-col. 3, line 11, whereas flow and congestion control in packet networks corresponds to a packet flooding defense, and whereas senders, receivers, and intermediate nodes in a packet communications network correspond to network computers per se as well as typically computers configured as gateways, routers, and firewalls (i.e., col. 1, lines 27-col. 2, line 8)]* for a network comprising a plurality of host computers, routers, communication lines and transmitted data

packets *[figure 1 as applied to appropriate figures 2-9 and accompanying descriptions]*, said system comprising:

means for

classifying data packets received at a host computer into

wanted data packets and

unwanted data packets *[col. 3, lines 12-46, col. 10, lines 8-col. 11, line 10, whereas the color coded green, yellow, etc., packet characterizations constitute classification, upon which flow and congestion 'control' in packet networks is in itself control of processing rate resources, which in such an environment would broadly constitute a classifying of said packets into wanted and unwanted, rendering that aspect of the claim limitation not patently distinct.]*;

means for

associating a maximum acceptable processing rate with

each class of data packet

received at said computer *[col. 3, lines 12-46, col. 10, lines 8-col. 11, line 10, whereas the color coded green, yellow, etc., packet characterizations constitute classification, upon which rate criteria is established, which in itself is control of processing rate resources.]*;

means for said computer

to determine the rate at which data packets of each class

are transmitted from

a router to

said computer *[col. 3, lines 12-46, col. 10, lines 8-col. 11, line 10, whereas the color coded green, yellow, etc., packet characterizations constitute classification, upon which rate criteria is established, which in itself is control of processing rate resources.]*;

means for said router

to receive information regarding

maximum acceptable transmission rate for

data packets being transmitted to

said computer *[col. 3, lines 12-46, col. 10, lines 8-col. 11, line 10, whereas the color coded green, yellow, etc., packet characterizations constitute classification, upon which rate criteria is established, which in itself is control of processing rate resources.]*;

means for said router

to control the rate of transmission of

data packets from

said router to

said computer *[figures 5-9 and accompanying descriptions, col. 3, lines 12-46, col. 10, lines 8-col. 11, line 10, whereas the packet characterizations constitute classification, upon which rate criteria is established, which in itself is control of processing rate resources (i.e., '* to

control the rate of transmission of *[i.e., the whole point of the Chang et al reference congestion and flow control]').]*; and

means in said computer for

keeping the rate of data packet transmissions

received at said computer

below the maximum acceptable processing rate for

each data packet class by

said control of the rate of transmission of data

packets from said router, and

freeing a portion of

the network providing data packet transmission to

said computer *[figures 5-9 and accompanying descriptions, col. 3, lines 12-46, col. 10, lines 8-col. 11, line 10, whereas the color coded green, yellow, etc., packet characterizations constitute classification, upon which rate criteria is established, which in itself is control of processing rate resources (i.e., 'keeping the rate of data packet ... below the maximum acceptable processing rate for each data packet class ... freeing a portion the network providing [i.e., the whole point of the Chang et al reference congestion and flow control'), rendering that aspect of the claim limitation not patently distinct.]*.".

As per claim 8, this claim is the method claim for the means plus function claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection.

As per claim 14, this claim is a variation on claim 2 above, insofar as the '… so that the rate of data packet transmissions … kept below the maximum … rate for each data packet class' aspect is explicitly part of the 'means for said router to control the rate of transmission' limitation in claim 14, whereas it is a broader aspect of the entire claim in claim 2, and is rejected for the same reasons provided for the claim 2 rejection.

As per claim 5, this claim is a narrower router versus a host receiving, and transmission versus processing rate variation of claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection (i.e., the packet communications network includes intermediate congestion control on a "hop by hop" (col. 1, lines 27-40) basis which broadly defined clearly encompasses network routers. Further, (col. 6, lines 2-4, "Such routing decisions…response to information in the header of the data packet.") determining the path by which the data arrives at the receiver is suggested by the fact that the header contains source / destination (IP) network addressing information which clearly constitutes routing (path) information (a router implemented function)).

As per claim 11, this claim is the method claim for the means plus function claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection.

As per claim 17, this claim is a variation on claim 5 above, insofar as the '… so that the rate of data packet transmissions … kept below the maximum … rate for each data packet class' aspect is explicitly part of the 'means for said router to control the rate of transmission' limitation in claim 17, whereas it is a broader aspect of the entire claim in claim 5, and is rejected for the same reasons provided for the claim 5 rejection.

8. Claim 3 ***additionally recites*** the limitations that; "A packet flooding defense system as described in claim 2, wherein:

said router is capable of receiving information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router is capable of control ling the rate of transmission of each class of data packets to said computer.".

The teachings of Chang et al (figures 5-9 and accompanying descriptions) suggest such limitations.

As per claim 9, this claim is the method claim for the means plus function claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection.

As per claim 15, this claim is a variation on claim 3 above, insofar as the '… so that the rate of data packet transmissions … kept below the maximum … rate for each data packet class' aspect is explicitly part of the 'means for said router to control the rate of transmission'

limitation in claim 14, whereas it is a broader aspect of the entire claim in claim 3, and is rejected for the same reasons provided for the claim 3 rejection.

As per claim 6, this claim is a narrower router versus a host receiving, and transmission versus processing rate variation of claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection (i.e., the packet communications network includes intermediate congestion control on a "hop by hop" (col. 1, lines 27-40) basis which broadly defined clearly encompasses network routers. Further, (col. 6, lines 2-4, "Such routing decisions…response to information in the header of the data packet.") determining the path by which the data arrives at the receiver is suggested by the fact that the header contains source / destination (IP) network addressing information which clearly constitutes routing (path) information (a router implemented function)).

As per claim 12, this claim is the method claim for the means plus function claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection.

As per claim 18, this claim is a variation on claim 6 above, insofar as the '… so that the rate of data packet transmissions … kept below the maximum … rate for each data packet class' aspect is explicitly part of the 'means for said router to control the rate of transmission' limitation in claim 18, whereas it is a broader aspect of the entire claim in claim 6, and is rejected for the same reasons provided for the claim 6 rejection.

Response to Arguments

9. As per applicant's argument concerning the lack of teaching by Chang et al of path detection, data mark detection, and classification insofar an a wanted and unwanted classes are established, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive.

At the very least, the path and associated data mark detection limitation is broadly claimed such that the effective path detection only deals with path detection 1 network node backwards (i.e., see claim 1 rejection above). Further, the 'classification' aspect limitation claimed is likewise, as broadly interpreted by the examiner, insofar as a 'wanted and unwanted' classification is established, not patently distinct (i.e., again, see the claim 1 rejection above) and the Chang et al reference would therefore be applicable in the rejection, collectively encompassing the said claim limitations in their entirety.

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

11. The examiner suggests for the sake of moving prosecution forward that the applicant direct the amendment of claim limitations towards the specifics of the 'path determination' aspects, insofar as those specifics that differentiate the inventive concept aspects concerning path determination farther back/more comprehensively, than a single network node backwards (i.e., not just from the host to the previous router back), such that simple packet header protocol aspects (i.e., source/destination address information per se) generally involved in the reference and possible related art, would therefore not necessarily apply.

12. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid, can be reached at (571) 272-4063. The Fax number for the organization where this application 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. For more 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).

Ronald Baum

Patent Examiner

/R. B./

Examiner, Art Unit 2139

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10841064	COHEN, DONALD N.
	Examiner	Art Unit
	RONALD BAUM	2139

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/25/2007	06/04/2008							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10841064	COHEN, DONALD N.
	Examiner	Art Unit
	RONALD BAUM	2139

SEARCHED			
Class	Subclass	Date	Examiner
726	22	6/4/08	rjb

SEARCH NOTES		
Search Notes	Date	Examiner
inventor search	6/4/08	rjb
Google(npl):packet flooding denial packet rate router classification	6/4/08	rjb
class 709,713,726,370,380 with text patent search: see attached EAST search history	6/4/08	rjb
discuss with C. Laforgia	6/4/08	rjb

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"6789190".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/06/04 14:14
L2	160	(726/22.ccls.) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/06/04 16:03
L3	0	(726/22.ccls.) and (packet adj3 flow adj2 (control or allocat$ or congest$ or ((high or large) adj1 (traffic or through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/06/04 16:03
L4	2	("726"/$.ccls.) and (packet adj3 flow adj2 (control or allocat$ or congest$ or ((high or large) adj1 (traffic or through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/06/04 16:04
L5	145	("370"/$.ccls. "380"/$.ccls. "709"/$.ccls. "713"/$.ccls. "726"/$.ccls.) and (packet adj3 flow adj2 (augment$ managem$ control allocat$ congest$ ((high large overflow ascend$ expand$) adj1 (traffic through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/06/04 16:08
L6	62	("370"/$.ccls. "380"/$.ccls. "709"/$.ccls. "713"/$.ccls. "726"/$.ccls.) and (packet adj1 flow adj2 (augment$ managem$ control allocat$ congest$ ((high large overflow ascend$ expand$) adj1 (traffic through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/06/04 16:09

S1	2070	713/201.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:35
S2	3	713/201.ccls. and packet with flooding and router	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:56
S3	3	713/201.ccls. and packet with flooding and router	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:56
S4	94	packet with flooding and router	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 16:03
S5	5	packet with flooding and router and denial and bandwidth	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:57
S6	495	router and denial and bandwidth	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:59
S7	471	router and denial adj1 service	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:59
S8	329	router and denial adj1 service and bandwidth	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 16:06
S9	64	router and denial and bandwidth and transmi$ adj1 rate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:00
S10	8	router and denial and bandwidth and send$ adj1 rate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:00

S11	982	network same router and flood$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:01
S12	118	network same router and flood$ and defen$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:01
S13	130	router and flood$ and defen$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:01
S14	91	ddos	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:02
S15	30	packet adj1 class$ and denial adj1 service	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:02
S16	6	thrott$ with bandwidth and denial	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:03
S17	8	709/238-244.ccls. and denial and allocate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:05
S18	4	709/238-244.ccls. and flood$ with rate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:07
S19	241	709/238-244.ccls. and transmi$ with rate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:07
S20	126	router with flow adj1 control	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:08

S21	7	packet adj1 flood$ and defense	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:08
S22	446	packet with overload$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:16
S23	50	packet adj2 overload$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:17
S24	96	packet adj1 flood$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:33
S25	568	packet with flow adj2 (control or allocat$) and router$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:34
S26	67	packet with flow adj2 (control or allocat$) and router$ and (defense or denial)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:50
S27	25	router with flow adj2 (control or allocat$) and (defense or denial)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:36
S28	2	"5367523".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:06
S29	2	"5007052".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:09
S30	2	"5699513".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:12

S31	2	"6412000".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:15
S32	2	"5434860".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:17
S33	2	"20020032871".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:19
S34	2	"4817080".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:21
S35	2	"6088804".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:21
S36	10	"5581559".pn. or "6044402".pn. or "5455865".pn. or "5353353".pn. or "5850515".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 15:51
S37	1	("5581559".pn. or "6044402".pn. or "5455865".pn. or "5353353".pn. or "5850515".pn.) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 15:51
S38	4	370/229-240.ccls. and packet with flooding and router	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 16:04
S39	17	370/229-240.ccls. and router and denial adj1 service and bandwidth	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:37
S40	5	370/229-240.ccls. and router and denial adj1 service and bandwidth and firewall	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 16:10

S41	7	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:57
S42	82	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router and denial adj1 service and bandwidth)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:57
S43	0	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial)) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:56
S44	54	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router and denial adj1 service and bandwidth) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:55
S45	1	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router and denial adj1 service and bandwidth) with firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:55
S46	2	(713/201,160.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router and denial adj1 service and bandwidth) with firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:55
S47	0	(713/201,160.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial)) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:56
S48	7	(713/201,160.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:53

S49	32	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:55
S50	444	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (router and denial adj1 service and bandwidth) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:56
S51	34	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (router and denial adj1 service and bandwidth) and firewall$ and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:58
S52	414	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (packet with flow adj2 (control or allocat$ or congest$ or ((high or large) adj1 (traffic or through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 16:02
S53	140	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (packet adj3 flow adj2 (control or allocat$ or congest$ or ((high or large) adj1 (traffic or through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 16:02

6/4/08 4:11:39 PM
C:\Documents and Settings\RBaum\My Documents\EAST\workspaces\10841064.wsp

PTO/SB/30EFS (09-08)
Approved for use through 10/31/2008. OMB 0651-0031
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 contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	10/841,064	Filing Date	2004-05-07	Docket Number (if applicable)	04-165-B	Art Unit	2136
First Named Inventor	Cohen			Examiner Name	Baum		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☐ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No _____

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

PTO/SB/30EFS (09-08)
Approved for use through 10/31/2008. OMB 0651-0031
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 contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/David A. Belasco/	Date (YYYY-MM-DD)	2008-10-16
Name	David A. Belasco	Registration Number	41609

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 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.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT
Docket 04-165-B

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Cohen	Examiner:	Baum
Serial No.:	10/841,064	Group Art Unit:	2136
Filed:	05/07/2004	Confirmation No.:	9716
Title:	PACKET FLOODING DEFENSE SYSTEM		

AMENDMENT B

In response to the Office Action of June 13, 2008, please amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 11 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

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.

2. (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; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer;

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

means for said computer to determine the rate at which data packets of each class are transmitted from a router to said computer;

means for said router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said computer;

means for said router to control the rate of transmission of data packets from said router to said computer; and

means in said computer for keeping the rate of data packet transmissions received at said computer below the maximum acceptable processing rate for each data packet class by said control of the rate of transmission of data packets from said router, and freeing a portion of the network providing data packet transmission to said computer.

3. (previously presented): A packet flooding defense system as described in Claim 2, wherein:

said router receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and said router controls the rate of transmission of each class of data packet to said computer.

4. (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 router into wanted data packets and unwanted data packets;

means for associating a maximum acceptable transmission rate with each class of data packet received at said router;

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

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.

5. (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 first router into wanted data packets and unwanted data packets; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer;

means for associating a maximum acceptable transmission rate with each class of data packet received at said first router;

means for said first router to determine the rate at which data packets of each class are transmitted from a second router to said first router;

means for said second router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said first router;

means for said second router to control the rate of transmission of data packets from said second router to said first router; and

means in said first router for keeping the rate of data packet transmissions received at said first router below the maximum acceptable transmission rate for unwanted data packets by said control of the rate of transmission of data packets from said second router, and freeing a portion of the network providing data packet transmission to said first router.

6. (previously presented): A packet flooding defense system as described in Claim 5, wherein:

said second router receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router controls the rate of transmission of each class of data packet to said first router.

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; 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.

8. (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:

classifying data packets received at a host computer into wanted data packets and unwanted data packets; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer;

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

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

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

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

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

9. (previously presented): A method as described in Claim 8, in which:

said router receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router controls the rate of transmission of each class of data packet to said computer.

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

classifying data packets received at 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 unwanted data packets.

11. (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:

classifying data packets received at a first router into wanted data packets and unwanted data packets; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer;

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

determining by said first router of the rate at which data packets of each class are transmitted from a second router to said first router;

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

controlling by said second router of the rate of transmission of data packets from said second router to said first router so that said rate of transmission is below the maximum acceptable transmission rate for each data packet class; and

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

12. (previously presented): A method as described in Claim 11, in which:

said second router receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router controls the rate of transmission of each class of data packets to said first router.

13. (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 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.

14. (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; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer;

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

means for said computer to determine the rate at which data packets of each class are transmitted from a router to said computer;

means for said router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said computer; and

means for said router to control the rate of transmission of data packets from said router to said computer so that the rate of data packet transmissions received at said computer is kept below the maximum acceptable processing rate for each data packet class; and

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

15. (previously presented): A packet flooding defense system as described in Claim 14, in which:

said router receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said computer; and

said router controls the rate of transmission of each class of data packet to said computer.

16. (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 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;

means for classifying data packets received at said router into wanted data packets and unwanted data packets by path;

means for associating a maximum acceptable transmission rate with each class of data packet received at said router; and

means for said router to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable processing rate.

17. (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 first router into wanted data packets and unwanted data packets; said data packets comprising data packets from all routers in said network via which said data packets are routed to said computer;

means for associating a maximum acceptable transmission rate with each class of data packet received at said first router;

means for said first router to determine the rate at which data packets of each class are transmitted from a second router to said first router;

means for said second router to receive information regarding maximum acceptable transmission rate for data packets being transmitted to said first router; and

means for said second router to control the rate of transmission of data packets from said second router to said first router so that the rate of data packet transmission received at said first router is kept below the maximum acceptable transmission rate for each data packet class; and

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

18. (previously presented): A packet flooding defense system as described in Claim 17, wherein:

said second router receives information regarding maximum acceptable transmission rate for each class of data packet being transmitted to said first router; and

said second router controls the rate of transmission of each class of data packet to said first router.

REMARKS/ARGUMENTS

Claim Rejections - 35 USC § 112

The Applicant thanks the examiner for withdrawing his rejection under 35 U.S.C. 112, second paragraph.

Claim Rejections - 35 USC § 102

The Examiner again rejected claims 1-18 under 35 U.S.C. 102(b) as being anticipated by Chang et al., U.S. Patent 5,367,523.

Response to Arguments

The Examiner fully considered the Applicant's arguments, presented in the response to the first Office Action, and found them not to be persuasive. However, the examiner suggested amending the claims "towards the specifics of the 'path determination' aspects, insofar as those specifics that differentiate the inventive concept aspects concerning path determination farther back/more comprehensively, than a single network node backwards (i.e., not just from the host to the previous router back), such that simple packet header protocol aspects (i.e., source/destination address information per se) generally involved in the reference and possible related art, would therefore not necessarily apply."

The Applicant thanks the Examiner for this suggestion and has so amended the claims. The Applicant also thanks the Examiner for his preliminary review of draft claims via e-mail correspondence.

This Amendment is being submitted with a Request for Continued Examination. A fee of $405 is due with this document. An extension fee of $525 for a small entity is due because this Amendment is being submitted within the second extension month. Both fees will be electronically paid on electronic filing. Reconsideration of this application and its early allowance are respectfully requested in view of the above presented amendments and remarks.

Respectfully submitted,

/David A. Belasco/

David A. Belasco
Applicant's Attorney
Registration No. 41,609

BELASCO JACOBS & TOWNSLEY, LLP
6100 Center Drive, Suite 630
Los Angeles, CA 90045
Phone: (310) 743-1188
Fax: (310) 743-1189

Electronic Patent Application Fee Transmittal

Application Number:	10841064
Filing Date:	07-May-2004
Title of Invention:	Packet flooding defense system
First Named Inventor/Applicant Name:	Donald N. Cohen
Filer:	Norton Russell Townsley
Attorney Docket Number:	04-165-B

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with $0 paid	2252	1	245	245

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for continued examination	2801	1	405	405
		Total in USD ($)		**650**

Electronic Acknowledgement Receipt

EFS ID:	4128768
Application Number:	10841064
International Application Number:	
Confirmation Number:	9716
Title of Invention:	Packet flooding defense system
First Named Inventor/Applicant Name:	Donald N. Cohen
Customer Number:	31718
Filer:	Norton Russell Townsley
Filer Authorized By:	
Attorney Docket Number:	04-165-B
Receipt Date:	16-OCT-2008
Filing Date:	07-MAY-2004
Time Stamp:	17:27:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$650
RAM confirmation Number	2590
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Request for Continued Examination (RCE)	RCEtransmittal.pdf	697118 c65a99e4f5ea4a698b3c283387e0e3677a8c163	no	3
Warnings:					
Information:					
2	Amendment Submitted/Entered with Filing of CPA/RCE	AmendmentB.pdf	94164 76a2a2ed86d128b67f8564a8fca1b796c65a6	no	12
Warnings:					
Information:					
3	Fee Worksheet (PTO-06)	fee-info.pdf	31750 9896ec3db837ea4eb73671c19873c6146c33379	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	823032		

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.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/841,064	05/07/2004	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 10/16/2008	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 18	Minus	** 20	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 12	Minus	***12	= 0	X $110 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/STEFANIE BRYCE/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 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: 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.

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

31718 7590 12/23/2008

BELASCO, JACOBS & TOWNSLEY LLP
HOWARD HUGHES CENTER
6100 CENTER DRIVE
SUITE 630
LOS ANGELES, CA 90045

EXAMINER	
BAUM, RONALD	
ART UNIT	PAPER NUMBER
2439	

DATE MAILED: 12/23/2008

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/841,064	05/07/2004	Donald N. Cohen	04-165-B	9716

TITLE OF INVENTION: PACKET FLOODING DEFENSE SYSTEM

APPL.N. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	03/23/2009

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

Cloudflare, Inc. Exhibit 1003 Page 648

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

31718 7590 12/23/2008

BELASCO, JACOBS & TOWNSLEY LLP
HOWARD HUGHES CENTER
6100 CENTER DRIVE
SUITE 630
LOS ANGELES, CA 90045

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/841,064	05/07/2004	Donald N. Cohen	04-165-B	9716

TITLE OF INVENTION: PACKET FLOODING DEFENSE SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	03/23/2009

EXAMINER	ART UNIT	CLASS-SUBCLASS
BAUM, RONALD	2439	726-022000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 .....
2 .....
3 .....

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies .....

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number ..... (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ..... Date .....

Typed or printed name ..... Registration No. .....

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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.

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.
10/841,064	05/07/2004	Donald N. Cohen	04-165-B	9716

31718 7590 12/23/2008

BELASCO, JACOBS & TOWNSLEY LLP
HOWARD HUGHES CENTER
6100 CENTER DRIVE
SUITE 630
LOS ANGELES, CA 90045

EXAMINER	
BAUM, RONALD	
ART UNIT	PAPER NUMBER
2439	

DATE MAILED: 12/23/2008

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 719 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 719 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

Notice of Allowability	Application No.	Applicant(s)	
	10/841,064	COHEN, DONALD N.	
	Examiner	Art Unit	
	RONALD BAUM	2439	

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

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *16 October 2008*.

2. ☒ The allowed claim(s) is/are *1-18*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Examiner's Statement of Reasons for Allowance

1. Claims 1-18 are allowed over prior art.

2. This action is in reply to applicant's correspondence of 16 October 2008.

3. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

4. As per claims 1, 2, 4, 7, 8, 10, 11, 13, 14, 16 and 17 generally, prior art of record, Chang et al, U.S. Patent 5,367,523, fails to anticipate, disclose, teach or suggest alone, or in combination, at the time of the invention, the features as set forth in the claims in this application as allowed, and not necessarily as summarized and/or characterized by the examiner, whether or not as italicized, as discussed and remarked upon in the response of 16 October 2008 to office action of 13 June 2008.

Specifically, (as per claim 1, for example) prior art dealing with DDoS defense against various attack scenarios (e.g., path identification DDoS defense scheme utilizing a deterministic packet marking scheme allowing a DDoS victim to filter out attack packets via router originated information; Yaar, A., et al, 'StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense', IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 10, OCTOBER 2006, entire document, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01705617), is generally known per se. Nowhere in the prior art is found collectively the *italicized* claim elements (i.e., path information forwarding along the entire path to the victim, said path information encompassing the entire path through the associated routers, and subsequent use of said information to effect filtering via allocation of

packet processing rate), at the ***time*** *of the invention*, serving to patently distinguish the invention from said prior art;

"1. 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"

5. Dependent claims 3, 6, 9, 12, 15 and 18 are allowable by virtue of their dependencies.

Conclusion

6. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand, can be reached at (571) 272-3811. The Fax number for the organization where this application 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. For more 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).

Ronald Baum

Patent Examiner

/R. B./

Examiner, Art Unit 2439

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434

Notice of References Cited	Application/Control No. 10/841,064	Applicant(s)/Patent Under Reexamination COHEN, DONALD N.	
	Examiner RONALD BAUM	Art Unit 2439	Page 1 of 1

U.S. PATENT DOCUMENTS

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

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Yaar, A., et al. 'StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense', IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 10, OCTOBER 2006, entire document, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01705617
	V	
	W	
	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.

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	162	(726/22.ccls.) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/12/17 15:24
L3	62	("370"/$.ccls. "380"/$.ccls. "709"/$.ccls. "713"/$.ccls. "726"/$.ccls.) and (packet adj1 flow adj2 (augment$ managem$ control allocat$ congest$ ((high large overflow ascend$ expand$) adj1 (traffic through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/12/17 15:25
L4	178	(713/201.ccls. 709/238-244.ccls. 370/229-240.ccls.) and (router and denial adj1 service and bandwidth)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/12/17 15:26
L5	10	(713/201.ccls. 709/238-244.ccls. 370/229-240.ccls.) and (router and denial adj1 service and bandwidth) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/12/17 15:26
L6	40	("713"/$.ccls. "709"/$.ccls. "726"/$.ccls.) and (router and denial adj1 service and bandwidth) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/12/17 15:27
L7	48	("713"/$.ccls. "709"/$.ccls. "726"/$.ccls.) and (router$ and ((denial adj1 service) (dos with attack)) and bandwidth) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/12/17 15:28
L8	5	(router$ and ((denial adj1 service) (dos with attack)) and bandwidth).clm.	US-PGPUB	OR	OFF	2008/12/17 15:29
S1	2070	713/201.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:35

S2	3	713/201.ccls. and packet with flooding and router	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:56
S3	3	713/201.ccls. and packet with flooding and router	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:56
S4	94	packet with flooding and router	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 16:03
S5	5	packet with flooding and router and denial and bandwidth	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:57
S6	495	router and denial and bandwidth	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:59
S7	471	router and denial adj1 service	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 11:59
S8	329	router and denial adj1 service and bandwidth	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 16:06
S9	64	router and denial and bandwidth and transmi$ adj1 rate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:00
S10	8	router and denial and bandwidth and send$ adj1 rate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:00
S11	982	network same router and flood$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:01

S12	118	network same router and flood$ and defen$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:01
S13	130	router and flood$ and defen$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:01
S14	91	ddos	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:02
S15	30	packet adj1 class$ and denial adj1 service	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:02
S16	6	thrott$ with bandwidth and denial	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:03
S17	8	709/238-244.ccls. and denial and allocate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:05
S18	4	709/238-244.ccls. and flood$ with rate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:07
S19	241	709/238-244.ccls. and transmi$ with rate	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:07
S20	126	router with flow adj1 control	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:08
S21	7	packet adj1 flood$ and defense	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:08

S22	446	packet with overload$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:16
S23	50	packet adj2 overload$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:17
S24	96	packet adj1 flood$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:33
S25	568	packet with flow adj2 (control or allocat$) and router$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:34
S26	67	packet with flow adj2 (control or allocat$) and router$ and (defense or denial)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 12:50
S27	25	router with flow adj2 (control or allocat$) and (defense or denial)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:36
S28	2	"5367523".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:06
S29	2	"5007052".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:09
S30	2	"5699513".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:12
S31	2	"6412000".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:15

S32	2	"5434860".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:17
S33	2	"20020032871".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:19
S34	2	"4817080".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:21
S35	2	"6088804".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2003/10/23 13:21
S36	10	"5581559".pn. or "6044402".pn. or "5455865".pn. or "5353353".pn. or "5850515".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 15:51
S37	1	("5581559".pn. or "6044402".pn. or "5455865".pn. or "5353353".pn. or "5850515".pn.) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 15:51
S38	4	370/229-240.ccls. and packet with flooding and router	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 16:04
S39	17	370/229-240.ccls. and router and denial adj1 service and bandwidth	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:37
S40	5	370/229-240.ccls. and router and denial adj1 service and bandwidth and firewall	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/02/23 16:10

S41	7	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:57
S42	82	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router and denial adj1 service and bandwidth)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:57
S43	0	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial)) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:56
S44	54	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router and denial adj1 service and bandwidth) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:55
S45	1	(713/201.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router and denial adj1 service and bandwidth) with firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:55
S46	2	(713/201,160.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router and denial adj1 service and bandwidth) with firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:55
S47	0	(713/201,160.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial)) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/06/01 11:56
S48	7	(713/201,160.ccls. or 709/238-244.ccls. or 370/229-240.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:53

S49	32	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (router with flow adj2 (control or allocat$) and (defense or denial))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:55
S50	444	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (router and denial adj1 service and bandwidth) and firewall$	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:56
S51	34	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (router and denial adj1 service and bandwidth) and firewall$ and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 15:58
S52	414	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (packet with flow adj2 (control or allocat$ or congest$ or ((high or large) adj1 (traffic or through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 16:02
S53	140	("370"/$.ccls. or "380"/$.ccls. or "709"/$.ccls. or "713"/$.ccls. or "726"/$.ccls.) and (packet adj3 flow adj2 (control or allocat$ or congest$ or ((high or large) adj1 (traffic or through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/09/25 16:02
S54	2	"6789190".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/06/04 14:14
S55	160	(726/22.ccls.) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/06/04 16:03

S56	0	(726/22.ccls.) and (packet adj3 flow adj2 (control or allocat$ or congest$ or ((high or large) adj1 (traffic or through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/06/04 16:03
S57	2	("726"/$.ccls.) and (packet adj3 flow adj2 (control or allocat$ or congest$ or ((high or large) adj1 (traffic or through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/06/04 16:04
S58	145	("370"/$.ccls. "380"/$.ccls. "709"/$.ccls. "713"/$.ccls. "726"/$.ccls.) and (packet adj3 flow adj2 (augment$ managem$ control allocat$ congest$ ((high large overflow ascend$ expand$) adj1 (traffic through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/06/04 16:08
S59	62	("370"/$.ccls. "380"/$.ccls. "709"/$.ccls. "713"/$.ccls. "726"/$.ccls.) and (packet adj1 flow adj2 (augment$ managem$ control allocat$ congest$ ((high large overflow ascend$ expand$) adj1 (traffic through$))) and router$) and @ad<"20001116"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/06/04 16:09

12/17/08 3:32:41 PM
C:\Documents and Settings\RBaum\My Documents\EAST\workspaces\10841064.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10841064	COHEN, DONALD N.
	Examiner	Art Unit
	RONALD BAUM	2439

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/25/2007	06/04/2008	12/17/2008						
1	1	✓	✓	=						
2	2	✓	✓	=						
3	3	✓	✓	=						
4	4	✓	✓	=						
5	5	✓	✓	=						
6	6	✓	✓	=						
7	7	✓	✓	=						
8	8	✓	✓	=						
9	9	✓	✓	=						
10	10	✓	✓	=						
11	11	✓	✓	=						
12	12	✓	✓	=						
13	13	✓	✓	=						
14	14	✓	✓	=						
15	15	✓	✓	=						
16	16	✓	✓	=						
17	17	✓	✓	=						
18	18	✓	✓	=						

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
10841064	COHEN, DONALD N.
Examiner	**Art Unit**
RONALD BAUM	2439

ORIGINAL		INTERNATIONAL CLASSIFICATION									
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED				
726	22	G	0	6	F	11 / 30 (2006.01.01)	G	0	6	F	11 / 50 (2006.01.01)

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
726	20				
709	235	238	239	240	
370	229	231	235	237	

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	17	17												
2	2	18	18												
3	3														
4	4														
5	5														
6	6														
7	7														
8	8														
9	9														
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
16	16														

/RONALD BAUM/ Examiner.Art Unit 2439	20081217	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	18	
/KAMBIZ ZAND/ Supervisory Patent Examiner.Art Unit 2434	12/17/2008	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10841064	COHEN, DONALD N.
	Examiner	Art Unit
	RONALD BAUM	2439

SEARCHED

Class	Subclass	Date	Examiner
726	22	12/17/08	rjb

SEARCH NOTES

Search Notes	Date	Examiner
inventor search	12/17/08	rjb
Google(npl):"packet flooding" denial packet rate router classification	12/17/08	rjb
class 709,713,726,370,380 with text patent search: see attached EAST search history	12/17/08	rjb
discuss with primary (C. Laforgia)	12/17/08	rjb
claim text interference patent search: see attached EAST search history	12/17/08	rjb

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
none	(router$ and ((denial adj1 service) (dos with attack)) and bandwidth).clm.	12/17/08	rjb

MAR 0 6 2009
PATENT & TRADEMARK OFFICE

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

$1718 7590 12/23/2008

BELASCO, JACOBS & TOWNSLEY LLP
HOWARD HUGHES CENTER
6100 CENTER DRIVE
SUITE 630
LOS ANGELES, CA 90045

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Donna Miller (Depositor's name)
Donna Miller (Signature)
3/6/09 (Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/841,064	05/07/2004	Donald N. Cohen	04-165-B	9716

TITLE OF INVENTION: PACKET FLOODING DEFENSE SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	03/23/2009

EXAMINER	ART UNIT	CLASS-SUBCLASS
BAUM, RONALD	2439	726-022000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 David A. Belasco
2 Belasco Jacobs & Townsley, LLP
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)
☐ A check is enclosed.
☒ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)
☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date 3/6/09

Typed or printed name David A. Belasco Registration No. 41,609

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

03/06/2009 EAREGAY2 00000131 10841064
01 FC:2501 755.00 OP
02 FC:1504 300.00 OP

PAGE 1/2 * RCVD AT 3/6/2009 1:36:32 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/18 * DNIS:2732885 * CSID:310 743 1189 * DURATION (mm-ss):01-06

03/06/2009 EAREGAY2 00000131 10841064
01 FC:2501 755.00 OP
02 FC:1504 300.00 OP

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.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/841,064	04/21/2009	7523497	04-165-B	9716

31718 7590 04/01/2009

BELASCO, JACOBS & TOWNSLEY LLP
HOWARD HUGHES CENTER
6701 CENTER DRIVE
14th Floor
LOS ANGELES, CA 90045

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 719 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Donald N. Cohen, Los Angeles, CA;

506209009 08/18/2020

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT6255749

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT

CONVEYING PARTY DATA

Name	Execution Date
COMPUTING SERVICES SUPPORT SOLUTIONS, INC.	08/12/2020

RECEIVING PARTY DATA

Name:	PACSEC3 LLC
Street Address:	5218 CHANDLER STREET
City:	HOUSTON
State/Country:	TEXAS
Postal Code:	77007

PROPERTY NUMBERS Total: 3

Property Type	Number
Patent Number:	6789190
Patent Number:	7047564
Patent Number:	7523497

CORRESPONDENCE DATA

Fax Number: (713)481-0031

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Phone: 7134810031
Email: carlos@dynaipdeals.com
Correspondent Name: CARLOS GORRICHATEGUI
Address Line 1: 5218 CHANDLER STREET
Address Line 4: HOUSTON, TEXAS 77007

ATTORNEY DOCKET NUMBER:	Q982-DB
NAME OF SUBMITTER:	CARLOS GORRICHATEGUI
SIGNATURE:	/DrCOGIII/
DATE SIGNED:	08/18/2020
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 1
source=Cs3 Inc - PacSec3 LLC Assignment#page1.tif

EXHIBIT B – ASSIGNMENT OF PATENT RIGHTS

This Assignment Agreement (the "Agreement") is made and entered into this 12th day of August 12, 2020 (the "Effective Date"), by Computing Services Support Solutions dba Cs3 Inc., a California S corporation, having an address at 5777 W Century Blvd, Suite 1185, Los Angeles, CA 90045 ("Assignor") and PacSec3 LLC, a Texas limited liability company, having and address at 5218 Chandler Street, Houston, TX, 77007 ("Assignee").

RECITALS

A. Assignor is the owner of:

- the United States Patents set forth on Exhibit A hereto (the "US Patents");
- the non-United States patents set forth on Exhibit B.1 hereto (the "Foreign Patents");
- the United States patent applications set forth on Exhibit B.2 hereto (the "US Patent Applications");
- the United States provisional patent applications set forth on Exhibit B.3 hereto (the "US Provisional Patent Applications"); and/or
- the foreign patent applications set forth on Exhibit B.4 hereto (the "Foreign Patent Applications");

which collectively shall be referred to herein as the "Patents".

B. Assignor and Assignee have agreed by way of a purchase agreement (the "Purchase Agreement") dated April 23rd, 2020 «EFFECTIVE_DATE», by and between Assignor and Assignee, that Assignor shall sell, transfer, and assign and set over unto Assignee and Assignee shall accept, all rights, title and interest in and to the Patents.

AGREEMENT

NOW, THEREFORE, in consideration of the foregoing premises, and the covenants and agreements in this Assignment, Assignor and Assignee agree as follows:

1. Assignor does hereby sell, transfer, convey, assign and deliver to Assignee all of Assignor's right, privilege, title and interest in, to and under the Patents and in the case of patent applications in and to any patents that may issue therefrom, including, in all instances, any counterparts of any of the foregoing in any jurisdiction throughout the world, and any and all divisions, continuations, reissues or reexaminations of any of the foregoing, and, further, all applications for industrial property protection, including without limitation, all applications for patents, utility models, copyright, and designs which may hereafter be filed

Cloudflare, Inc. Exhibit 1003 Page 671

Exhibit 1003

Declaration of Dr. Vijay Madisetti ("Madisetti")

Customer No.: 000027683

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651.5000
Fax [214] 200.0853

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE CENTRAL REEXAMINATION UNIT

UNIFIED PATENTS, LLC

Third Party Requester

DECLARATION OF VIJAY K. MADISETTI, PHD, UNDER 37 C.F.R. § 1.68 IN SUPPORT OF REQUEST FOR *EX PARTE* REEXAMINATION OF U.S. PATENT NO. 7,523,497

Cloudflare, Inc. Exhibit 1003 Page 673

TABLE OF CONTENTS

I. Introduction 5

II. Background and Qualifications 10

III. Summary of My Opinions 17

IV. Level of Ordinary Skill in the Pertinent Art 18

V. Prior Art Printed Publications 20

VI. Claim Construction 22

VII. Understanding of Patent Law 23

VIII. The '497 Patent 27

A. Summary of Alleged Invention 27

B. Embodiments of the '497 Patent 30

C. Claims 7 and 10 35

D. Packet Marking 37

E. Prosecution History 38

IX. Overview of Prior Art 43

A. Packet Flooding and Denial of Service Attacks 44

B. Packet Marking was Well-Known in the Art 47

C. Overview of *Savage* 49

D. Overview of *Maher* 51

E. Overview of Schuba 54

F. Proposed Rejection #1: Motivation to Combine *Savage* with *Maher* and *Schuba* 57

1. A POSITA would have been motivated to modify *Savage* to incorporate *Maher*'s conventional network implementation details 58

2. A POSITA would have been motivated to utilize *Savage*'s packet marking technique to determine the path of a packet including all routers between an attacker and a victim 61

3. 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 64

G. Proposed Rejection #2: Motivation to Combine *Maher* with *Savage* and *Schuba* 67

1. 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 68

2. 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 74

X. Detailed Invalidity Analysis 80

A. Proposed Rejection #1: Claim 7 would have been obvious over *Savage* in view of *Maher* and further in view of *Schuba*. 80

B. Proposed Rejection #2: Claim 10 would have been obvious over *Maher* in view of *Savage* and further in view of *Schuba*. 111

C. Proposed Rejection #1 (Claims 13 and 1): Claims 13 and 1 would have been obvious over *Savage* in view of *Maher* and further in view of *Schuba*. 121

1. Overview of Claim 13 121

2. Overview of Claim 1 130

D. Proposed Rejection #2 (Claims 16 and 4): Claims 16 and 4 would have been obvious over *Maher* in view of *Savage* and *Schuba* 137

1. Overview of Claim 16 137

2. Overview of Claim 4 142

XI. Availability for cross-examination 149

XIII. Conclusion 150

Declaration of Dr. Vijay K. Madisetti Under 37 C.F.R. § 1.68 in Support of Request for *Ex Parte* Reexamination of U.S. Patent No. 7,523,497

I, Vijay K. Madisetti, do hereby declare as follows:

I. INTRODUCTION

1. I have been retained by counsel for Unified Patents, LLC ("Unified") as an independent expert witness in support of the above-captioned Request for *Ex Parte* Reexamination ("Request") of U.S. Patent No. 7,523,497 ("the '497 patent"). I am being compensated at my usual and customary rate for the time I spend in connection with this reexamination proceeding. My compensation is not affected by the outcome of this reexamination proceeding.

2. I have been asked to provide my opinions regarding whether claims 7 and 10 (each a "Challenged Claim" and collectively the "Challenged Claims") of the '497 Patent are invalid as they would have been obvious to a person having ordinary skill in the art ("POSITA") as of the earliest claimed priority date. It is my opinion that all of the Challenged Claims would have been obvious to a POSITA after reviewing the prior art discussed below.

3. In preparing this Declaration, I have reviewed:

a) EX1001, the '497 Patent;

b) EX1002, the file history of the '497 Patent;

c) the prior art references discussed below:

- 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 7,0858,974 by Robert D. Maher, III ("Maher");
- EX1007, U.S. Patent 6,725,378 by Christoph L. Schuba et al. ("Schuba");

d) other documents listed below:

- EX1008, U.S. Patent 5,367,523 by Rong-Feng Chang et al. ("Chang");
- 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");

- EX1017, Program of ACM SIGCOMM 2000 Conference in Stockholm, Sweden, August 28, 2000 to September 1, 2000[1];
- 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[2];
- EX1022, Association for Computing Machinery (ACM), "About the ACM Organization"[3];
- EX1023, "ACM SIGCOMM: Welcome" page[4];
- EX1027, U.S. Patent 6,789,190 by Donald N. Cohen;
- EX1028, the file history of U.S. Patent 6,789,190;

---

[1] EX1017 is available at http://conferences.sigcomm.org/sigcomm/2000/, by clicking on the link "here" at "Aug 2000: The final program is available, check out here." The link "here" is http://conferences.sigcomm.org/sigcomm/2000/conf/sigcomm2000-final-prog.pdf.

[2] EX1018 is available at https://web.archive.org/web/20000820231540/http://www.acm.org/sigcomm/sigcomm2000/conf/techprog.htm.

[3] EX1022 is available at https://www.acm.org/about-acm/about-the-acm-organization.

[4] EX1023 is available at http://www.sigcomm.org/.

- EX1036, K. Ramakrishnan et al., "A Proposal to add Explicit Congestion Notification (ECN) to IP," Network Working Group Request for Comments: 2481 (Jan. 1999) ("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) ("RFC 2474");
- EX1038, S. Blake et al., "An Architecture for Differentiated Services," Network Working Group Request for Comments: 2475 (Dec. 1998) ("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");
- EX1044, "Internet Protocol – DARPA Internet Program Protocol Specification," IETF Network Working Group, Request for Comments: 791 (J. Postel ed., Sept. 1981) ("RFC 791"); and

- EX1045, T. Socolofsky, "A TCP/IP Tutorial," Network Working Group Request for Comments 1180 (Jan. 1991) ("RFC 1180").

e) any other documents cited below.

4. I understand that the '497 patent issued on April 21, 2009, from U.S. Patent Application No. 10/841,064, filed on May 7, 2004. I understand that the '497 patent claims priority back to U.S. Patent No. 6,789,190, which was filed as U.S. Application No. 09/715,813 on November 16, 2000. The face of the '497 patent lists Donald N. Cohen as the purported inventor. I have been informed that PacSec3, LLC is the current assignee of the '497 patent.

5. In forming the opinions expressed in this Declaration, I relied upon my education and experience in the relevant field of art and have considered the viewpoint of a Person of Ordinary Skill in the Art (POSITA), as of September 20, 2001. I have also considered:

a) the documents listed above,

b) any additional documents and references cited in the analysis below,

c) the relevant legal standards, including the standard for obviousness, and

d) my knowledge and experience based upon my work in this area as described below.

II. BACKGROUND AND QUALIFICATIONS

6. My qualifications are set forth in my *curriculum vitae*, a copy of which is included as Exhibit 1004 (EX1004). As set forth in my curriculum vitae:

7. I obtained my Ph.D. in Electrical Engineering and Computer Science at the University of California, Berkeley, in 1989. I received the Demetri Angelakos Outstanding Graduate Student Award from the University of California, Berkeley and the IEEE/ACM Ira M. Kay Memorial Paper Prize in 1989.

8. I joined Georgia Tech in the Fall of 1989 and am now a Professor in Electrical and Computer Engineering. I have been active in the areas of IP (Internet Protocol) networking, wireless communications, digital signal processing, integrated circuit design (analog & digital), software engineering, system-level design methodologies and tools, and software systems. I have been the principal investigator ("PI") or co-PI in several active research programs in these areas, including DARPA's Rapid Prototyping of Application Specific Signal Processors, the State of Georgia's Yamacraw Initiative, the United States Army's Federated Sensors Laboratory Program, and the United States Air Force Electronics Parts Obsolescence Initiative. I have received an IBM Faculty Award and the NSF's Research Initiation Award. I have been awarded the 2006 Frederick Emmons

Terman Medal by the American Society of Engineering Education for contributions to Electrical Engineering, including authoring a widely-used textbook in the design of VLSI digital signal processors.

9. I have developed and taught undergraduate and graduate courses in hardware and software design for computer systems and software (e.g., IP networking), signal processing and wireless communication circuits at Georgia Tech for the past twenty years. I graduated more than 20 Ph.D. students that now work as professors or in technical positions around the world.

10. I have been an active consultant to industry and various research laboratories (including Massachusetts Institute of Technology ("MIT") Lincoln Labs and Johns Hopkins University Applied Physics Laboratory). I have founded three companies in the areas of IP networking, embedded software, military chipsets involving imaging technology, and wireless communications. I have supervised the Ph.D. dissertations of over twenty engineers in the areas of computer engineering, signal processing, communications, rapid prototyping, and system-level design methodology, five of which have resulted in thesis prizes or paper awards.

11. My consulting work for MIT Lincoln Labs involved high resolution imaging for defense applications, where I worked in the area of prototyping complex and specialized computing systems. My consulting work for Johns Hopkins Applied Physics Lab ("APL") mainly involved localization of objects in image fields, where

I worked on identifying targets in video and other sensor fields and identifying computer architectures and circuits for power and space-efficient designs.

12. I have developed wireless baseband and protocol stack software and assembly code for a leading telecommunications handset vendor that focused on efficient realization of speech codecs and echo-cancellation.

13. The first of the companies I founded, VP Technologies, offers products in the area of semiconductor integrated circuits, including building computing systems for helicopter imaging systems for the United States Air Force. I remain a director of VP Technologies. The second of these companies, Soft Networks, LLC, offers software for multimedia and wireless computing and network platforms, including the development of a set-top box for Intel that decodes MPEG-2 video streams and imaging codes for multimedia phones. The technology involved with the design, development, and implementation of the Intel set-top box included parsing the bit streams, decoding communications protocols, extracting image and video data, and then processing for subsequent display or storage over IP networks. The third of these companies, Elastic Video, uses region-of-interest based video encoding or decoding for capturing high quality video at very low bit rates for distribution over IP networks, with primary application for wireless video systems.

14. I have been active in the area of IP networking and network data transmission, including wireline and wireless networking. Some of my publications

in this area around the priority date of the '497 patent include "Adaptive Mobility Management in Wireless Networks," Electronics Letters, Vol. 34, No. 15, July 23, 1998, pp. 1453-1455; "A Transport Layer Technology for Improving the QoS of Networked Multimedia Applications," IETF Internet-Draft, July 25, 2002;[5] and "Voice & Video Over Mobile IP Networks, IETF Internet-Draft, November 20, 2002.[6]

15. I have authored or co-authored several books, including VLSI Digital Signal Processors (IEEE Press 1995) and the Digital Signal Processing Handbook (CRC Press, 1998). I am Editor of the three-volume DSP Handbook set (Volume 1: Digital Signal Processing Fundamentals; Volume 2: Video, Speech, and Audio Signal Processing and Associated Standards; and Volume 3: Wireless, Networking, Radar, Sensory Array Processing, and Nonlinear Signal Processing), which was published in 2010 by CRC Press in Boca Raton, Florida.

16. Additional representative peer-reviewed publications in the area of IP networking and network data transmission include the following (i) Argyriou, A. and Madisetti, V.K., "Bandwidth aggregation with SCTP," *GLOBECOM '03, IEEE Global Telecommunications Conference*, San Francisco, CA, USA, 2003, vol. 7, pp.

[5] Available at https://tools.ietf.org/html/draft-madisetti-argyriou-qos-sctp-00.
[6] Available at https://tools.ietf.org/html/draft-madisetti-argyriou-voice-video-mip-00.

3716-3721; (ii) Argyriou, A. and Madisetti, V.K., "Realizing load-balancing in ad-hoc networks with a transport layer protocol," *2004 IEEE Wireless Communications and Networking Conference*, Atlanta, GA, USA, 2004, Vol. 3, pp. 1897-1902; (iii) Argyriou, A. and Madisetti, V.K., "Performance evaluation and optimization of SCTP in wireless ad-hoc networks," *28th Annual IEEE International Conference on Local Computer Networks*, 2003. LCN '03. Proceedings., Bonn/Konigswinter, Germany, 2003, pp. 317-318; and (iv) Khan, M.H. and Madisetti, V.K., "System design and re-engineering through virtual prototyping: a temporal model-based approach," *Conference Record of Thirty-Second Asilomar Conference on Signals, Systems and Computers* (Cat. No.98CH36284), Pacific Grove, CA, USA, 1998, Vol. 2, pp. 1720-1724.

17. I am knowledgeable and familiar with standards related to IP networking and network data transmission, including the TCP/IP (Transmission Control Protocol and Internet Protocol) protocol as defined in Request for Comments (RFC) 793 (EX1044) and RFC 1180 (EX1045). I am also familiar with common network infrastructure devices such as routers, gateways, and source and destination host computers, and how such devices utilize the TCP/IP protocol with Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) addressing. I am a member of the Computer Systems and Software, and Digital Signal Processing Technical Groups at Georgia Tech, and teach classes in these technical

areas. One of my primary research interests is in networking, including wireline and wireless networking.

18. I have designed several specialized computer and communication systems over the past two decades at Georgia Tech for tasks including wireless audio and video processing and protocol processing for portable platforms, like cell phones and Person Digital Assistants. I have worked on designing systems that are efficient from a performance, size, weight, area, and thermal point of view. I have developed courses and classes for the industry on these topics, and many of my lectures in advanced computer system design, developed under the sponsorship of the United States Department of Defense in the late 1990s, are available for educational use at http://www.eda.org/rassp. These lectures have been used by several U.S. and international universities as part of their course work. Some of my recent publications in the area of design of wireless communications systems and associated protocols are listed in EX1004.

19. In conjunction with a leading telecom vendor in Asia, through a joint venture called Soft Networks ("SN"), LLC in Atlanta in the late 1990s and early 2000s, I collaborated with a team of engineers to support mobile and wireless services offerings in India. These involved the design and development of micropayment services for mobile phones, design of smartphones, soft switches, and

telecom customer billing and fraud detection algorithms that included establishment of secure sessions and privileged access to customer account and billing data.

20. I have been elected a Fellow of the IEEE. The Fellow is the highest grade of membership of the IEEE, a world professional body consisting of over 300,000 electrical and electronics engineers, with only one-tenth of one percent (0.1%) of the IEEE membership being elected to the Fellow grade each year. Election to Fellow is based upon votes cast by existing Fellows in IEEE.

21. I have also been awarded the 2006 Frederick Emmons Terman Medal by the American Society of Engineering Education for contributions to Electrical Engineering, including authoring a widely used textbook in the design of VLSI digital signal processors. I was awarded the VHDL International Best PhD Dissertation Advisor Award in 1997 and the NSF Research Initiation Award in 1990. I was Technical Program Chair for both the IEEE MASCOTS in 1994 and the IEEE Workshop on Parallel and Distributed Simulation in 1990. In 1989 I was recognized with the Ira Kay IEEE/ACM Best Paper Award for Best Paper presented at the IEEE Annual Simulation Symposium.

22. In view of the above and my curriculum vitae (EX1004), I had (i) a Ph.D. degree in electrical engineering; (ii) over ten years lecturing at the college level on the topic of electrical engineering, including IP networking and network data transmission; and (iii) several years of experience in the design and

development of IP networking and network data transmission prior to the earliest priority date of the '497 patent. Thus, as of the earliest possible priority date of the '497 patent (i.e., November 16, 2000), I was at least a person of ordinary skill in the art of the '497 patent (Section IV, *infra*), and I had direct personal knowledge of the technologies involved in the '497 patent. When I refer to the "priority date of the '497 patent," I am referring to November 16, 2000.

III. SUMMARY OF MY OPINIONS

23. In my opinion, claims 7, 10, 13, 16, 1 and 4 of the '497 patent are unpatentable. My opinions are based on my expertise in the technology of the '497 patent as of the priority date of the '497 patent, its file history, and the prior art discussed in my Declaration and the Request. In this Declaration, I first analyze claims 7 and 10. Claims 7 and 10 are "method" claims. Claims 13, 16, 1, and 4 are "system" claims. Claims 13 and 1 are substantially similar to claim 7. Claims 16 and 4 are substantially similar to claim 10.

24. I reviewed and contributed to the Request's explanation as to why claims 7, 10, 13, 16, 1 and 4 are unpatentable. The Request's explanation as to why these claims are unpatentable reflects my understanding, and I incorporate it in Section X below.

25. In Section VIII below, I provide an explanation of the '497 patent as well as the alleged inventions of claims 7 and 10. In Section IX below, I provide an

overview of the prior art, including why a POSITA would have been motivated to combine the prior art based on the teachings of the prior art. In Section X below, I also explore how claims 13 and 1 differ from claim 7, and how claims 16 and 4 differ from claim 10. My analysis of claims 13, 1, 16 and 4 follows my analysis of claims 7 and 10 in Section X below.

IV. LEVEL OF ORDINARY SKILL IN THE PERTINENT ART

26. I understand that the level of ordinary skill may be reflected by the prior art of record, and that a POSITA to which the claimed subject matter pertains would have the capability of understanding the scientific and engineering principles applicable to the pertinent art. I understand that one of ordinary skill in the art has ordinary creativity and is not a robot.

27. I understand there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and experience of persons working in the field at the time of the invention; (2) the sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems. There are likely a wide range of educational backgrounds in the technology fields pertinent to the '497 patent. The concepts disclosed in the '497 patent are relatively simple and would have been covered, for example, by an undergraduate-level course on network data transmission, including computer networking and/or IP networking.

28. I am very familiar with the knowledge and capabilities that a person of ordinary skill in the arts of network data transmission would have possessed in November 2000. Specifically, my experience in the industry, with colleagues from academia, with graduate students whose work I supervised, and with engineers practicing in the industry during the relevant timeframe allowed me to become personally familiar with the knowledge and capabilities of a person of ordinary skill in the areas of network data transmission. Unless otherwise stated, my testimony below refers to the knowledge of one of ordinary skill in the art in the field of wireless communications at the time of the November 16, 2000, the priority date of the '497 patent.

29. In my opinion, the level of a person of ordinary skill in the art needed to have the capability of understanding of network data transmission in the '497 patent is a bachelor's degree in electrical engineering, computer engineering, computer science, physics, or a related subject, and one to two years of work experience in network data transmission. Less experience is necessary with additional education (e.g., a Master's degree), and likewise, less education is necessary with additional work experience (e.g., 5–6 years). Such academic and industry experience would be necessary to appreciate what was obvious and/or anticipated in the industry and what a person of ordinary skill in the art would have thought and understood at the time. I believe I possess such experience and

knowledge, and am qualified to opine on the '497 patent from the perspective of a person of ordinary skill in the art.

30. For purposes of this Declaration, in general, and unless otherwise noted, my testimony below refers to the knowledge of one of ordinary skill in the art during the time period around the earliest claimed priority date of the '497 patent. I would have been a person with at least ordinary skill in the art at that time.

V. PRIOR ART PRINTED PUBLICATIONS

31. The Association for Computing Machinery (ACM) is (and has been since well before November 2000) a well-known technical professional organization. ACM has "nearly 100,000 members" worldwide including "educators, researchers, and professionals," as well as "undergraduate and graduate members." EX1022, 1; EX1023, 1. ACM indicates that it is "the world's largest computing society." EX1022, 1. ACM is "a leading global source for scientific information," and "promotes research and innovation through its journals, magazines, and the proceedings of more than 170 annual conferences and symposia." EX1022, 3. A POSITA in the relevant time frame would have frequently reviewed ACM publications and attended ACM conferences for information on relevant technologies, such as computer networking and network data transmission. I have been an ACM member for more than two decades. I have also published articles through ACM: (1) Vijay Madisetti et al., "Efficient distributed simulation," *ACM*

Simulation Digest, Mar. 1989;[7] and (2) Vijay Madisetti et al., "Synchronization mechanisms for distributed event-driven computation," *ACM Transactions on Modeling and Computer Simulation*, Jan. 1992.[8]

32. ACM has several special interest groups (SIG), including the Special Interest Group on Data Communication (SIGCOMM). EX1022, 1; EX1023, 1; EX1024, 1. SIGCOMM members, which include "scientists, engineers, educators and students," "study all aspects of computer communications and networks." EX1023, 1. SIGCOMM members "are particularly interested in the systems engineering and architectural questions surrounding computer communication." EX1023, 1. SIGCOMM has an annual conference in various locations throughout the world. EX1023, 1 ("The annual SIGCOMM Conference, our flagship conference."); EX1024, 1-2 (identifying years and locations of annual SIGCOMM Conference). The SIGCOMM conference has occurred annually beginning in 1998 and continues through this year. EX1024, 1-2. The annual SIGCOMM Conference seeks the submission of papers "describing significant research contributions to the field of computer and data computer networks.," including "submissions on network

[7] Available at https://dl.acm.org/doi/10.1145/66488.66489.

[8] Available at https://dl.acm.org/doi/abs/10.1145/132277.132279.

architecture, design, implementation, operations, analysis, measurement, and simulation." EX1024, 1.

33. According to the program of the ACM SIGCOMM 2000 Conference, *Savage* (EX1005) was presented on September 1, 2000 (Session 8) at the ACM SIGCOMM 2000 Conference in Stockholm, Sweden. EX1017, 2 (conference program); EX1018, 2 (Internet Archive version of online conference program).

34. A POSITA in November 2000 would have been aware of the ACM SIGCOMM conference, and the publications produced by ACM and SIGCOMM. As a POSITA in network data transmission, I would regularly review ACM conference papers, and the publications of ACM, including the *Computer Communication Review*, which was (and still is) a publication of all papers presented at ACM SIGCOMM conferences. See EX1023, 1 (identifying *Computer Communication Review* as one of ACM SIGCOMM's publications).

VI. CLAIM CONSTRUCTION

35. It is my understanding that in order to properly evaluate the '497 patent, the terms of the claims must first be interpreted. It is my understanding that the claims are to be construed according to their broadest reasonable interpretation in light of the specification.

36. Based upon my review of the intrinsic record and my experience in network data transmission, I agree with the position taken in the Request for *Ex*

Parte Reexamination that a POSITA would apply the ordinary and customer meaning to all terms in the challenged claims, such that no specific claim construction is necessary. A POSITA would understand all terms in claims 7 and 10 of the '497 patent according to their ordinary and customary meaning.

VII. UNDERSTANDING OF PATENT LAW

37. I am not an attorney. For the purposes of this declaration, I have been informed about certain aspects of the law that are relevant to my opinions. My understanding of the law was provided to me by Unified's attorneys.

38. I understand that prior art to the '497 patent includes patents and printed publications in the relevant art that predate the priority date of the '497 patent. For purposes of this Declaration, I have applied the date of November 16, 2000, the filing date of U.S. Patent No. 6,789,190 to which the '497 patent claims priority, as the priority date.

39. I have been asked to provide my opinions regarding whether claims 7 and 10 (the "Challenged Claims") of the '497 patent would have been anticipated by the prior art or would have been obvious to a POSITA at the time of the alleged invention in light of the prior art.

40. It is my understanding that, to anticipate a claim under 35 U.S.C. § 102, a reference must disclose each and every element of the claim.

41. I understand that a claim is also unpatentable if it would have been obvious. Obviousness of a claim requires that the claim would have been obvious from the perspective of a POSITA at the time the alleged invention was made. I understand that a claim could have been obvious from a single prior art reference or from a combination of two or more prior art references.

42. I understand that an obviousness analysis requires an understanding of the scope and content of the prior art, any differences between the alleged invention and the prior art, and the level of ordinary skill in evaluating the pertinent art.

43. I further understand that a claim would have been obvious if it unites old elements with no change to their respective functions, or alters prior art by mere substitution of one element for another known in the field and that combination yields predictable results. Also, I understand that obviousness does not require physical combination/bodily incorporation, but rather consideration of what the combined teachings would have suggested to persons of ordinary skill in the art at the time of the alleged invention. I understand that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.

44. As above, I understand that a claim would have been obvious if it unites old elements with no change to their respective functions, or alters prior art by mere substitution of one element for another known in the field and that combination

yields predictable results. While it may be helpful to identify a reason for this combination, I understand that there is no rigid requirement of finding an express teaching, suggestion, or motivation to combine within the references. When a product is available, design incentives and other market forces can prompt variations of it, either in the same field or different one. If a POSITA can implement a predictable variation, obviousness likely bars its patentability. For the same reason, if a technique has been used to improve one device and a POSITA would recognize that it would improve similar devices in the same way, using the technique would have been obvious. I understand that a claim would have been obvious if common sense directs one to combine multiple prior art references or add missing features to reproduce the alleged invention recited in the claims.

45. I further understand that certain factors may support or rebut the obviousness of a claim. I understand that such secondary considerations include, among other things, commercial success of the patented invention, skepticism of those having ordinary skill in the art at the time of invention, unexpected results of the invention, any long-felt but unsolved need in the art that was satisfied by the alleged invention, the failure of others to make the alleged invention, praise of the alleged invention by those having ordinary skill in the art, and copying of the alleged invention by others in the field. I understand that there must be a nexus—a connection—between any such secondary considerations and the alleged invention.

I also understand that contemporaneous and independent invention by others is a secondary consideration tending to show obviousness.

46. I am not aware of any allegations by the named inventor of the '497 patent or any assignee of the '497 patent that any secondary considerations are relevant to the obviousness analysis of any Challenged Claim of the '497 patent.

47. I understand that in considering obviousness, it is important not to determine obviousness using the benefit of hindsight derived from the patent being considered.

48. I understand that other challenges to the validity of a patent, including patent ineligibility, enablement, written description, and definiteness, cannot be raised in an ex parte reexamination proceeding before the U.S. Patent and Trademark Office to challenge the validity of the '497 patent. Accordingly, I did not consider those other challenges.

49. I understand that Unified, as the Third Party Requester, has the burden of showing that the prior art presents a substantial new question of patentability.

50. I have been informed that the references that I rely on in support of the proposed rejections below (*Savage* (EX1005), *Maher* (EX1006), and *Schuba* (EX1007) were not of record during prosecution of the '497 patent).

51. The analysis in this declaration is in accordance with the above-stated legal principles.

VIII. THE '497 PATENT[9]

52. The '497 patent is titled "Packet Flooding Defense System." 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, Abstract ("The invention prevents 'packet flooding,' where an attacker uses up all available bandwidth to a victim with useless data.").

A. Summary of Alleged Invention

53. The '497 patent states that its "primary objective…is to defend against 'packet flooding attacks.'" EX1001, 2:6-7. As described above, the '497 patent explains that in a packet flooding attack, "an attacker tries to use up all the bandwidth to the victim by sending data of little or no value (at least to the victim), thereby making more valuable communication with the victim slow or unreliable." EX1001, 2:7-10.

---

[9] 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*.

54. 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" (e.g., a website hosted by a server), in order 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 (e.g., a server hosting a website). EX1001, 2:54-55, 2:32-36, 3:4-6. The '497 patent describes that "[i]n this invention a path (which is not controlled by the attacker) is used to determine the actual direction of the packet flow towards the victim. Bandwidth is allocated based upon path (which is done via packet marks provided by routers leading up to the victim)." EX1001, 3:62-66.

55. In addition to permitting the source of the attack to be determined, the '497 patent explains that in its packet flooding defense technique, "routers will limit the rate at which they forward packets to places that so request" to assist in "limiting the bandwidth used by 'unwanted' packets." EX1001, 3:4-8. Some embodiments of the '497 patent thus classify packets into "wanted packets" and "unwanted packets." EX1001, 3:6-8, 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, 6:46-51.

56. The '497 patent does not define a specific procedure to determine how packets are determined to be "wanted data packets" or "unwanted data packets." Rather, the '497 patent explains that packets are determined to be "wanted packets" or "unwanted packets" based on whether the packets are expected to be received:

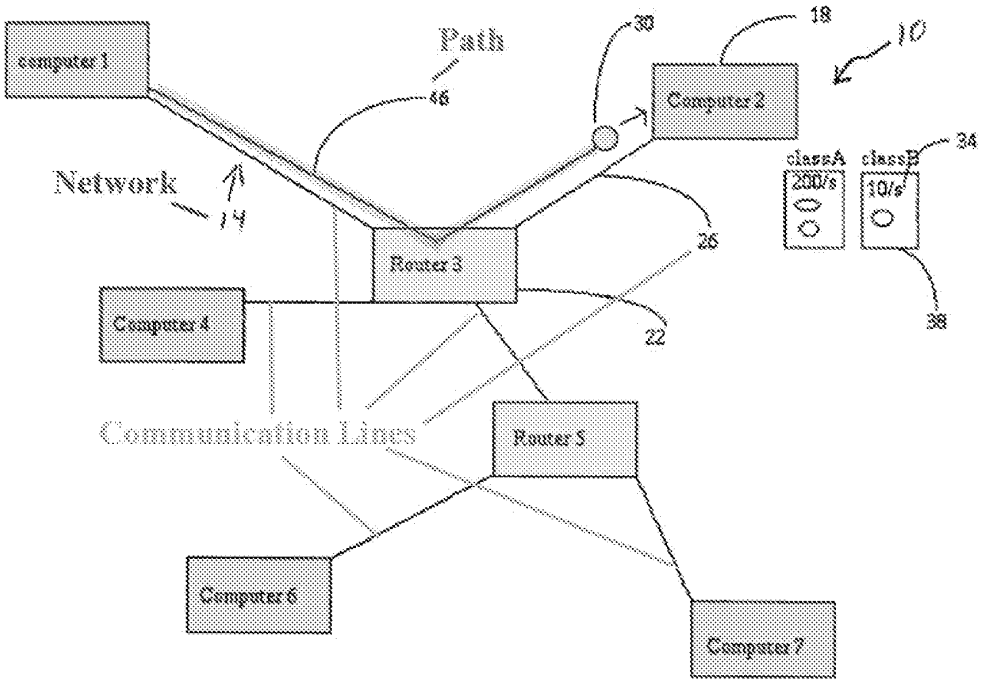
> [T]he distinction between "wanted" and "unwanted" packets plays an important role in "reasonable" allocation [of processing rate]. For a site there are normally some packets (in fact, the great majority) that are expected in a very strong sense. It is reasonable to process these at the highest possible 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).

EX1001, 3:13-23. Thus, the '497 patent classifies packets based on whether they are expected to be received. If a packet is expected to be received, then it is a "wanted data packet." EX1001, 3:15-18. On the other hand, if a packet is unexpected, it is "not exactly unwanted," but is processed at a limited rate. EX1001, 3:18-23. Based on this disclosure, "unwanted data packets" are not prevented from reaching a destination host computer, but are rather processed at a "limited rate." *Id.* The '497 patent explains that the processing or transmission rate for unwanted packets can then be reduced. EX1001, 6:23-25, 6:59-63.

B. Embodiments of the '497 Patent

57. Figure 1 of the '497 patent below discloses a packet flooding defense system 10 for a network 14 that includes a plurality of host computers (computers 1, 2, 4, 6 and 7), routers 22 (routers 3 and 5), communication lines 26, and transmitted data packets 30. EX1001, 6:26-29. In Figure 1, computer 18 (computer 2) receives data packets 30 from computer 1 via router 3.

Figure 1



EX1001, Fig. 1 (annotated)

58. With reference to Figure 1 above, the '497 patent explains that:

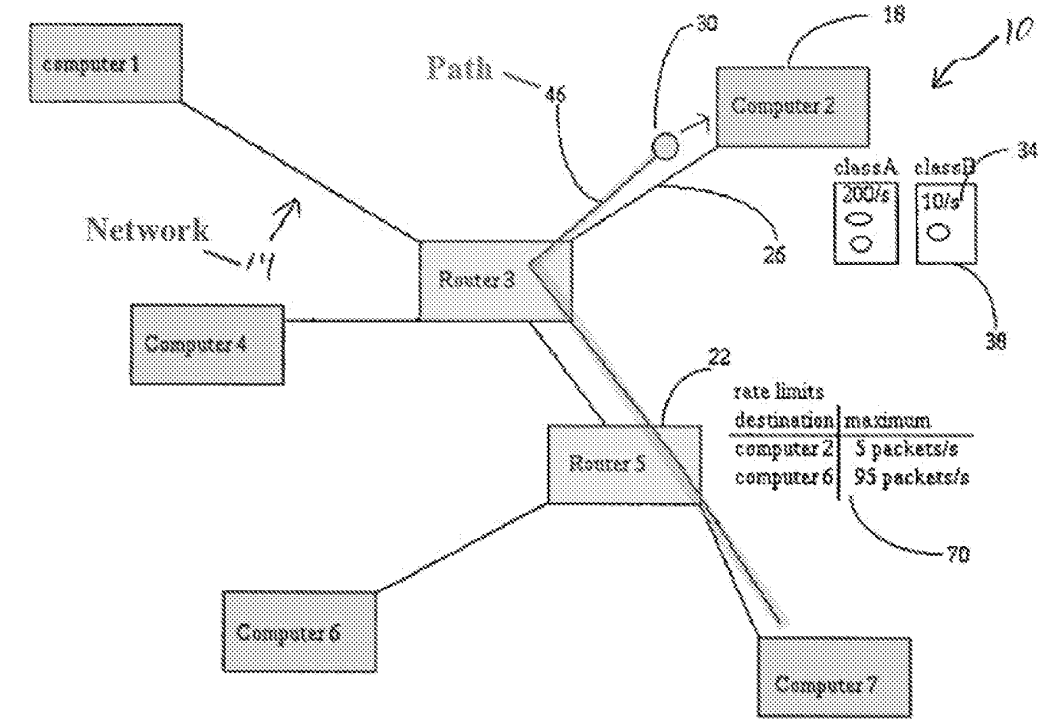
Means are provided for classifying data packets 30 received at a host computer 18 as are means for associating a maximum acceptable

> processing rate 34 with each class 38 of data packet 30 received at the computer 18. Means are also provided for the computer 18 to find information for packets 30 it receives regarding the path 46 by which the packets 30 came to the computer 18. Thus, the computer 18 can use the information to allocate the processing rate for each class 38 in a desired way among the places from which packets 30 are transmitted.

EX1001, 6:16-25. In the embodiment of Figure 1, the computer 18 "allocates the processing rate for each class 38." EX1001, 6:23-25.

59. Figure 2 below is a variation of Figure 1. EX1001, 6:26. In Figure 2, computer 18 receives data packets 30 from computer 7 via routers 3 and 5.

Figure 2



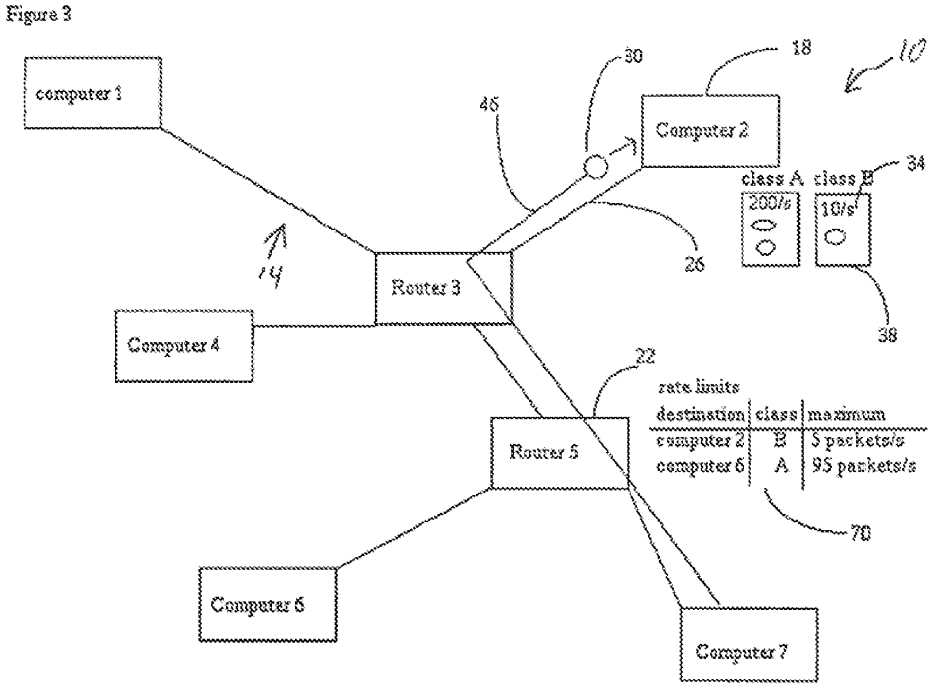
EX1001, Fig. 2 (annotated)

60. With reference to Figure 2 above, the '497 patent explains that the system 10 includes:

> means for classifying data packets 30 received at a host computer 18 and means for associating a maximum acceptable processing rate 34 with each class 38 of data packet 30 received at the computer 18. Means are provided for the computer 18 to determine the rate at which data packets 30 of each class 38 are transmitted from a router 22 to the computer 18 as are means for the router 22 to receive information regarding maximum acceptable transmission rate 70 for data packets 30 being transmitted to the computer 18. Means are provided for the router 22 to control the rate of transmission of data packets 30 from the router 22 to the computer 18. Thus, the rate of data packet transmissions received at the computer 18 is kept below the maximum acceptable processing rate 34 for each data packet class 38 by the control of the rate of transmission of data packets 30 from the router 22, thereby freeing a portion of the network 14 providing data packet transmission to the computer 18.

EX1001, 6:29-45.

61. Figure 3 is another variation of Figures 1 and 2. Relative to Figures 1 and 2, the embodiment of Figure 3 reproduced below newly includes the feature that "the router 22 is capable of receiving information regarding maximum acceptable transmission rate 70 for each class 38 of data packet 30 being transmitted to the computer 18 and the router 22 is capable of controlling the rate of transmission of each class 38 of data packets 30 to the computer 18." EX1001, 6:46-51.

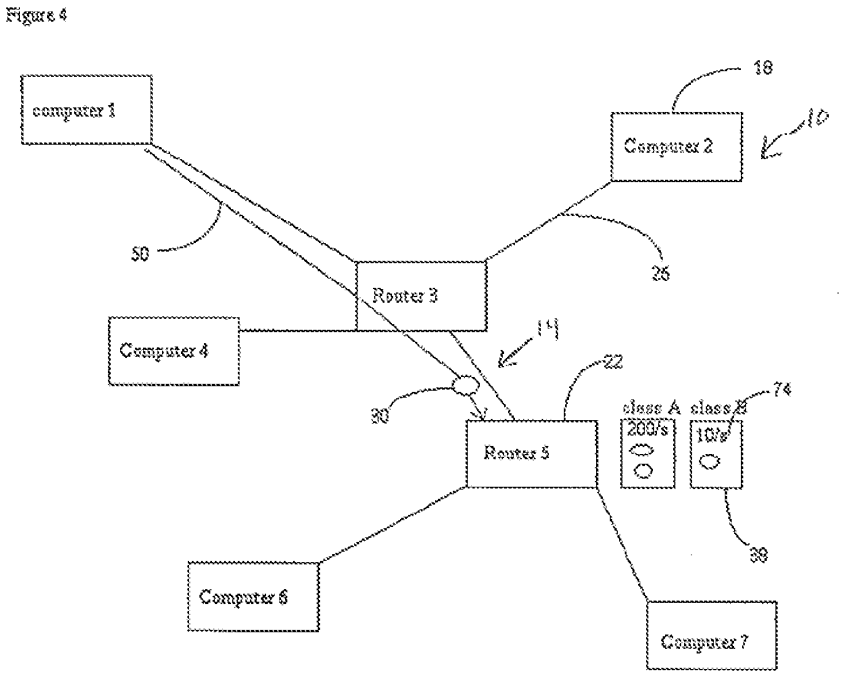


EX1001, Fig. 3

62. Figure 4 is a further variation of the embodiments of Figures 1-3. In Figures 1-3, the host computer 18 has means for classifying data packets received at the host computer and associating a maximum acceptable processing rate 34 with each class 38 of data packet 30 received by the host computer 30. EX1001, 6:16-20. On the contrary, in Figure 4 reproduced below, the '497 patent explains that the router 22 (router 5) classifies the data packets, associates a maximum acceptable transmission rate with each class of data packet received at the router, and allocates a transmission rate, as follows:

> [The system 10 includes] means for classifying data packets 30 received at a router 22 and means for associating a maximum acceptable transmission rate 74 with each class 38 of data packet 30 received at the router 22. Means are provided 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. Thus, the router 22 can use the information to allocate the transmission rate for each class 38 in a desired way.

EX1001, 6:52-63.



EX1001, Fig. 4

63. Claims 7 and 10 recite various features of the above-described embodiments of the '497 patent. Claims 7 and 10 are reproduced below with the

same claim numbering used in the Request. Claim 7 corresponds generally to the embodiment of Figures 1, because claim 7 recites "allocating a processing rate…." (limitation [7.4]). As described above, in the embodiment of Figure 1, the computer 18 "allocates the processing rate for each class 38." EX1001, 6:23-25 (emphasis added). On the contrary, claim 10 generally corresponds to features included in Figures 2-4, because claim 10 recites "allocating a transmission rate…." (limitation [10.4]). In the embodiments of Figures 2-4, the router allocates a transmission rate for packets to be transmitted to the host computer. EX1001, 6:38-40 (Fig. 2) ("Means are provided for the router 22 to control the rate of transmission of data packets 30 from the router 22 to the computer 18."), 6:49-51 (Fig. 3) ("…the router 22 is capable of controlling the rate of transmission of each class 38 of data packets 30 to the computer 18."), 6:61-63 ("…the router 22 can use the information to allocate the transmission rate for each class 38 in a desired way.").

C. Claims 7 and 10

64. Claims 7 and 10 are reproduced below with the same claim numbering used in the Request. As described in Section VIII.E below, claims 7 and 10 were identified as being allowable over the prosecution prior art after limitations [7.1.2] and [10.1.2] were added by amendment. The features of claims 13, 16, 1 and 4 are reproduced beneath the analysis of claims 7 and 10 in Sections X.A and X.B below. I have also included claim charts showing the differences between claim 7 and claim

13, the differences between claim 7 and claim 1, the differences between claim 10 and claim 16, and the differences between claim 10 and claim 4. As I discuss in more detail below, claim 7 is substantially similar to claims 13 and 1, and claim 10 is substantially similar to claims 16 and 4.

Claim 7

[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:

[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;

[7.2] 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

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

Claim 10

[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:

[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;

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

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

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

D. Packet Marking

65. Limitations [7.1.1] and [10.1.1] use the term "packet marks." The term "packet mark" is mentioned only once in the specification of the '497 patent. In the Summary of the Invention section, the '497 patent contains the following description.

> In this invention a path (which is not controlled by the attacker) is used to determine the actual direction of the packet flow towards the victim. Bandwidth is allocated based upon path (which is done via **packet marks** provided by routers leading up to the victim).

EX1001, 3:62-66.

66. Independent claims 1, 4, 7, 10, and 13 of the '497 patent all recite the term "packet marks," using the identical phrase in each claim: "…via packet marks provided by routers leading to said host computer." EX1001, 8:20-21 (claim 1), 9:3-

4 (claim 4), 9:50-51 (claim 7), 10:35-36 (claim 10), 11:1-12 (claim 13). Independent claim 16 of the '497 patent recites the term "packet marks," using the phrase: "…via packet marks provided by routers leading to said router." EX1001, 12:7-8 (claim 16). Claims 1, 4, 7, 10, 13, and 16 do not define the term "packet marks." Accordingly, I have interpreted the term "packet marks" as it was commonly used in prior art before the '497 patent as a mark inserted into a packet. Prior art teachings of packet marking are discussed in Sections IX.B and IX.C below.

E. Prosecution History

67. As noted above, the '497 patent was filed as a continuation of U.S. Patent 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).

68. 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.

69. The '497 patent was filed as Application No. 10/841,064 ("'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.

70. 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.

71. 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.[10]

72. In the final Office Action, the examiner rejected the applicant's argument, finding that Chang discloses determining a path by which data packets

[10] 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.

arrive at a 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.

73. 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.

74. EX1002, 129, 135, 130 (additional features shown with underlining, and claim numbering added). Similar amendments were made to claim 10 (addition of limitation [10.1.2]).

75. 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] and [10.1.2].

76. As described in Section X below, however, limitations [7.1.1] and [7.1.2] are disclosed by prior art (*Savage*) not considered by the examiner. Notably, claim 7 does 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. Limitations [10.1.1] and [10.1.2] are similarly disclosed by prior art not considered by the examiner.

IX. OVERVIEW OF PRIOR ART[11]

77. I considered the prior art below in reaching my opinion that claims 7 and 10 are unpatentable. In this section, I also explain why a POSITA would have been motivated to modify the teachings of the prior art, based on the level of ordinary skill in the art and the advantages taught by the prior art, to illustrate why all limitations of claims 7 and 10 were known in the art, and the combination of limitations in claims 7 and 10 would have been obvious to a POSITA.

[11] Unless otherwise noted, all **bold** and **bold *italics*** emphasis in any quoted material has been added. Text in *italics* is used to signify claim language, while the names of the *Savage* (EX1005), *Maher* (EX1006) and *Schuba* (1007) references are also *italicized*.

A. Packet Flooding and Denial of Service Attacks

78. As described above, 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 prior art references sought to prevent packet flooding attacks.

79. Other contemporaneous references describe packet flooding attacks as a type of "Denial of Service" (DoS) attack. For example, U.S. 2002/0032871 to Malan et al. (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.

80. 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.

81. Similarly, *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.

82. 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. For example, *Savage* (EX1005) discloses that its technique was "motivated by the increased frequency and sophistication of denial-of-service attacks and by the difficulty in tracing packets with incorrect, or 'spoofed', source addresses." EX1005, Abstract. Similarly, Stone (EX1011) recognized that "the attacker can forge the source address of the flood packets" to avoid detection," by engaging in a TCP SYN flood that exploits a vulnerability in the synchronization (SYN)[12] process of the TCP/IP protocol. EX1011, 1:44-54, 1:29-35. Likewise, *Schuba* (EX1007) discussed a synchronization (SYN) flooding

[12] RFC 791 (EX1044), § 2.7 discusses the synchronize (SYN) process (referred to as a "three-way hand shake") of TCP/IP, § 3.3, pp. 26-27 (discussing SYN process), § 3.4, pp. 30 (establishing a connection with SYN).

attack that exploits vulnerabilities in the TCP/IP framework by not engaging in synchronization: "[a]ttacker A initiates a SYN flooding attack by sending many connection requests with spoofed source addresses to the victim machine, destination host D." EX1007, 5:62-64.

83. As another example, *Maher* (EX1006) discussed a type of flooding attacks known as a "SYN attack" that

> **floods a targeted system with a series of TCP SYN packets**. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. This backlog queue has a finite length that is usually quite small. Once the queue is full, the system will either ignore all incoming SYN requests, or more likely crash. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. **A SYN attack creates each SYN packet in the flood with a bad source IP address**, which under routine procedure identifies the original packet. All responses are sent to the source IP address. But a bad source IP address either does not actually exist or is down; therefore the ACK that should follow a SYN-ACK response will never come back. This creates a backlog queue that's always full, making it nearly impossible for legitimate TCP SYN requests to get into the system.

EX1006, 1:56-2:9.

84. The prior art recognized that there were two components to preventing a packet flooding or DoS-type attack: (1) identifying the attacker, and (2) reducing the severity of a DoS-type attack on the network. As discussed below, *Maher* (EX1006) and *Schuba* (EX1007) are both directed to systems that reduce the severity of a packet flooding or DoS-type attack on a network by minimizing the rate and/or amount of packets that may be transmitted to a victim host computer.

B. Packet Marking was Well-Known in the Art

85. The concept of marking packets to convey information to devices receiving the packets was well-known in the art.

86. For example, RFC 2481 (EX1036) disclosed the concept of routers "marking packets" as a sign that the packets have encountered congestion in the network, and these marks are carried in the packet to the destination. EX1036, §§ 5, 6.1.1. This congestion marking is intended to inform destination terminals that the packets containing this congestion marking may be dropped. RFC 2481 discloses a technique of adding an "Explicit Congestion Notification" (ECN) marker in the header (two bits) of a packet received by a router. EX1036, § 5.

87. As another example, RFC 2474 (EX1037) discloses a "differentiated service" model for supporting multimedia Internet flows that involves marking packets to indicate whether they are "in specification" for a certain class of service, or whether they should only be given best effort service. EX1037, § 1 (¶6). Like

RFC 2481, RFC 2474 provides this "differentiated service" marker into the header of the packet. EX1037, Abstract. RFC 2474 teaches that a packet can be marked for "default behavior" (i.e., process as normal), or if the packet is not marked, can be processed with lower priority, §§ 3, 7.1 (in view of Denial of Service attacks, endpoint nodes can mark "codepoint values in packets to indicate that they are appropriate traffic), 4.2.2.2.

88. As yet another example of the well-known use of packet marking, RFC 2475 (EX1038) added packet marks to the "Differentiated Services" (DS) field of the headers of packets, and then network resources are allocated based on these markings. EX1038, Abstract, § 2.3.2 (discussing adding traffic profiles to DS header fields), § 2.3.3.2 (discussing markers used to set DS field in header), § 2.3.4.1 ("The traffic originating from the source domain across a boundary may be marked by the traffic sources directly or by intermediate nodes before leaving the source domain."), § 2.5 (packets marked to denote network resource allocation).

89. As yet another example of the well-known use of packet marking, 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 ("EX1039") discloses that end nodes (e.g., edge routers) store the state of the packet (e.g., whether the packet is a fragment or needs to be fragmented) in the packet header so that the state information can be processed by intermediate nodes

(core nodes) in the network. §§ 5.1 (adding state information to header of packet), 5.2 (example of adding state information to header).

90. Thus, in view of the above-discussed prior art, the concept of marking information about a packet, or the congestion of a network, in the packet was well-known in the art to inform downstream devices of that information so that the downstream devices could operate in response to that information.

C. Overview of *Savage*

Like the '497 patent, *Savage* teaches a packet flooding defense system and 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. In particular, *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.

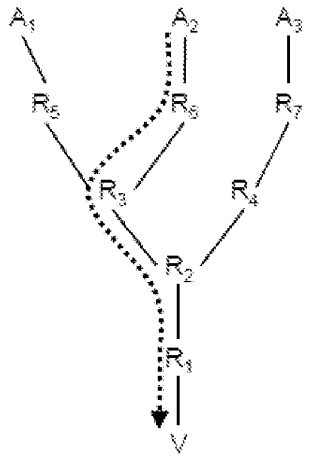


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1

91. *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.

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 $(R_0..R_j)$ from the suffix of w

Figure 2: Node append algorithm.

EX1005, Fig. 2

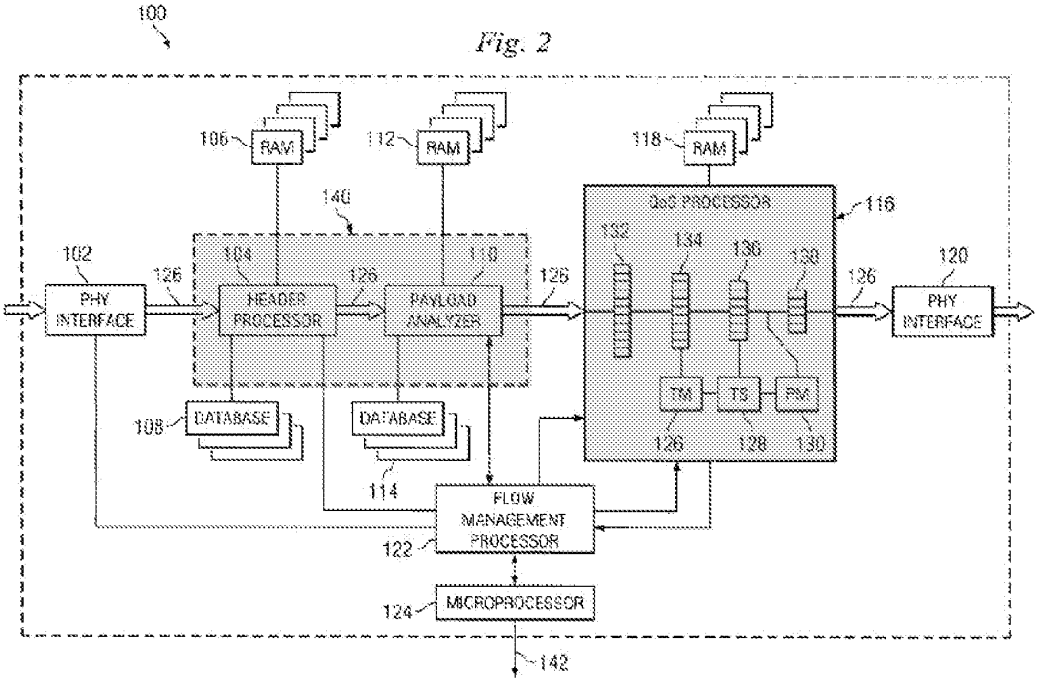
92. *Savage* teaches that the victim V then implements a "path reconstruction procedure" to "reconstruct the attack path using only the information in these marked packets." EX1005, 298.

D. Overview of *Maher*

93. 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* EX1006, 1:8-10 ("[T]he present invention relates to a method and device that prevents denial of service type internet attacks."), 2:52-53 ("The present invention provides for a method of preventing DoS attacks."). *Maher* explains that its network apparatus "for preventing DoS attacks" includes "a traffic flow scanning engine and a quality of service processor." EX1006, 3:6-9, Abstract. 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.

Fig. 2



EX1006, Fig. 2 (annotated)

94. 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. On the other hand, "[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.

95. *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." EX1006, 7:54-63 (emphases added).

96. 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. Accordingly, *Maher* is directed to a system that reduces the severity of a packet flooding or DoS-type attack on a network by minimizing the rate and amount of packets that may be transmitted to a victim host computer. For example, *Maher* discloses that "[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.

E. Overview of Schuba

97. 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 ("An active monitor detects and classifies messages transmitted on a network. In one form, the monitor includes a routine for classifying TCP packet source addresses as being of an acceptable, unacceptable, or suspect type."), 2:1-5 ("network 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."), 2:22-26 ("network 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."), 3:8-13 ("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."). *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.

98. Further, like *Maher*, *Schuba* is also directed to a system that reduces the severity of a packet flooding or DoS-type attack on a network by minimizing the rate and amount of packets that may be transmitted to a victim host computer. For example, *Schuba* teaches 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. For example, with reference to the flowchart of Figure 4 below, Schuba discloses that

> If, on the other hand, the source address of a newly detected SYN packet is not one of the acceptable addresses, control flows to conditional 70 to test whether the newly detected SYN packet has a

source address that is unacceptable or "evil" as represented by one of another set of entries in database 57. If so, classification operation 65 of routine 60 is exited and a RST packet is sent in stage 72 to the targeted destination host 54 that receives the SYN packet with an unacceptable address to **close the corresponding TCP connection**. By closing the connection, the RST packet frees resources of the targeted destination host 54. FIG. 5 is a diagram illustrating the packet sequence observed for processing through state 72 for a SYN packet with an unacceptable source address. **Any subsequent RST packets are ignored with regard to the FIG. 5 packet sequence**. From stage 72, routine 60 continues to stage 76.

EX1007, 8:18-33.

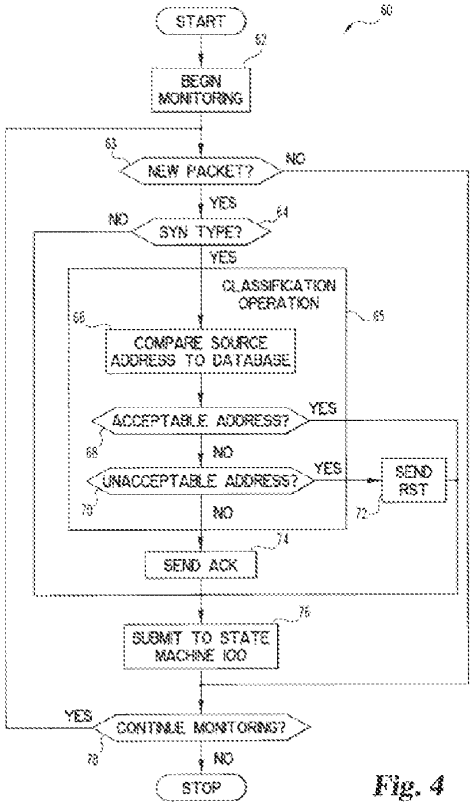


Fig. 4

EX1007, Fig. 4

99. Thus, like *Maher*, *Schuba* teaches a system that reduces the severity of a packet flooding or DoS-type attack on a network by minimizing the rate and amount of packets that may be transmitted to a victim host computer.

F. Proposed Rejection #1: Motivation to Combine *Savage* with *Maher* and *Schuba*

100. As described in Section X.A below, all the limitations of claim 7 of the '497 are taught by *Savage*, *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*. These references are analogous art to the challenged claims of the '497 patent. As discussed in Sections IX.C-IX.E 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."). 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 ("The primary objective of the present invention is to defend against 'packet flooding attacks.'"). EX1001, 2:6-7.

1. A POSITA would have been motivated to modify *Savage* to incorporate *Maher*'s conventional network implementation details

101. *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.

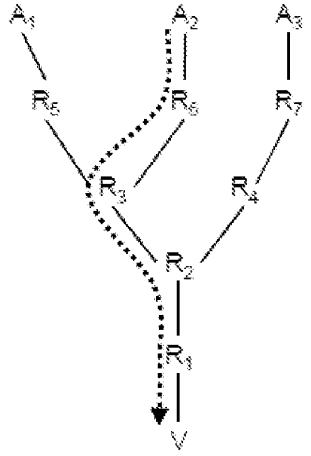


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

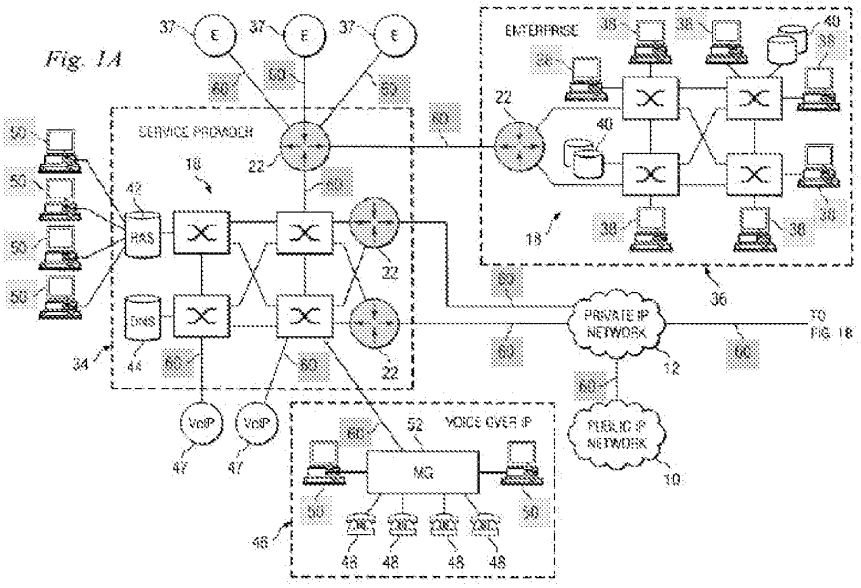
EX1005, Fig. 1

102. *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 a single host computer, or a network border device representing many host computers downstream of routers.

103. 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.").

104. 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.



EX1006, Fig. 1A (annotated)

105. 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.

106. 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.

107. 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. *Savage* discloses that its traceback technique is "backwards compatible and can be efficiently implemented using conventional technology," such as *Maher*'s conventional network architecture. EX1005, Abstract. 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.

2. A POSITA would have been motivated to utilize *Savage*'s packet marking technique to determine the path of a packet including all routers between an attacker and a victim

108. As described above, *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). With reference to the attack path shown in *Savage*'s Figure 1 below, I prepared the following example showing how *Savage* would insert the address of each router along the attack path (routers R_6, R_3, R_2, and R_1).

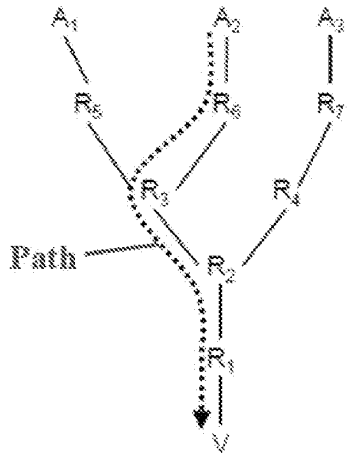


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

109. With reference to Figure 2 below, *Savage* teaches that "[t]he simplest marking algorithm…is to append each node'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. Figure 2 of Savage is reproduced below.

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 (annotated)

110. Using the above example of Figure 1, I have assigned the following IP addresses to routers R_6, R_3, R_2, and R_1 through which the packet traverses between Attacker A_2 and victim host computer V.

Router	Example IP address
R_6	127.0.0.1
R_3	172.16.0.9
R_2	192.0.0.7
R_1	69.89.31.226

Using these example addresses and the Node append algorithm disclosed in Figure 2 of Savage, a data packet (including header and payload) from Attacker A_2 in Figure 1 would reach victim V with the addresses of routers R_6, R_3, R_2, and R_1 appended to the end of the packet, as shown below.

Header	Payload	127.0.0.1	172.16.0.9	192.0.0.7	69.89.31.22
		R_6	R_3	R_2	R_1

Example packet received at victim V based on attack path in Figure 1

3. 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.

111. As described above in Section IX.C, *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. In other words, *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.

112. 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. As described in Sections IX.D and IX.E above, both *Schuba* and *Maher* are directed to systems that reduce the severity of a packet flooding or DoS-type attack on a network by minimizing the rate and amount of packets that may be transmitted to a victim host computer.

113. *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.

114. 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 denial of service 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. EX1006, 7:67-8:3, 3:30-35. *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. *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* involve 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). 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.*

115. 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. 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).

116. 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*.

G. Proposed Rejection #2: Motivation to Combine *Maher* with *Savage* and *Schuba*

117. As described in Section X.B below, all the limitations of claim 10 of the '497 are taught by *Maher*, *Savage*, and *Schuba*. For the following reasons, 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*. The *Maher*, *Savage*, and *Schuba* references are analogous art to the claims of the '497 patent. As discussed in Sections IX.C-IX.E 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."). 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.

1. 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

118. As discussed above in Section IX.D, *Maher* is directed to "a method and apparatus for preventing denial of service type attacks on data networks." EX1006, Abstract; *see also* EX1006, 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).

119. As discussed above in Sections IX.C and IX.F.2, and as discussed above in Section X.A.[7.1.2], *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. 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. *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.

120. *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. 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.

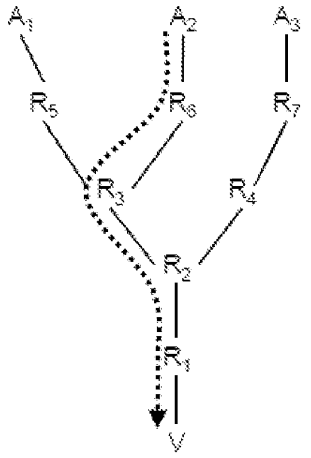


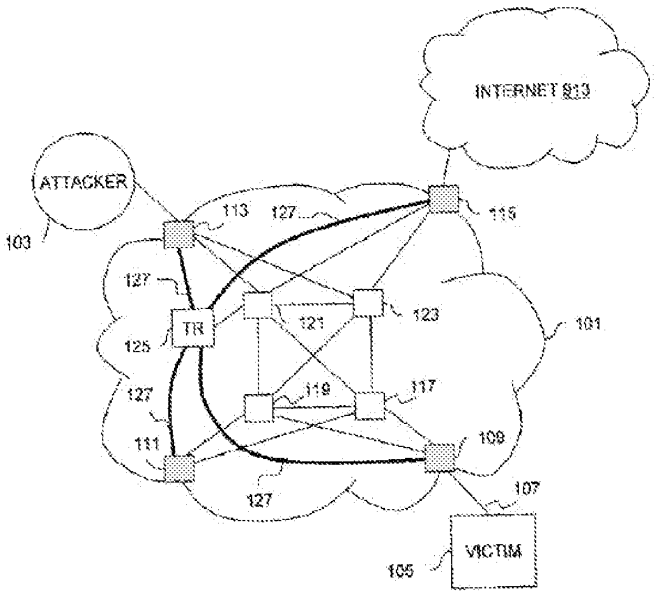
Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1

121. 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.

122. 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.



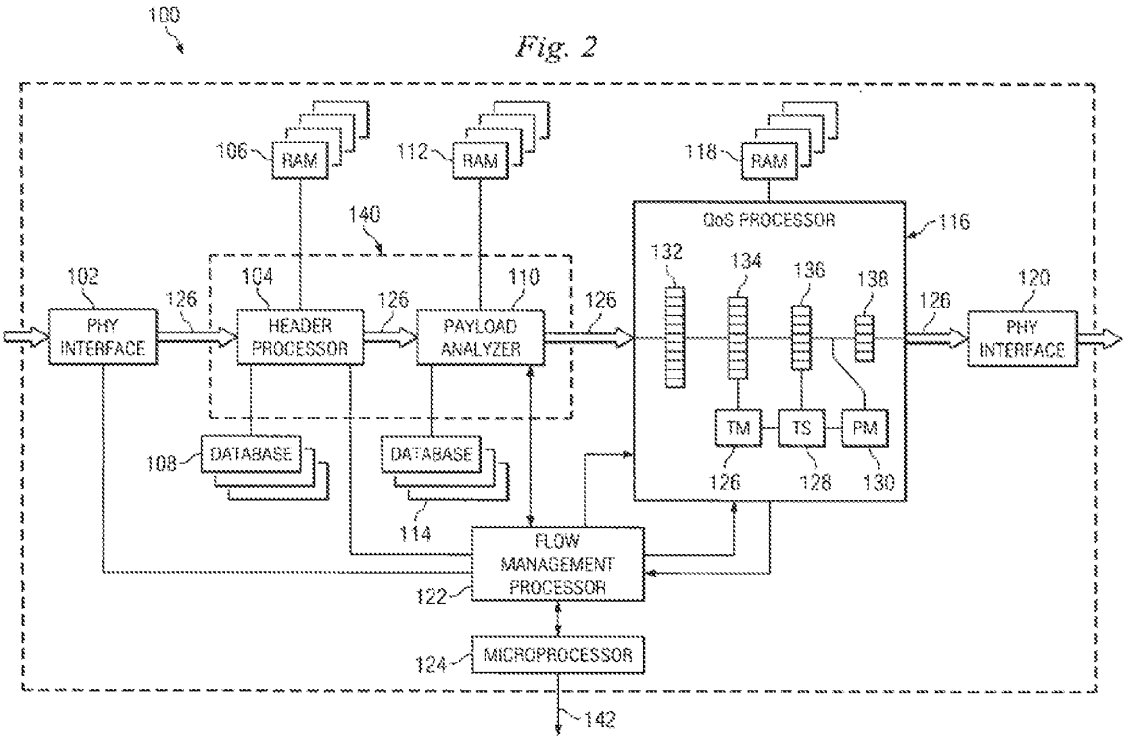
EX1011, Fig. 1 (annotated)

123. 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.

124. 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. 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. A POSITA would have known that a router or host device receiving a packet containing path information of the path that the packet took, as taught by *Savage*, would be read and processed by the router or host device receiving the packet, in the same way that a router or host device reads and processes information in a received

packet, as taught by *Maher*. See EX1005, 298 (disclosing marking algorithm of adding path information to packet), 299 (disclosing node append algorithm of appending "each node's address to the end of the packet as it travels to the end of the packet as it travels through the network"). For instance, as shown in Figure 2 below, *Maher* discloses that the network apparatus 100 includes a header processor 104 to process routing information in the header of the packet (EX1006, 6:16-21, 6:49-55), and a payload analyzer 110 that "scans the contents of the data packets," including the payload content and optionally the headers, to "act on [] the content of the data packets being scanned [and] the contents of the entire traffic flow." EX1006, 7:8-24; *see also* EX1006, 6:11-13 (describing scanning processor 140 as including a header processor 104 and a payload analyzer 110).

Fig. 2



EX1006, Fig. 2

2. 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

125. 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.

126. *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* 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).

127. *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 (describing Maher's network apparatus as a "bump-in-the-line" device. 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.

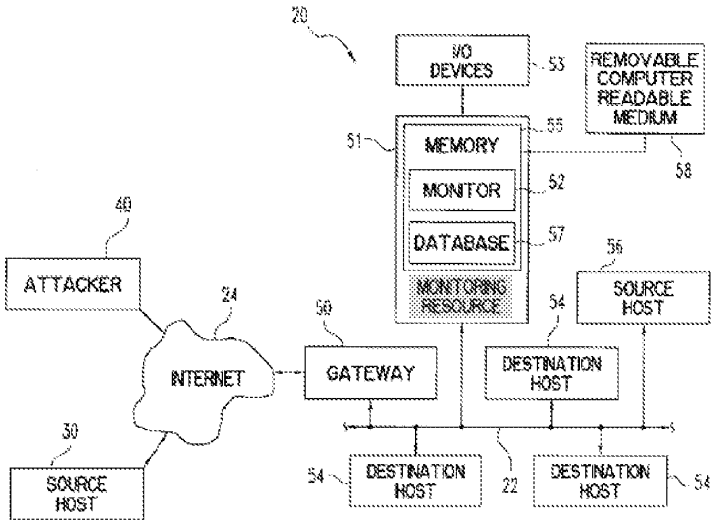


Fig. 3

EX1007, Fig. 3 (annotated)

128. 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.

129. 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. As discussed above in Section IX.C, *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*.

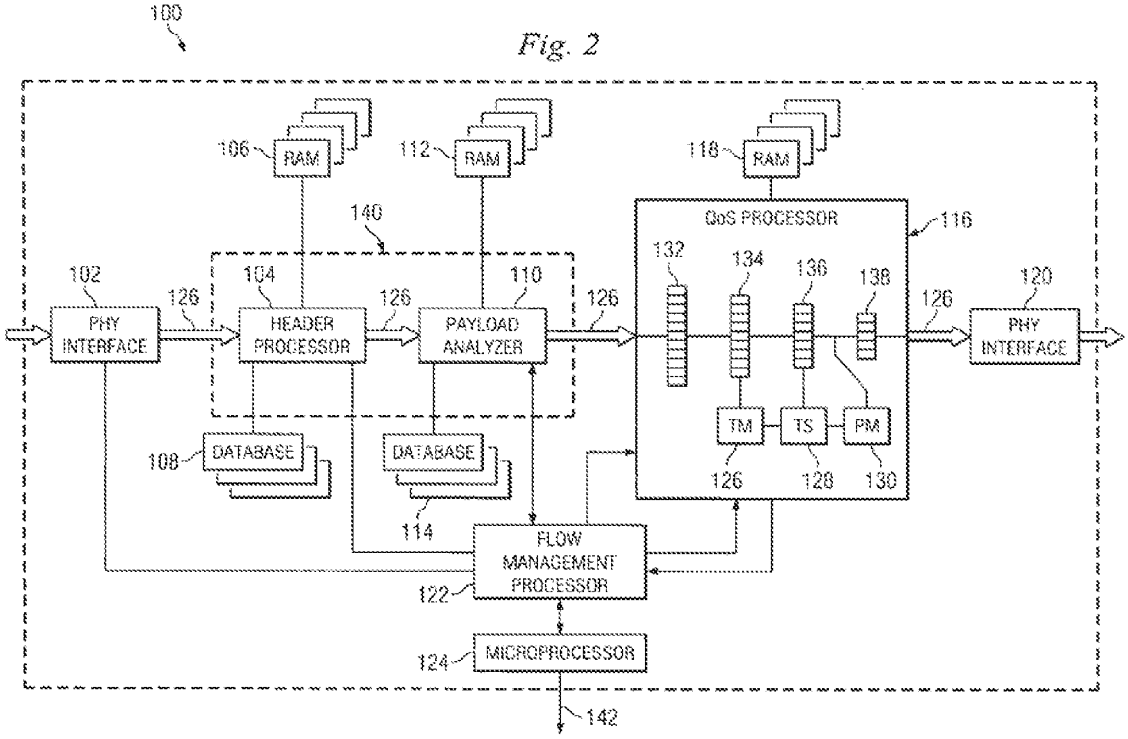
130. These modifications involve the combination of prior art elements (combining *Maher*'s classification technique with *Schuba*'s classification of packets as wanted or unwanted, and *Savage*'s teaching of adding packet marks at routers along the path of data flow to aid in the identification of the 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).

131. 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."). Thus, a POSITA would have had a reasonable expectation of success in performing *Schuba*'s traceback technique in a router or bump-in-the-line type device, because *Maher* and *Schuba* both teach that the classification operations can be at a network router and/or a bump-in-the-line type device in a network, and *Maher* teaches that its network apparatus 100, which may be a network router and/or a bump-in-the-line type device, includes a header processor 104 to process routing information in the header of the packet (EX1006, 6:16-21, 6:49-55), and a payload analyzer 110 that "scans the contents of the data packets," including the payload content and optionally the headers, to "act on [] the

content of the data packets being scanned [and] the contents of the entire traffic flow," as shown in Figure 2 below. EX1006, 7:8-24; *see also* EX1006, 6:11-13 (describing scanning processor 140 as including a header processor 104 and a payload analyzer 110). Thus, a POSITA would have had a reasonable expectation of success in 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, in view of Maher's teaching that its network apparatus 100 may be a network router and/or a bump-in-the-line type device. EX1006, 6:59-66.

Fig. 2



EX1006, Fig. 2

X. DETAILED INVALIDITY ANALYSIS

132. I have been asked to provide my opinion as to whether the Challenged Claims of the '497 patent would have been obvious in view of the prior art. The discussion below provides a detailed analysis of how the prior art references I reviewed disclose, teach, or suggest the limitations of the Challenged Claims of the '497 patent. As discussed above in Section III, it is my opinion that claims 7 and 10 of the '497 patent are unpatentable as obvious. The chart below summarizes my conclusions of unpatentability regarding claims 7 and 10 of the '497 patent.

Ground	Claim	Basis
1	7	Obvious over *Savage* in view of *Maher* and *Schuba*
2	10	Obvious over Maher in view of *Savage* and *Schuba*

133. I will now describe, in the grounds below, on an element-by-element basis how the prior art discloses or teaches all elements of claims 7 and 10. Unless otherwise noted, all **bold**, *italics*, and **bold *italics*** emphasis in any quoted material has been added.

A. Proposed Rejection #1: Claim 7 would have been obvious over *Savage* in view of *Maher* and further in view of *Schuba*.

134. It is my opinion that *Savage*, *Maher* and *Schuba* teach or suggest to a POSITA the subject matter of each and every limitation of claim 7 of the '497 patent.

[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:

135. To the extent that the preamble of limitation [7.0] is limiting, it is rendered obvious by *Savage* in view of *Maher*. *Savage* and *Maher* each disclose a method of providing packet flooding defense for a network as recited in limitation [7.0].

136. *Savage* discloses *a method of providing packet flooding defense for a network*. In particular, *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.

137. 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.

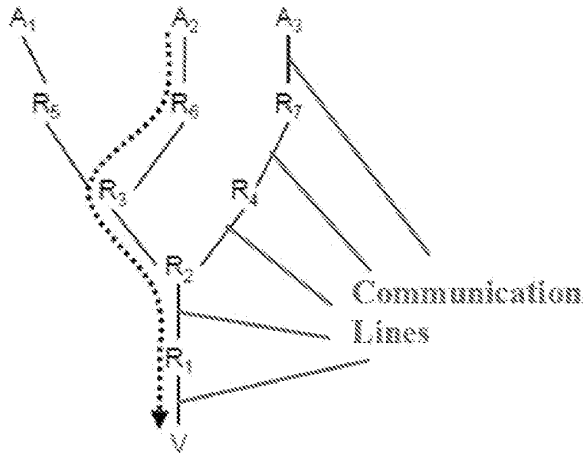


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

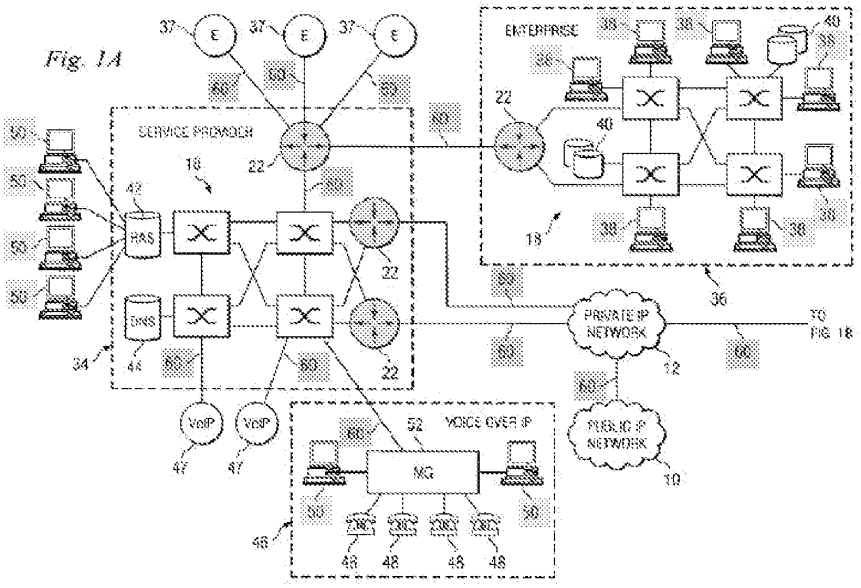
EX1005, Fig. 1 (annotated)

138. *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.

139. *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.

140. 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*.

141. *Maher* teaches "[a] method and apparatus for preventing denial of service type attacks on data networks." EX1006, Abstract; *see also id.*, 1:8-10 ("the present invention relates to a method and device that prevents denial of service type internet attacks."), 2:52-53 ("The present invention provides for a 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. 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." *Maher*, 2:53-55.



EX1006, Fig. 1A (annotated)

142. Thus, *Maher* discloses a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, as recited in limitation [7.0]. A POSITA would have been motivated modify *Savage* to incorporate *Maher*'s conventional network implementation details, for the reasons presented above in Section IX.F.1.

143. Accordingly, *Savage* and *Maher* render obvious limitation [7.0].

[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;

144. *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*, as recited in limitation [7.1.1], 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.

145. *Savage* discloses that its "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**." *Savage*, 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.

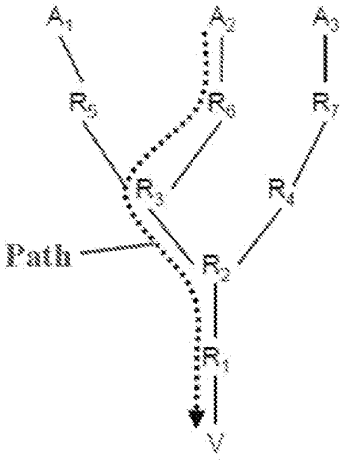


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1 (annotated)

146. *Savage* discloses that the "attack path from [attacker] A_i is the **unique ordered list of routers between A_i and V.**" EX1005, 298. *Savage* discloses that 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. *Savage* explains that in the *path reconstruction procedure*, the victim "reconstruct[s] the attack path using only the information in these marked packets." EX1005, 298; *see also* Section IX.F.2 above providing an example of path marking based on the path shown in Figure 1 of *Savage*.

147. 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 (emphases added). As shown in Figure 2 below, 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.

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)

148. 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*, as recited in limitation [7.1.1].

[7.1.2] said path comprising all routers in said network via which said packets are routed to said computer;

149. *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. As described in Section VIII.E 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.

150. 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).

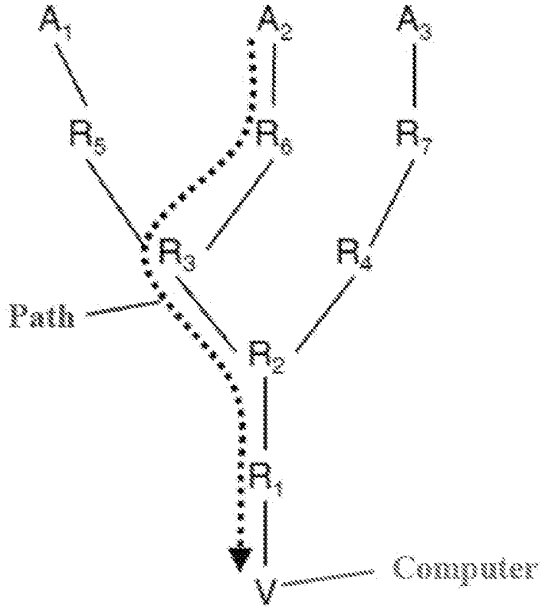


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1 (annotated)

151. *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.

152. With reference to Fig. 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.

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)

153. Accordingly, in the following annotated example of Figure 1, *Savage* discloses appending to the packet the addresses of routers R_6, R_5, R_2 and R_1 along the path between the attacker A_2 and the victim V. EX1005, 298.

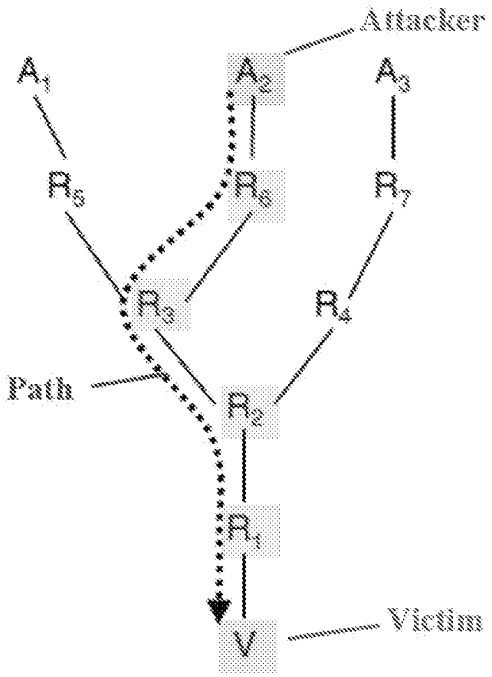


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1 (annotated)

154. 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*, as recited in limitation [7.1.2].

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

155. Limitation [7.2] is rendered obvious over *Savage* in view of *Schuba* and *Maher*. 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*.

156. 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. *Id.*

157. Neither the specification nor the claims of the '497 patent require a classification into *only* "wanted data packets" and "unwanted data packets." The concept of "wanted" and "unwanted" data packets is discussed only in the Background of the Invention section (EX1001, 3:4-23), and the "distinction between 'wanted' and 'unwanted' packets" is based on whether packets are expected to be received. EX1001, 3:13-17. The '497 patent explains that expected packets are processed "at the highest possible rate," while packets that are unexpected "are not exactly unwanted," but are "process[ed] [] at only a limited rate." EX1001, 3:17-19. Thus, the '497 patent does not exclude another category besides "wanted" or "unwanted" data packets.

158. 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 one or more host computers 54 in the local area network 22 over a public network such as the Internet 24 (referred to as "untrusted network"). EX1007, 7:10-22, 6:46-67 (explaining network architecture). Monitoring resource 51 is operatively coupled to the local area network 22, and executes monitoring program "to protect other resources on network 22 from SYN flooding by sources from untrusted network 24, such as from attacker 40, and still facilitate establishment of connections with legitimate external sources, such as source host 30." EX1007, 6:54-62.

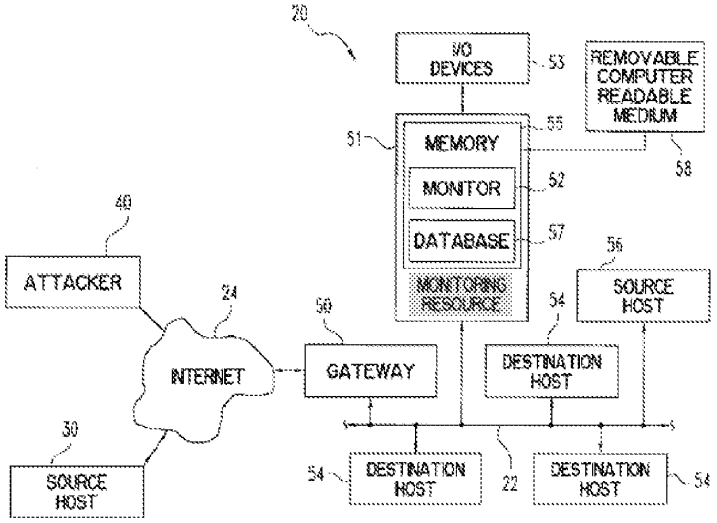


Fig. 3

EX1007, Fig. 3 (annotated)

159. *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, including any TCP packets involved in a three-way handshake with destinations 54. 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.

160. 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.

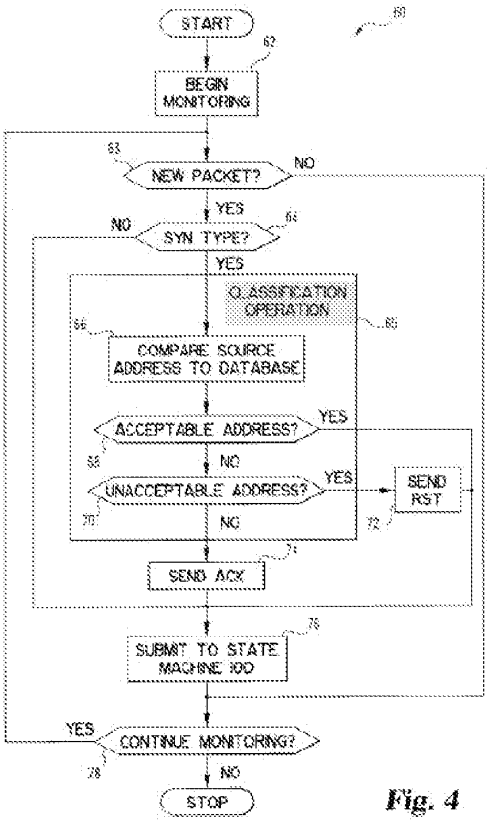


Fig. 4

EX1007, Fig. 4 (annotated)

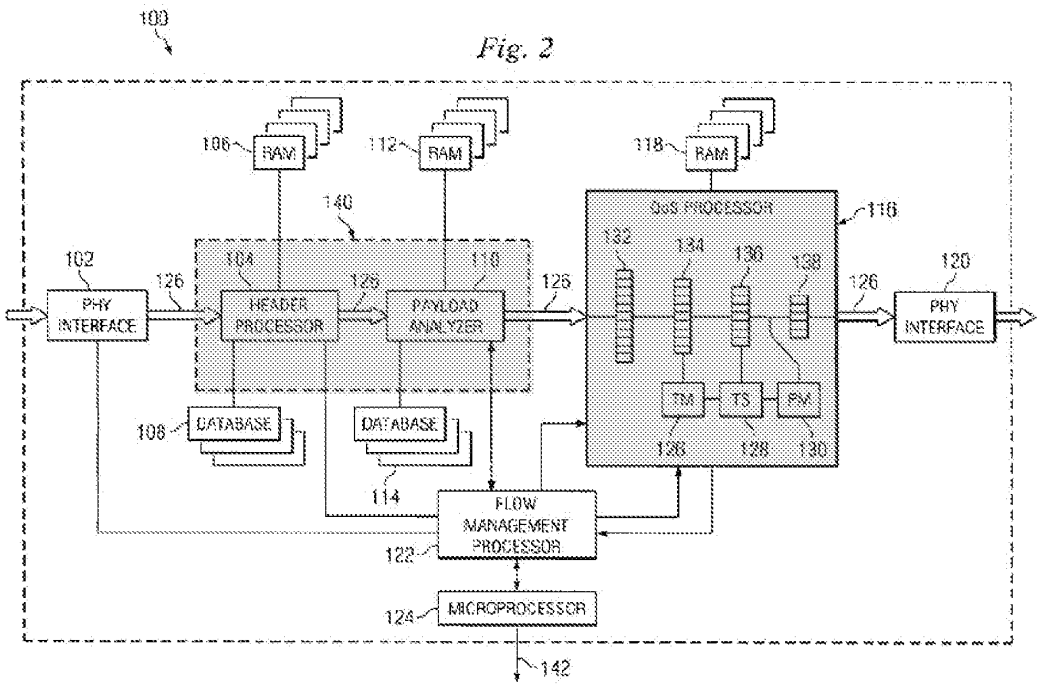
161. By classifying the packets based on source address, *Schuba* teaches that incoming data packets are classified as unwanted data packets ("unacceptable") or

wanted data packets ("acceptable") based on at least partial path information (source address).

162. 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 the source and destination of the packet.

163. *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.

Fig. 2



EX1006, Fig. 2 (annotated)

164. 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. On the other hand, "[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.

165. *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." EX1006, 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).

166. 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].

167. I note that 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.

168. 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 IX.F.3. 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.

169. 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. 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.

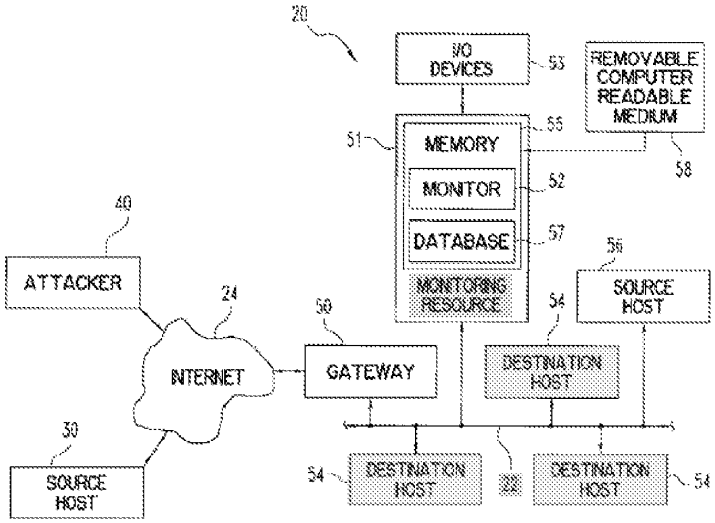


Fig. 3

EX1007, Fig. 3 (annotated)

170. 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

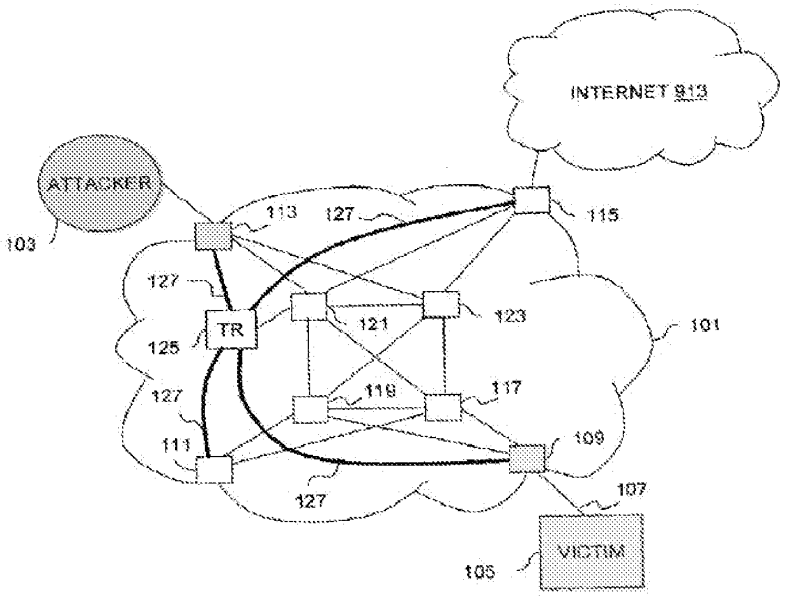
POSITA would have been motivated to include a bump-in-the-line type network device that receives data packets transmitted to *Savage*'s victim host computer V, as taught by *Schuba* and *Maher*, to *classify[] data packets received at said host computer into wanted data packets and unwanted data packets 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 IX.F.3.

171. 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 minimize the effects of a packet flood attack, as taught by *Schuba* and *Maher*. 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 VIII.E 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" indicating the rate at which the host computer is able to receive incoming data packets, 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. 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.

172. As another example, Stone (EX1011) teaches that is was known to classify data packets into wanted packets and unwanted packets by path. With reference to Figure 1 below, Stone discloses that data packets from attacker 103 are classified to aid in tracking down the ingress edge router that is responsible for forwarding packet flood attacks into the network 101 to victim 105. As shown in Figure 1 below, packets from the attacker 103 enter through the ingress edge router 113. Stone discloses tracing an attacker from an ingress edge router (e.g., edge router 113 in Fig. 1) to the destination (victim 105 in Fig. 1). Stone discloses that an attack signature is developed to identify an attack launched by attacker 103, where the attack signature "refers to some pattern that can be used to help distinguish malicious packets from normal traffic[, and at] the very least, an attack signature is defined by the IP address or address range of the victim 105." EX1011, 5:50-55. Stone discloses that tracking router (TR) 125 forms an overlay network with edge routers (including edge router 109 and edge router 113) to track down the ingress edge router (edge router 113) that is responsible for forwarding packet floods into the IP network 101 based on the attack signature. EX1011, 5:56-6:1. In Stone, the attack signature is developed by path, such as the path from edge router 113 to edge router 109, which is a "pattern [] used to help distinguish malicious packets from normal traffic." EX1011, 5:50-55. Thus, like Chang, Stone 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 network device receiving data packets.



EX1011, Fig. 1 (annotated)

173. Therefore, limitation [7.2] is rendered obvious by *Savage* in view of *Maher* and *Schuba*.

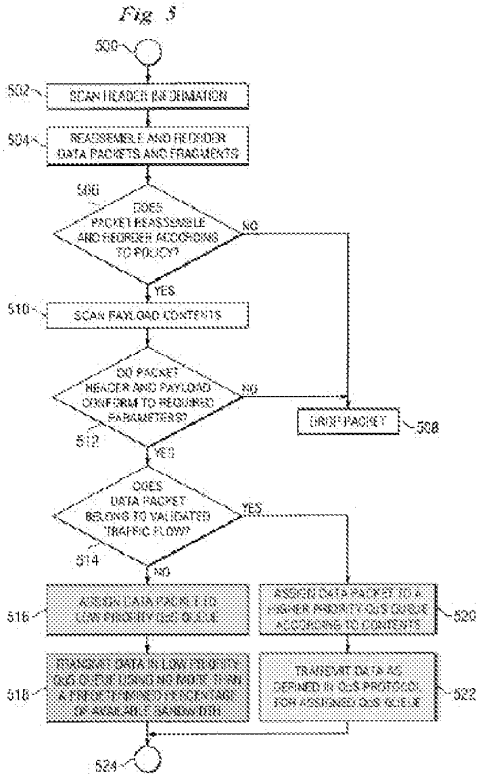
[7.3] associating a maximum acceptable processing rate with each class of data packet received at said host computer; and

174. 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].

175. *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). EX1006, 7:63-8:3. *Maher* discloses that validated traffic (wanted data packets) are placed in different quality of service (QoS) queues than unvalidated (unwanted data packets) for processing. EX1006, 11:67-12:19.

176. With reference to Fig. 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), which is 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).

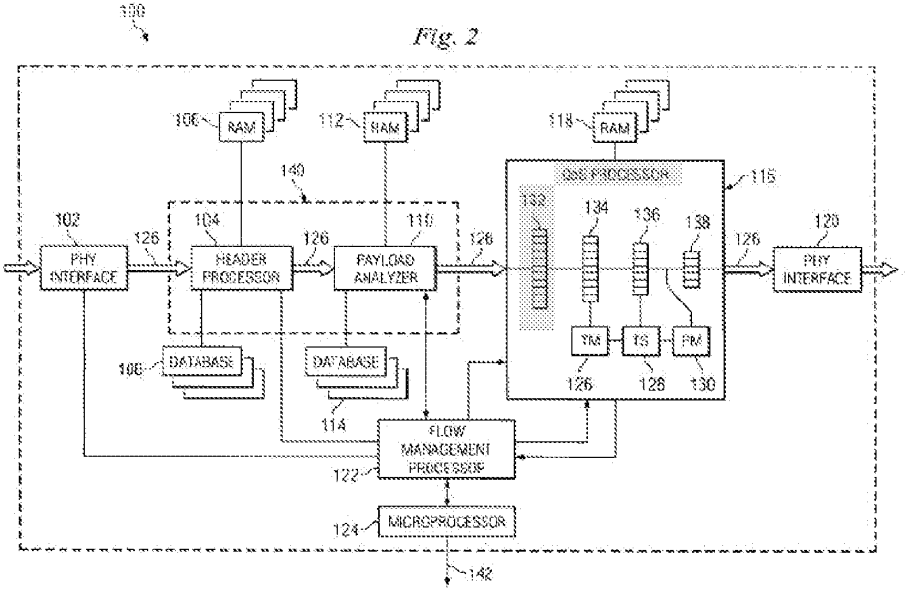


EX1006, Fig. 5 (annotated)

177. 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) are assigned to a different priority QoS queue in the QoS processor 116, where each QoS queue is allocated a different bandwidth rate.

178. For instance, as shown in Fig. 2 below, the QoS processor 116 assigns processing rates (bandwidth) by allocating the received packets to different "quality of service queues 132" based on the determined quality of the received packet (validated or unvalidated data flows).



EX1006, Fig. 2 (annotated)

179. *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).

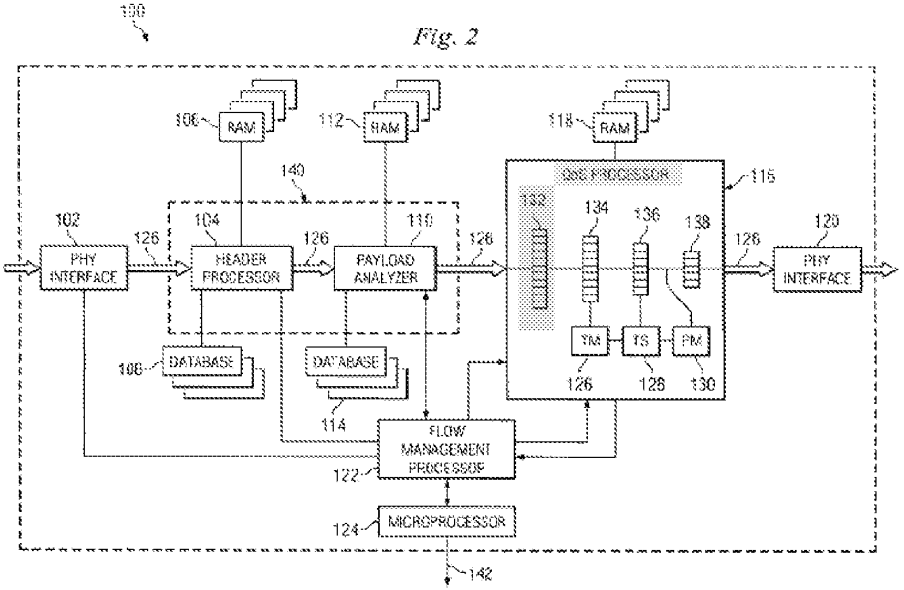
180. Therefore, *Maher* teaches limitation [7.3]. A POSITA would have been motivated to modify *Savage* in view of *Maher* and *Schuba* for the reasons presented above in Sections IX.F.3 and X.A[7.2]. As discussed above with respect to limitation [7.2], a POSITA would have been motivated to modify *Savage* 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 *Maher* and *Schuba* in the "bump-in-the-line" device. 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. Accordingly, limitation [7.3] is rendered obvious by *Savage* in view of *Maher* and *Schuba*.

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

181. 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.

182. 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. 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.



EX1006, Fig. 2 (annotated)

183. A POSITA would have been motivated to modify *Savage* to incorporate the rate allocation techniques of *Maher* for the reasons presented above in Section IX.F.3. 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. 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.

B. Proposed Rejection #2: Claim 10 would have been obvious over *Maher* in view of *Savage* and further in view of *Schuba*.

184. It is my opinion that *Maher*, *Savage*, and *Schuba* teach or suggest to a POSITA the subject matter of each and every limitation of claim 10 of the '497 patent.

185. Before I discuss the limitations of claim 10 in view of the teachings of *Maher*, *Savage*, and *Schuba*, it is instructive to identify the differences between claims 7 and 10 of the '497 patent. Claim 10 is generally similar in scope to claim 7. Both claims 7 and 10 are directed to "[a] method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets." However, claim 10 differs from claim 7 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." On the other hand, 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." Thus, some of the features of claim 7 are performed by the host computer, whereas some of the features of claim 10 are performed by a router in the path leading to the host computer. I note that 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]. 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

	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.

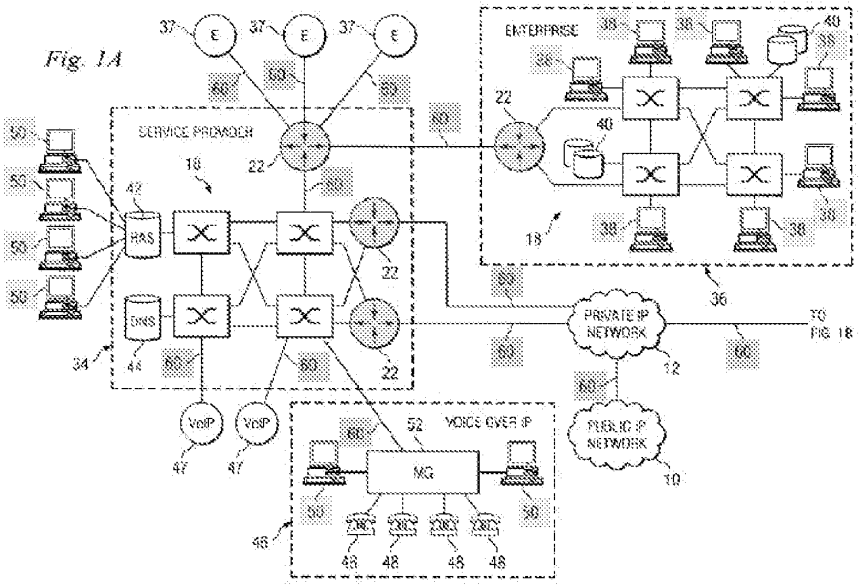
186. The above differences in claim 10 do not make claim 10 patentable. On the contrary, claim 10 would have been obvious to a POSITA over *Maher* in view of *Savage* and *Schuba*, as discussed below.

[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:

187. 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, as recited in limitation [10.0].

188. *Maher* teaches "[a] method and apparatus for preventing denial of service type attacks on data networks." EX1006, Abstract; *see also id.*, 1:8-10 ("the present invention relates to a method and device that prevents denial of service type internet attacks."), 2:52-53 ("The present invention provides for a 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.



EX1006, Fig. 1A (annotated)

189. 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*, as recited in limitation [10.0]. Thus, *Maher* renders obvious limitation [10.0].

[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;

190. 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.

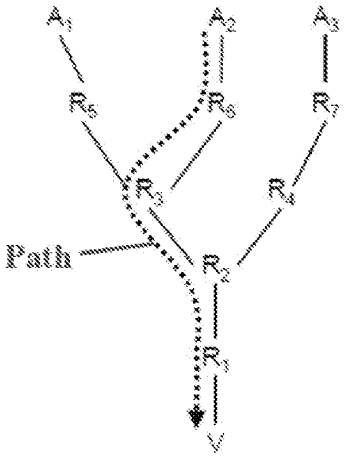


Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1 (annotated)

191. *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 IX.G.2, *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.

192. Thus, *Maher* in view of *Savage* renders obvious limitation [7.1.1].

[10.1.2] said path comprising all routers in said network via which said packets are routed to said computer;

193. 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].

194. Thus, *Maher* in view *Savage* renders obvious this limitation.

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

195. 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).

196. *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 IX.G.2, the classification functions of *Maher* are disclosed as being performed in a router. Therefore, *Maher* also teaches the features of limitation [10.2].

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

197. 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," 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).

198. As described above in Section X.A[7.3], *Maher* discloses the features of limitation [7.3]. *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.

199. *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 or switch."). This is the same technique that is described in the '497 patent. As discussed above in Section VIII.B (¶ 63), the '497 patent discloses with reference to Figures 2-4 that the router allocates a transmission rate for packets to be transmitted to the host computer. EX1001, 6:38-40 (Fig. 2) ("Means are provided for the router 22 to control the rate of transmission of data packets 30 from the router 22 to the computer 18."), 6:49-51 (Fig. 3) ("…the router 22 is capable of controlling the rate of transmission of each class 38 of data packets 30 to the computer 18."), 6:61-63 ("…the router 22 can use the information to allocate the transmission rate for each class 38 in a desired way.").

200. 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. Therefore, *Maher* also teaches the features of limitation [10.3].

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

201. 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).

202. *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].

203. Having described why claims 7 and 10 would have been obvious in Sections X.A and X.B above, I will now turn to claims 13 and 1, which are substantially similar to claim 7, and to claims 16 and 4, which are substantially similar to claim 10. In my analysis of claims 13 and 1 below, I focus primarily on the differences between claims 13 and 1 and claim 7. Similarly, in my analysis of claims 16 and 4 below, I focus primarily on the differences between claims 16 and 4 and claim 10.

C. Proposed Rejection #1 (Claims 13 and 1): Claims 13 and 1 would have been obvious over *Savage* in view of *Maher* and further in view of *Schuba*.

1. Overview of Claim 13

204. 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.

205. 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	[13.1.2]	said path comprising all routers in said network via which said packets

	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;	[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 unwanted data packets.	[10.4]	means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets.

206. 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.

[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:

207. 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].

208. 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.

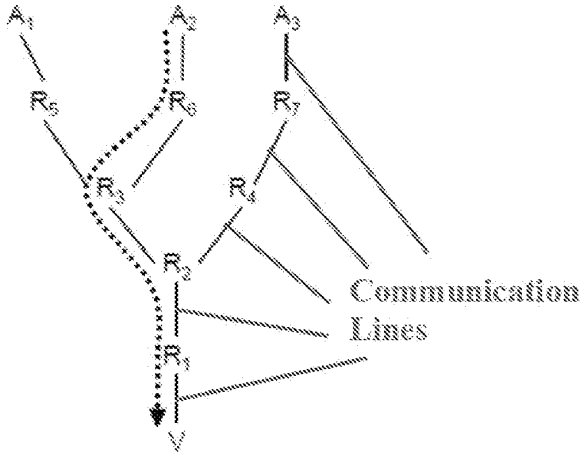


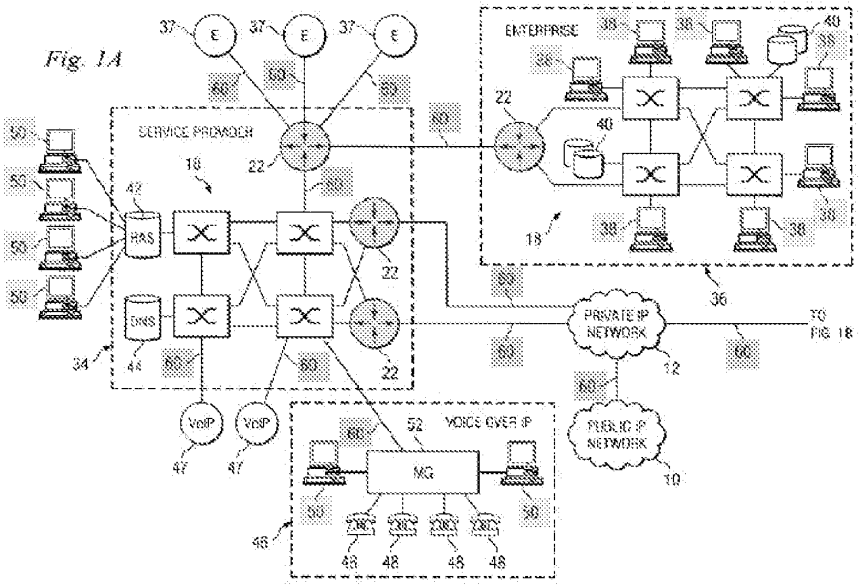
Figure 1: Network as seen from the victim of an attack, V. Routers are represented by R_i, and potential attackers by A_i. The dotted line represents a particular *attack path* between an attacker and the victim.

EX1005, Fig. 1 (annotated)

209. *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.

210. 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.



EX1006, Fig. 1A (annotated)

211. Thus, *Maher* discloses *a packet flooding defense system for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets*.

212. A POSITA would have been motivated to modify *Savage* to incorporate *Maher*'s conventional network implementation details, for the reasons presented above in Section IX.F.1.

213. Accordingly, *Savage* in view of *Maher* renders obvious limitation [13.0].

[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;

214. Limitation [13.1.1] is substantially identical to limitation [7.1.1], except that limitation [13.1.1] additionally recites "*means for*." I have been informed that in a parallel proceeding involving the '497 patent, Patent Owner identified alleged structure in the '047 patent that performs the functions of means-plus-function limitations in the Challenged Claims.

215. I have been informed that Patent Owner has identified that a computer 18 in the embodiments of Figures 1, 4 and 7 is disclosed as *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]. 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].

[13.1.2] said path comprising all routers in said network via which said packets are routed to said computer;

216. 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].

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

217. Limitation [13.2] is substantially similar to limitation [7.2], except that limitation [13.2] additionally recites "means for."

218. I have been informed that Patent Owner has identified that a router 22 in the embodiments of Figures 1, 4 and 7 of the '497 patent is disclosed 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].

219. 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].

[13.3] means for assigning a maximum acceptable processing rate to each class of data packet; and

220. 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).

221. 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].

222. I have been informed that Patent Owner identified that a router 22 in the embodiments of Figures 1, 4 and 7 of the '497 patent is disclosed as performing the function of *assigning a maximum acceptable processing rate to each class of data packet*, as recited in limitation [13.3].

223. 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].

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

224. Limitation [13.4] is substantially identical to limitation [7.4], except that limitation [13.4] additionally recites "means for."

225. I have been informed that Patent Owner identified that a router 22 in the embodiments of Figures 1, 4 and 7 of the '497 patent is disclosed 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].

226. 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].

2. Overview of Claim 1

227. 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].

228. 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 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:	[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:
[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:

229. 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].

[1.1] means for classifying data packets received at a host computer into wanted data packets and unwanted data packets;

230. Limitation [1.1] is substantially similar to limitation [7.2], except that limitation [1.1] recites "means for." I have been informed that Patent Owner has identified that a router 22 in the embodiments of Figures 1, 4 and 7 of the '497 patent is disclosed 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].

231. 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].

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

232. Limitation [1.2] is substantially similar to limitation [7.3], except that limitation [1.1] recites "means for." I have been informed that Patent Owner has