

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

JUNIPER NETWORKS, INC.,
Petitioner,

v.

MONARCH NETWORKING SOLUTIONS LLC,
Patent Owner.

U.S. Patent No. 8,693,369

“Method of Routing a Data Packet in a Network and an Associated Device”

IPR2024-00175

**DECLARATION OF DR. SAMRAT BHATTACHARJEE IN SUPPORT OF
PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 8,693,369**

I.	INTRODUCTION	13
A.	Qualifications	13
B.	Materials Considered.....	16
II.	LEGAL UNDERSTANDINGS.....	16
A.	Claim Construction.....	17
B.	Anticipation	18
C.	Obviousness.....	18
III.	TECHNOLOGY BACKGROUND.....	20
A.	Exhaustion of IPv4 Addresses.....	20
B.	Network Address And Port Translation.....	21
C.	Masks.....	27
IV.	OVERVIEW OF THE '369 PATENT	31
A.	Priority	31
B.	Specification.....	31
1.	Configuration	33
2.	Routing.....	35
V.	LEVEL OF ORDINARY SKILL IN THE ART.....	36
VI.	IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	37
A.	Ground 1: Claims 7-14, 16-17 Are Obvious in View of Biswas and Kumar	37
1.	Biswas (EX1022)	37
2.	Kumar (EX1023).....	39
3.	The Biswas-Kumar Combination	41

4.	Motivations to Combine	42
5.	Claim 7	42
6.	Claim 8: The method according to claim 7 of configuring a piece of terminal equipment, comprising a step of assigning to said piece of terminal equipment an identifier of a routing device adapted to route a data packet comprising said primary address as the destination address to said piece of terminal equipment, and the configuration message further comprising said routing device identifier.....	54
7.	Claim 9: The configuration method according to claim 7, wherein said configuration message is further sent to a routing device that routes to said piece of terminal equipment a data packet containing said primary address as the destination address.....	56
8.	Claim 10	57
9.	Claim 11	60
10.	Claim 12: The configuration method according to claim 11, wherein, once an identifier of a routing device adapted to route a data packet comprising said primary address as the destination address to said piece of terminal equipment has been received, said method further comprises a step of sending the configuration data to said routing device.	64
11.	Claim 13: The configuration method according to claim 11, wherein, on reception of a data packet comprising a destination address, a port number, and a routing identifier, said method further comprises a step of verifying that the port number belongs to the range of port numbers defined by the port mask, and a step of rejecting said packet if result of the verification is negative.	66
12.	Claim 14.....	70

13.	Claim 16: A non-transitory computer readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 7.....	71
14.	Claim 17: A non-transitory computer-readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 11.....	71
B.	Ground 2: Claims 1-3, 5-6, and 15 Are Obvious in View of Fangman and Kumar	71
1.	Fangman (EX1024).....	72
2.	The Fangman-Kumar Combination	74
3.	Motivations to Combine	75
4.	Claim 1	75
5.	Claim 2: The method according to claim 1 of routing an IP data packet, wherein said at least one identifier is a secondary destination address of the destination equipment.....	89
6.	Claim 3: The method according to claim 2 of routing an IP data packet, comprising, before the routing step, a step of transforming the packet by adding said secondary address to the packet, and routing the packet based on said secondary destination address.	90
7.	Claim 5	90
8.	Claim 6.....	92
9.	Claim 15: A non-transitory computer readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 1.....	94
C.	Ground 3: Claims 1-3, 5-6, and 15 Are Obvious in View of King and Kumar	94

1.	King (EX1025).....	94
2.	The King-Kumar Combination	96
3.	Reasons to combine King and Kumar	97
4.	Claim 1	97
5.	Claim 2: The method according to claim 1 of routing an IP data packet, wherein said at least one identifier is a secondary destination address of the destination equipment.....	108
6.	Claim 3: The method according to claim 2 of routing an IP data packet, comprising, before the routing step, a step of transforming the packet by adding said secondary address to the packet, and routing the packet based on said secondary destination address.	108
7.	Claim 5	109
8.	Claim 6.....	111
9.	Claim 15: A non-transitory computer readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 1.....	112
D.	Ground 4: Claim 4 Is Obvious in View of Fangman, Kumar and RFC 791	112
1.	RFC 791 (EX1026).....	112
2.	Claim 4: The routing method according to claim 1, wherein the at least one identifier is a route identifier specific to said destination equipment and the packet is routed based on said specific route identifier.	115
E.	Ground 5: Claim 4 Is Obvious in View of King, Kumar and RFC 791	117
1.	Claim 4: The routing method according to claim 1, wherein the at least one identifier is a route identifier	

specific to said destination equipment and the packet is
routed based on said specific route identifier. 117

VII. CONCLUSION.....119

PETITIONER'S EXHIBIT LIST

EX1001	U.S. Patent No. 8,693,369 to Mohamed Boucadair (“’369 patent”)
EX1002	Prosecution history of U.S. Patent No. 8,693,369 (“’369 Prosecution History”)
EX1003	Declaration of Dr. Samrat Bhattacharjee under 37 C.F.R. § 1.68
EX1004	<i>Curriculum Vitae</i> of Dr. Bhattacharjee
EX1005	Declaration of Dr. Sylvia Hall-Ellis under 37 C.F.R. § 1.68
EX1006	P. Richter et al., “A Primer on IPv4 Scarcity,” (Feb. 27, 2015), available at https://arxiv.org/pdf/1411.2649.pdf
EX1007	H. Yeom et al., “IP Multiplexing by Transparent Port-Address Translator,” 10th USENIX System Administration Conference (LISA X) (Sept. 29, 1996), available at https://www.usenix.org/conference/lisa-96/ip-multiplexing-transparent-port-address-translator
EX1008	RFC 3022 (Traditional NAT), dated January 2001, available at https://datatracker.ietf.org/doc/html/rfc3022
EX1009	U.S. Patent Application Publication No. 2002/0016826 to Johansson et al. (“Johansson”)
EX1010	A. Reitz, “The Dynamic Port Reservation Protocol,” Univ. Ill. at Urbana-Champaign (2001), available at http://redefine.dyndns.org/~andyr/documents_and_writings/thesis/docs/areitz_msthesis.pdf
EX1011	M. Shin et al., “Using a Single IPv4 Global Address in DSTM,” Internet Engineering Task Force (“IETF”) (Feb. 22, 2001), available at https://www.ietf.org/archive/id/draft-shin-dstm-single-ipv4-00.txt (“Shin”)
EX1012	U.S. Patent No. 7,356,045 to Satapati et al. (“Satapati”)

EX1013	U.S. Patent Application Publication No. 2003/0154306 to Perry (“Perry”)
EX1014	RFC 950 (Internet Standard Subnetting Procedure), dated August 1985, available at https://datatracker.ietf.org/doc/html/rfc950
EX1015	U.S. Patent No. 7,624,195 to Biswas et al. (“Biswas-195”)
EX1016	WO Publication No. 01/02965 A2 to Herbst et al. (“Herbst”)
EX1017	RFC 7597 (Mapping of Address and Port with Encapsulation), dated July 2015, available at https://datatracker.ietf.org/doc/html/rfc7597
EX1018	RFC 4632 (Classless Inter-domain Routing), dated August 2006, available at https://datatracker.ietf.org/doc/html/rfc4632
EX1019	U.S. Patent Application No. 10/873,547 to Tornetta et al. (“Tornetta”)
EX1020	U.S. Patent No. 7,873,038 to LaVigne et al. (“LaVigne”)
EX1021	U.S. Patent Application No. 11/699,765 to McAlister (“McAlister”)
EX1022	U.S. Patent No. 8,019,889 to Biswas et al. (“Biswas”)
EX1023	U.S. Patent No. 7,394,809 to Kumar et al. (“Kumar”)
EX1024	U.S. Patent No. 7,068,647 to Fangman et al. (“Fangman”)
EX1025	U.S. Patent No. 8,032,639 to King et al. (“King”)
EX1026	RFC 791, Internet Protocol Specification (September 1981), available at https://datatracker.ietf.org/doc/html/rfc791
EX1027	U.S. Patent No. 5,014,221 to Mogul (“Mogul”)
EX1028	U.S. Patent No. 5,163,131 to Row et al. (“Row”)
EX1029	July 20, 2006 Capture of RFC 791, Wayback Machine, available at https://web.archive.org/web/20060720182319/http://www.ietf.org/rfc/rfc791.txt

EX1030	Michael Witt, A Comment on Current Source Routing Techniques (1987), available at https://dl.acm.org/doi/pdf/10.1145/36727.36728
EX1031	Andrew Tanenbaum, Computer Networks (5th Ed. 2011)
EX1032	Monarch's Opposition to Juniper's Motion to Transfer, <i>Monarch Networking Solutions LLC v. Juniper Networks, Inc.</i> , No. 1:23-cv-670-TSE-LRV (E.D. Va. Oct. 3, 2023), ECF No. 52
EX1033	PTO Reexamination Operational Statistics, available at https://www.uspto.gov/learning-and-resources/statistics/reexamination-information
EX1034	Complaint, <i>Monarch Networking Solutions LLC v. Juniper Networks, Inc.</i> , No. 1:23-cv-670-TSE-LRV (E.D. Va. May 23, 2023), ECF No. 1
EX1035	Unified EPR (Control No. 90/015,315), filed on October 23, 2023

LIST OF CHALLENGED CLAIMS

Claim	Limitation
1[pre]	A method of routing an IP data packet in a telecommunications network to a destination equipment, said packet comprising a primary destination address and a destination port number, said method comprising, on reception of said packet, the following steps:
1[a]	determining a port mask assigned to the destination equipment, the port mask defining a range of port numbers to which the destination port number belongs;
1[b]	selecting at least one identifier of the destination equipment of the packet from a plurality of equipment identifiers associated with said primary destination address based on the port mask; and
1[c]	routing the packet to the destination equipment based on said identifier.
2	The method according to claim 1 of routing an IP data packet, wherein said at least one identifier is a secondary destination address of the destination equipment.
3	The method according to claim 2 of routing an IP data packet, comprising, before the routing step, a step of transforming the packet by adding said secondary address to the packet, and routing the packet based on said secondary destination address.
4	The routing method according to claim 1, wherein the at least one identifier is a route identifier specific to said destination equipment and the packet is routed based on said specific route identifier.
5[pre]	A device for routing an IP data packet in a telecommunications network to a destination equipment, said packet comprising a primary destination address and a destination port number, wherein said device comprises, on reception of said packet:
5[a]	a processor that determines a port mask assigned to the destination equipment, the port mask defining a range of port numbers to which the destination port number belongs;

Claim	Limitation
5[b]	the processor selects an identifier of the destination equipment of the packet from a plurality of equipment identifiers associated with said primary destination address based on the port mask; and
5[c]	a communication unit that routes the packet to the destination equipment based on said identifier.
6[pre]	Telecommunications network equipment adapted to receive an IP data packet comprising a primary destination address and a destination port number, comprising at least one routing device comprising:
6[a]	a processor that determines a port mask assigned to a destination equipment, the port mask defining a range of port numbers to which the destination port number belongs;
6[b]	the processor selects an identifier of the destination equipment of the packet from a plurality of equipment identifiers associated with said primary destination address based on the port mask; and
6[c]	a communication unit that routes the packet to the destination equipment based on said identifier.
7[pre]	A method of configuring a piece of terminal equipment connected to a telecommunications network, comprising, on reception of a configuration request sent by said equipment, the following steps:
7[a]	assigning to said piece of terminal equipment a primary address shared with a plurality of pieces of terminal equipment;
7[b]	assigning to said piece of terminal equipment a port mask defining a range of numbers dedicated to it and a routing identifier; and
7[c]	sending to said piece of terminal equipment a configuration message comprising said primary address, said port mask, and said routing identifier.
8	The method according to claim 7 of configuring a piece of terminal equipment, comprising a step of assigning to said piece of terminal equipment an identifier of a routing device adapted to route a data packet comprising said primary address as the destination address to said piece of terminal equipment, and the

Claim	Limitation
	configuration message further comprising said routing device identifier.
9	The configuration method according to claim 7, wherein said configuration message is further sent to a routing device that routes to said piece of terminal equipment a data packet containing said primary address as the destination address.
10[pre]	A configuration server in a telecommunications network, wherein, on reception of a configuration request sent by a piece of terminal equipment, comprising:
10[a]	a processor that assigns a primary address to said piece of terminal equipment, said primary address being shared with a plurality of pieces of terminal equipment;
10[b]	the processor assigns to said piece of terminal equipment a port mask defining a range of numbers dedicated to it and a routing identifier; and
10[c]	a communication unit that sends to said piece of terminal equipment a configuration message comprising said primary address, said port mask, and said routing identifier.
11[pre]	A method of configuring a piece of terminal equipment connected to a telecommunications network, wherein, on reception of a configuration message comprising configuration data comprising a primary address, a port mask defining a range of port numbers that is dedicated thereto, and a routing identifier, said method comprises the following steps:
11[a]	storing said configuration data; and
11[b]	before sending a data packet into the telecommunications network, selecting a port number in the range of port numbers defined by the port mask, said data packet comprising as source address the primary address of said piece of terminal equipment and as source port number the selected port number.
12	The configuration method according to claim 11, wherein, once an identifier of a routing device adapted to route a data packet comprising said primary address as the destination address to said

Claim	Limitation
	piece of terminal equipment has been received, said method further comprises a step of sending the configuration data to said routing device.
13	The configuration method according to claim 11, wherein, on reception of a data packet comprising a destination address, a port number, and a routing identifier, said method further comprises a step of verifying that the port number belongs to the range of port numbers defined by the port mask, and a step of rejecting said packet if result of the verification is negative.
14[pre]	A piece of client terminal equipment connected to a telecommunications network, wherein, on reception of a configuration message comprising configuration data comprising a primary address shared with a plurality of pieces of terminal equipment, a port mask defining a range of port numbers that is dedicated to the piece of client terminal equipment, and a routing identifier, the piece of client terminal equipment comprising:
14[a]	a memory that stores said configuration data;
14[b]	before sending a data packet in the telecommunications network, a processor that selects a port number in the range of port numbers defined by the port mask, said data packet comprising as source address the primary address of said piece of client terminal equipment and as source port number the selected port number.
15	A non-transitory computer readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 1.
16	A non-transitory computer readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 7
17	A non-transitory computer-readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 11.

I. INTRODUCTION

1. I have been retained by Quinn Emanuel Urquhart & Sullivan, LLP on behalf of Juniper Networks, Inc. (“Juniper” or “Petitioner”) as an independent expert in this *inter partes* review before the Patent Trial and Appeal Board of the United States Patent and Trademark Office to review claims 1-17 (“Challenged Claims”) of U.S. Patent No. 8,693,369 (“the ’369 patent”). I have been asked by Petitioner to assist in evaluating the claims and the disclosure of the ’369 patent.

2. I understand that the ’369 patent is currently asserted in a litigation by Monarch Networking Solutions LLC (“Monarch” or “Patent Owner”) against Petitioner in *Monarch Networking Solutions LLC v. Juniper Networks, Inc.*, Case No. 4:23-cv-05076 (N.D. Cal.).

A. Qualifications

3. I provide below an overview of my background and qualifications.

4. I earned a Ph.D. in Computer Science from Georgia Institute of Technology in 1999. Before that, I earned Bachelor of Science degrees in Mathematics and Computer Science from Georgia College and State University in 1994. I was a Teaching Assistant at the Georgia Institute of Technology from 1994 to 1995 and an Instructor in 1998.

5. From 1999 through 2005, I was an Assistant Professor at the University of Maryland, College Park, in the Department of Computer Science, and then an

Associate Professor with tenure from 2005 through 2009. In 2006, I was a Visiting Professor at Max Planck Institut für Software Systems in Saarbrücken, Germany. In 2007, I was a Visiting Researcher at AT&T Labs in Florham Park, New Jersey.

6. Since 2009, I have been a tenured Professor at the University of Maryland. My teaching and research have focused on computer networking and other aspects of the technologies pertaining to the '369 patent. My Ph.D. dissertation was on the design of novel network architectures, and I have been teaching NAT, NAPT, and various address realm architectures in my undergraduate and graduate courses since 1999.

7. I served as a reviewer for ACM/IEEE Transactions on Networking, IEEE Journal on Selected Areas in Communications, Computer Communications Journal (Special Issue on Network Security), ACM Transactions on Computer Systems, Performance Evaluation Journal, Computer Communications Review, European Transactions on Telecommunications, IEEE Transactions on Parallel and Distributed Systems, and ACM Transactions on Internet Technology.

8. I am the author of numerous publications in the field of networking, including journal articles, book chapters, publications in proceedings, technical reports, and invited papers.

9. I have been active in a number of professional organizations and conferences. I have served with the National Science Foundation (NSF) Workshop

on Network Testbeds, the NSF Networking Research Panel, the Department of Education High Performance Networking Panel, and as an Evaluator for the Intel Science Talent Search.

10. I have received several honors and awards. These include the Alfred P. Sloan Jr. Fellowship; the Best Paper Award, 14th Annual IEEE International Conference on High Performance Computing (HiPC) (with Vijay Gopalakrishnan, Ruggero Morselli, Peter Keleher, and Aravind Srinivasan); the Best Paper Award, 7th IEEE/ACM Conference on Grid Computing (with Jiksoo Kim, Byomsuk Nam, Peter Keleher, Michael Marsh, and Alan Sussman); and the NSF CAREER Award. I also received Teaching Excellence Awards in 2004, 2008, and 2012.

11. In 2017, along with colleagues from Cornell University and the Max Planck Society in Germany, I started an annual school for introducing undergraduate students from across the world to research. This school is partially supported by the NSF and had student participants from 29 countries.

12. I am also the co-director of a new joint Ph.D program in computer science between the University of Maryland and the Max Planck Society in Germany.

13. Additional details of my education and employment history, professional service, patents, publications, and other testimony are set forth in my current curriculum vitae, which is attached as Petitioner's Exhibit 1004.

B. Materials Considered

14. In forming my opinions, I have considered the '369 patent specification, including the Abstract, the figures, and the claim language itself, as would have been understood by a person having ordinary skill in the art. I have also reviewed the file history of the '369 patent, the exhibits listed within the petition, and any other material cited in the petition and this declaration.

15. In forming my opinions, I have relied on my personal knowledge and professional experience in designing, developing, deploying, or using software related to computer networks, Network Address Translation, Port Address Translation, IPv4, IPv6, and related technologies, and on the documents and information referenced in this declaration.

16. I am being compensated for my time spent on this matter at a rate of \$700 per hour, and my compensation is in no way contingent upon the outcome of this matter or on the opinions I offer.

II. LEGAL UNDERSTANDINGS

17. In this section, I describe my understanding of certain legal standards that I have relied upon in forming my opinions set forth in this declaration. I am not an attorney. I have been informed of these legal standards by Petitioner's attorneys.

18. I understand that the claims define the invention. I also understand that an unpatentability analysis is a two-step process. First, the claims of the patent are

construed to determine their meaning and scope. Second, after the claims are construed, the content of the prior art is compared to the construed claims.

19. I understand that a claimed invention is only patentable when it is new, useful, and non-obvious in light of the “prior art.” That is, the invention, as defined by the claims of the patent, must not be anticipated by or rendered obvious by the prior art.

A. Claim Construction

20. I understand that the United States Patent and Trademark Office interprets claim terms in an inter partes review proceeding under the “*Philips*” claim construction standard. I understand that under this standard, the meaning of claim terms is considered from the viewpoint of one of ordinary skill in the art at the time of the alleged invention. For this declaration, I have been asked to apply March 31, 2008 as the priority date for the ’369 patent, which is the date I have used for claim interpretation purposes. However, the interpretations that I provide below would have also been correct if the date of alleged invention was a year earlier or later.

21. I have been informed that, for the purposes of my analysis in this IPR proceeding, the terms appearing in the claims of the ’369 patent should be interpreted according to how a POSITA would have understood the claim terms at the time of the earliest priority date, in light of the patent specification, the prosecution history, and any other relevant intrinsic and extrinsic evidence.

B. Anticipation

22. I understand that a patent claim is anticipated when a single piece of prior art describes every element of the claimed invention, either expressly or inherently, arranged in the same way as in the claim. For inherent anticipation to be found, it is required that the missing descriptive material is necessarily present in the prior art. I understand that, for the purpose of an *inter partes* review, prior art that anticipates a claim can include both patents and printed publications from anywhere in the world.

C. Obviousness

23. I understand that a patent may not be valid even though the invention is not identically disclosed or described in the prior art if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art in the relevant subject matter at the time the invention was made.

24. I understand that the following factors are evaluated to determine whether the claimed subject matter is obvious: (1) the scope and content of the prior art; (2) the difference or differences, if any, between each claim of the patent and the prior art; and (3) the level of ordinary skill in the art at the time the patent was filed. Unlike anticipation, which allows consideration of only one prior art reference, I

understand that obviousness may be shown by considering more than one prior art reference.

25. I understand that the following rationales may be used to determine whether a piece of prior art can be combined with other prior art or with other information within the knowledge of one of ordinary skill in the art:

- Combining prior art elements according to known methods to yield predictable results;
- Simple substitution of one known element for another to obtain predictable results;
- Use of known techniques to improve similar devices (methods, or products) in the same way;
- Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
- “Obvious to try” - choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
- Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; or

- Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

26. Moreover, I understand that certain secondary considerations may be considered in evaluating obviousness in order to prevent hindsight bias. These secondary considerations may include : (1) commercial success; (2) long-felt but unresolved needs; (3) copying of the invention by others in the field; (4) initial expressions of disbelief by experts in the field; (5) failure of others to solve the problem that the inventor solved; and (6) unexpected results. I also understand that evidence of objective indicia of non-obviousness must be commensurate in scope with the claimed subject matter.

III. TECHNOLOGY BACKGROUND

A. Exhaustion of IPv4 Addresses

27. Internet Protocol Version 4 (“IPv4”), described in RFC 791 (September 1981), is a standard for communicating over the Internet by sending a data packet from a source to a destination computer. Both the source computer and the destination computer have IPv4 addresses that inform the network where to route data packets. EX1006, 1. An IPv4 address consists of 32 bits—*i.e.*, 1s and 0s. The following is an example of an IPv4 address in binary form:

11000000 10101000 00000000 00000001

28. IPv4 addresses are often depicted using the “dotted quad” notation for easier readability. The following is the dotted quad notation of the above IPv4 address:

192.168.0.1

29. There is a finite number of possible IPv4 addresses, approximately 4 billion. Long before the '369 patent was filed, “[t]he Internet engineering community ... recognized the impending exhaustion of IPv4” addresses and began developing means for combating the exhaustion. EX1006, 1, 8-9.

B. Network Address And Port Translation

30. One of these ideas for addressing the exhaustion of IPv4 addresses, disclosed in the 1990s, is called Port Address Translation (“PAT”).¹ EX1007, 113. PAT techniques are described in various prior art documents and publications, including RFC 3022 that was issued in January of 2001 and is entitled “Traditional Network Address Translator (Traditional NAT).” EX1008.

¹ PAT itself is a variation of Network Address Translation (“NAT”), another network configuration that allows internal clients to access the Internet via a single global IPv4 address. EX1007, at 113; EX1006, at 8-9. PAT is sometimes referred to as Network Address And Port Translation (“NAPT”).

31. PAT recognizes that computers have 2^{16} (approximately 65,000) ports—*i.e.*, connection points that computers use to access different services, like websites, file transfer protocols, or online applications. EX1007, 113. “[T]here are a lot of ports in a node and only a small portion of them are used at any time.” *Id.*, 115. PAT utilizes these unused ports to share one “global” IPv4 address among multiple computers. *Id.* Accordingly, each computer does not need its own public IPv4 address, thereby mitigating IPv4 address exhaustion. *Id.*

32. Specifically, PAT implements an internal network that contains multiple internal clients (*e.g.*, servers, personal computers, smartphones, smart appliances). *Id.*, 114. A proxy server sits on the edge of the internal network and routes all communications between these internal clients and an outer network (*e.g.*, the Internet). *Id.* For example, if an internal client (orange), such as a personal computer, wants to communicate with a device on the outer network (purple), it will first send its request to the proxy server (red), which will then route the request to the external server. An embodiment of this implementation is pictured below:

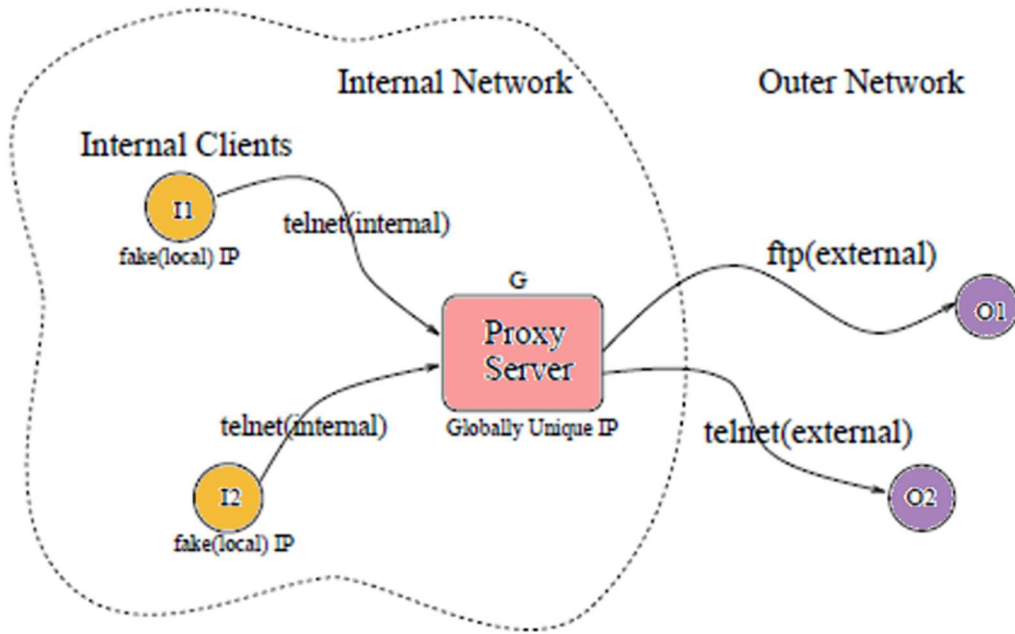


Figure 1: Connecting through a Proxy Server

Id. (colors added).

33. In a PAT implementation, the internal clients do not have public IPv4 addresses. *Id.*, 114-15. Instead, the internal clients have a local IP address that is known only within the internal network, not the Internet at large. *Id.* The proxy server, on the other hand, does have a public IPv4 address and shares this single public IPv4 address with the internal clients. *Id.* When an internal client wants to send a data packet to a device on the outer network, it sends the packet to the proxy server. *Id.*, 115-16. The proxy server modifies the incoming data packet, replacing (1) the internal client's local IP address with the proxy server's global IPv4 address and (2) the internal client's port number with one of the proxy server's port numbers. *Id.*, 115. The proxy server then stores this association before ultimately routing the

data packet to the device on the outer network. *Id.* If the device on the outer network sends a data packet back to the internal client, the proxy server will know where to send the incoming data packet based on the destination port number in the received packet. *Id.*

34. For example, internal client I1 wants to send a data packet to outer client O1, so it constructs a data packet containing the following information:

Source IP Address	Source Port Number	Destination IP Address	Destination Port Number
I1	1000	O1	23

Id. Internal client I1 transmits the data packet. *Id.* Proxy server G intercepts the packet and edits the packet header in the following manner, replacing the source IP address and source port number:

Source IP Address	Source Port Number	Destination IP Address	Destination Port Number
H G	1000 3000	O1	23

Id. Proxy server G then stores the association between its port number 3000 and internal client I1's internal address and port number 1000. *Id.*, 116. After receiving and processing the data packet, outer client O1 might send the following data packet back to proxy server G in response:

Source IP Address	Source Port Number	Destination IP Address	Destination Port Number
O1	23	G	3000

Id., 115. Proxy server G searches its database and finds an entry that associates its port number 3000 with inner client I1's internal address and port number 1000, and modifies the incoming data packet accordingly:

Source IP Address	Source Port Number	Destination IP Address	Destination Port Number
O1	23	G I1	~~3000~~ 1000

Id. Proxy server G then routes the data packet to inner client I1, completing the PAT process. Thus, PAT is able to use a single public IPv4 address, with the help of unused port numbers, to service multiple internal computers.

35. Since the first disclosure of PAT in the 1990s, numerous public documents have discussed PAT and variations of PAT.

36. In 2001, U.S. Patent Application No. 09/904,837 ("Johansson") discussed a network setup that "map[s] internal addresses" to "external addresses" "using ports 20000 to 20255." Ex. 1007, ¶¶ 54-55. "In this way, the 256 external addresses together with the 256 ports can represent the 65536 addresses of the internal network." *Id.*, ¶ 56.

37. In 2001, Andrew Joseph Reitz published his thesis on "dynamic port reservation protocol," such that "[w]hen an application decides that it needs inbound connectivity from the outside world, it can send a 'protocol port request' message" to a gateway that "will examine its internal translation tables and satisfy

the request with an appropriate port.” EX1010, 15-16. The internal clients are therefore able to “reserve ports” on their local gateways. *Id.*, 45.

38. In February 2001, Myung-Ki Shin et al. published an IETF Internet Draft entitled “Using a Single IPv4 Global Address in DSTM.” EX1011. Like the ’369 patent, Shin recognizes that if a large number of hosts in a local network “want to get IPv4 addresses,” then “a lot of IPv4 global address[es] will be needed.” *Id.*, 1. Shin therefore describes a way to share “a single IPv4 global address” by assigning “TCP/UDP port range[s]” to the hosts within its network. *Id.* Specifically, Shin describes assigning “a single IPv4 global address with TCP/UDP port range” to a plurality of dual-stack hosts, thus enabling the dual-stack hosts “to communicate with IPv4 only hosts using a single IPv4 global address only.” *Id.*, Abstract. “The proposed mechanism can increase the utilization of IPv4 addresses when the pool of IPv4 addresses assigned ... is exhausted.” *Id.*, 1.

39. In 2002, U.S. Application No. 10/278,327, later issued as U.S. Patent No. 7,356,045, (“Satapati”) described prior art PAT implementations, including “where port numbers are used to further identify different devices with the same address.” EX1012, 1:7-4:4. Satapati describes a variation of PAT that can simultaneously serve both IPv4 internal clients and IPv6 internal clients. *Id.*, 4:8-19.

40. In early 2003, U.S. Patent Application No. 10/347,374 (“Perry”) disclosed a variation of PAT for “dynamic inbound connectivity to hosts addressed with a private IP address.” EX1013, ¶ 22. This variation, termed Reverse Port Address Translation (“RPAT”) “maps the private address to the dynamic port assigned for the session and maintains a log of these address mappings, defined as an address table, so that it can intercept inbound packets and rewrite the packet header with the private address before forwarding, and vice versa.” *Id.*, ¶ 70. Figure 7 of Perry depicts the invention, in which it sequentially assigns port numbers for each connection opened on an internal device:

FIG.7 Address table diagram showing mappings of dynamically assigned port numbers to privately addressed hosts.

Destination Computer's IP Address	Assigned Port Number	Source Computer's IP Address	Source Port Number
192.168.32.10	50101	215.37.32.203	2400
192.168.32.12	50102	128.45.22.5	3345
192.168.32.15	50103	199.5.9.33	5601
192.168.32.18	50104	201.12.19.6	5999

Id., Fig. 7.

C. Masks

41. Masks are an efficient way of defining a range of numbers and determining whether a number is within that range. Masks are a bit operation, which

means they are performed on binary numbers. For example, masks can be used to determine whether a number is within the range 0-15. In binary representation, that would be between 0 (corresponding to 0) and 1111 (corresponding to 15). Forming a mask for this range simply requires inverting the larger number and then padding the left side of that inverted number with binary 1s. For example, a mask for the range 0-15 could be 1111110000.

42. Masks work by performing bitwise operations on the number that is being evaluated and the mask itself. For example, the mask device might receive a number 0011100010 and want to know if that received number falls within the range 0-15. The device would perform a binary AND operation between every digit of the received number and every digit of the mask. A binary AND operation outputs a binary 1 if, and only if, the two inputted numbers are also 1s. For example, performing a binary AND between the received number, 0011100010, and the mask, 1111110000, would produce the result 0011100000, since the digits at the third, fourth, and fifth position of both numbers are binary 1s. Because the result is a non-zero number, the received number is outside of the range. This makes sense intuitively—the received number, converted to decimal format (also known as base-10 format, which is the format that we typically use in our day-to-day lives), is 226, which is outside of the range 0-15.

43. A further example, the mask might receive a number 0000000110 and want to know if that received number falls within the range 0-15. Again, the device would first perform a binary AND operation between every digit of the received number and every digit of the mask. Performing a binary AND between the received number, 0000000110, and the mask, 1111110000, would produce the result 0000000000 because the received number does not have a binary 1 in the same digit place as the mask. Because the result equals zero, the received number is within the range. This also makes sense—the received number, converted to decimal format is 6, which is inside of the range 0-15.

44. Using masks in this manner has been known in the field of computer networking for decades. For example, RFC 950, which was published in August 1985, describe using “a bit mask (‘address mask’) to identify which bits of the local address field indicate the subnet number.” EX1014, 4. In other words, the mask in RFC 950 is used to determine whether a received data packet that contains an IP address falls within a range of addresses within the network.

45. RFC 4632, which was published in August 2006, also describes masks that are used to represent a range of IP addresses. EX1018, 15-16.

46. The '369 patent uses masks in order to define a port range. EX1001, 7:40-67. This too was well known in the prior art. In addition to the references discussed below, other references, like U.S. Patent No. 7,624,195 (“Biswas-195”),

which was filed on May 8, 2003 and published on November 24, 2009, explains that “[i]f port ranges were used, one convenient mechanism that could be used to quickly route messages based on port range is by extending subnetting concepts [*i.e.*, subnet masks] to port ranges.” EX1015, 7:42-54. Biswas-195 explains that “[a] 16-bit port number could be viewed” as four sets of four bytes; for example, 0000.0000.0011.1111. *Id.* “A subnet mask ... would then be used to distinguish subnets” according to these port numbers. *Id.* For example, the subnet mask of 1111.1111.1100.0000 could be used to define a port range between 0000.0000.0000.0000 and 0000.0000.0011.1111, in the same way I explain above. *Id.*

47. Additionally, WO 01/02965 (“Herbst”), published January 11, 2001, discusses using mask to filter data packets according to the content of the packets, including their port numbers. EX1016, 40:14-41:8, 43:6-11.

48. There are many other examples of masks being used to define an exact value or range of values in a computer system. For example, US Patent No. 7,623,519 (“Tornetta”), filed on June 21, 2004 and granted on November 24, 2009, discusses using bit masks to enable and disable routing rules in a network switch. EX1019, 11:41-49, 15:16-22.

49. Additionally, U.S. Patent No. 7,873,038 (“LaVigne”), filed on April 30, 2007 and granted on January 18, 2011, teaches using masks on network devices like

routers, switches, hubs, servers, etc. to “indicate a particular port is a member of a particular membership group.” EX1020, 3:8-42.

50. And U.S. Application No. 11/699,765 (“McAlister”), filed January 30, 2007, uses “destination address/mask combinations” to “determine if the packets are to be further processed or dropped.” EX1021, ¶17. For example, to determine if a network policy applies to a received packet. *Id.*, ¶23.

51. In summary, masks were ubiquitous and well-known in the field of computing and computer networking. Masks are used in a variety of applications and are well-known for use in defining a range of numbers and even defining a range of port numbers.

IV. OVERVIEW OF THE '369 PATENT

A. Priority

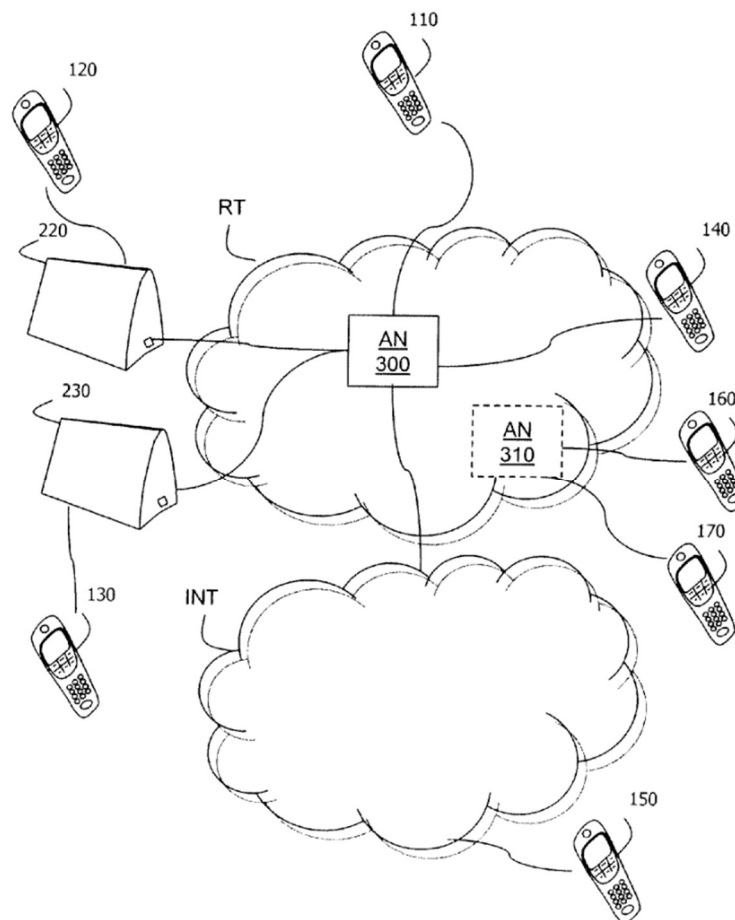
52. I am informed that because the prior art cited in this petition predates the earliest possible priority date of the '369 patent (March 31, 2008), each cited reference herein qualifies as prior art under at least one of pre-AIA 35 U.S.C. §§ 102(a), (b), and/or (e).

B. Specification

53. The '369 patent explains that “the exhaustion of public IPv4 addresses is inevitable” due to the discrete number of IPv4 addresses and the ever-increasing number of devices connected to the Internet. EX1001, 1:53-54. The patent claims that “[t]he inventors have found that pieces of terminal equipment do not make use

simultaneously of all the 2^{16} (i.e. 65536) port number values available thereto.” *Id.*, 7:22-35. Thus, the “general principle of the invention relies on assigning the same primary address to a plurality of pieces of terminal equipment,” along with a “port mask defining a range of port numbers” that serves to distinguish each piece of equipment with the same primary address. *Id.*, 7:12-17. By allowing pieces of terminal equipment to share an address, the ’369 patent purports to provide a solution that “economiz[es] the use of public IP addresses.” *Id.*, 2:45-50.

54. Figure 3 illustrates an embodiment of the alleged invention:



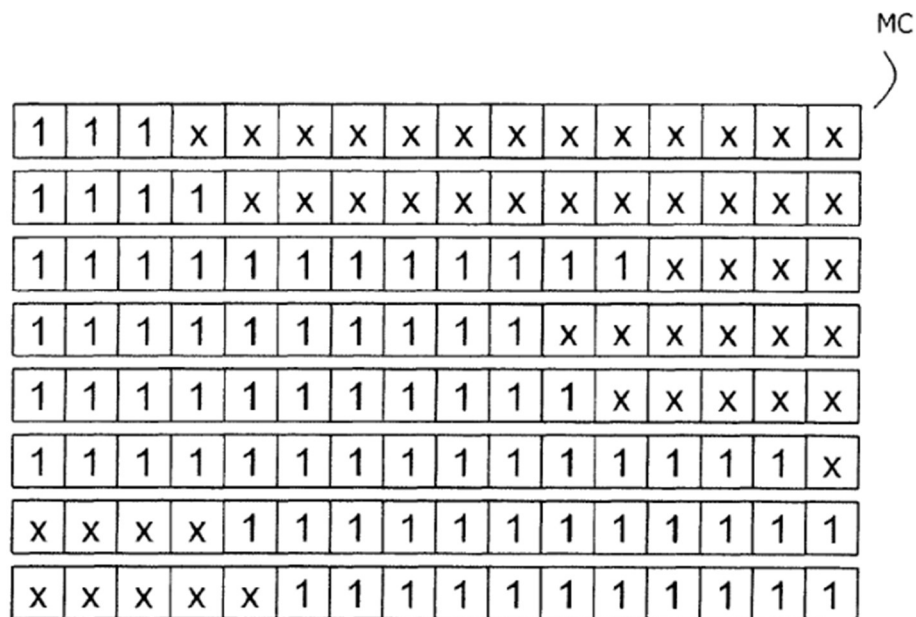
Id., Fig. 3.

1. Configuration

55. To effect its disclosures, the '369 patent describes “a method of configuring terminal equipment connected to a telecommunications network.” *Id.*, 4:58-61.

56. To start the configuration process, the terminal equipment (*e.g.*, **100**, **130**, **200**) “sends a configuration request to the IP connectivity service ... in a known manner,” for example, a DHCP request. *Id.*, 9:36-53. The IP connectivity service assigns the terminal equipment a primary address (which, in one embodiment, is a public address) that is shared with multiple other terminal equipment. *Id.*, 9:54-63. The terminal equipment is further assigned a range of port numbers dedicated to the terminal equipment. *Id.* For example, a first terminal equipment might be assigned port numbers 0-255, while a second terminal equipment might be assigned port numbers 256-511, and so on. *Id.*, 7:36-67.

57. The port ranges are defined by “port masks,” which are 16-bit numbers that represent the assigned port range. *Id.* For example, Figure 2A depicts several embodiments of as “continuous masks” in which the range associated with the mask is “a continuous and unique range”:

**FIG. 2A**

Id., Fig. 2A, 7:55-61. The patent also provides examples of non-contiguous port masks. *Id.*, 7:62-67, Fig. 2B.

58. Finally, the terminal equipment in the network is assigned a “routing identifier” for communication internal to the network. *Id.*, 7:12-17, 9:9-17. For example, a private IPv4 address. *Id.*, 3:48-56. The IP connectivity service then sends the configuration data back to the terminal equipment in a configuration message, completing the configuration process. *Id.*, 9:54-63.

59. Each terminal destination equipment is therefore uniquely identifiable by the combination of (1) the shared primary address (*e.g.*, public IP address), (2) the port mask that defines a range of port numbers dedicated to the terminal destination equipment, and (3) the routing identifier (*e.g.*, private IP address) that identifies the terminal destination equipment. *Id.*, 5:4-8.

2. Routing

60. Once configured, the network can process packets according to the '369 patent's disclosures. For example, when the routing device **300** receives a data packet, it determines whether the destination port number in the data packet belongs to an assigned port range (defined using a port mask) and, if so, uses the routing identifier (*e.g.*, private IP address) that is associated with that assigned port range to route the data packet to the corresponding destination terminal equipment. *Id.*, 8:21-36.

* * *

61. As I explained above (*see supra* Section III.B), assigning the same primary address (*e.g.*, a public IPv4 address) to a plurality of pieces of terminal equipment, along with a port number and routing identifier (*e.g.*, a private IP address) was a standard element of prior art PAT. Like the '369 patent, these prior art PAT technologies received a data packet, determined whether the destination port number in the data packet belonged to a port number assigned to a destination equipment, and, if so, used a private IP address of the destination equipment to route the packet. While the '369 patent uses a range of port numbers, defined by a mask, rather than a single port number, in my opinion that variation is not novel or non-obvious, as I will discuss further below. *See infra* § VI.

V. LEVEL OF ORDINARY SKILL IN THE ART

62. I understand that a person of ordinary skill in the art (“POSITA”) is a hypothetical person who is presumed to be aware of all pertinent art, thinks along conventional wisdom in the art, and is a person of ordinary creativity—not an automaton. In deciding the level of ordinary skill, I understand that the following factors may be considered: the levels of education and experience of persons working in the field, the types of problems encountered in the field, and the sophistication of the technology.

63. I understand that the asserted patents must be evaluated from the perspective of a POSITA. In my opinion, the relevant art for this patent relates to the field of computer networks and routing packets in a computer network. I understand that the relevant point in time for determining the qualifications of a POSITA is the time of the alleged invention, which I assume to be the earliest filing date for the patent. Here, I understand that the earliest invention date contended by Patent Owner is March 31, 2008.

64. In my opinion, a POSITA at the time of the invention (*i.e.*, in March 2008) would have had a Bachelor of Science degree in electrical engineering, computer engineering, computer science, or a related subject, and three years of work experience in computer networking, including experience with the IPv4 protocol, or a related field. This level of skill is approximate, and lack of

professional experience can be remedied by additional education, and vice versa. I meet these criteria and have applied it in my analysis.

VI. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 7-14, 16-17 Are Obvious in View of Biswas and Kumar

65. In my opinion, Biswas in view of Kumar renders claims 7-14 and 16-17 of the '369 patent obvious.

66. In particular, this ground asserts that Biswas discloses the '369 patent's methods, apparatuses, and computer-readable mediums that configure terminal devices by assigning them a primary address, a range of port numbers, and a routing identifier. Kumar further discloses representing the range of port numbers as a port mask and rejecting data packets that do not satisfy any established rules. In my opinion, Biswas in view of Kumar renders obvious claims 7-14 and 16-17.

1. Biswas (EX1022)

67. U.S. Patent No. 8,019,889 ("Biswas") was filed on May 21, 2002 and issued on September 13, 2011. EX1022.

68. Like the '369 patent and the various prior art references discussed above, Biswas recognized that "[w]ith the explosion of the Internet, the number of IP address is not enough to give each computer a unique IP address." EX1022, 1:7-24. Accordingly, Biswas disclosed a form of PAT that assigned a global address and global port range to hosts in a private network. *Id.*, 2:23-33.

69. Biswas teaches its invention based on the following network embodiment:

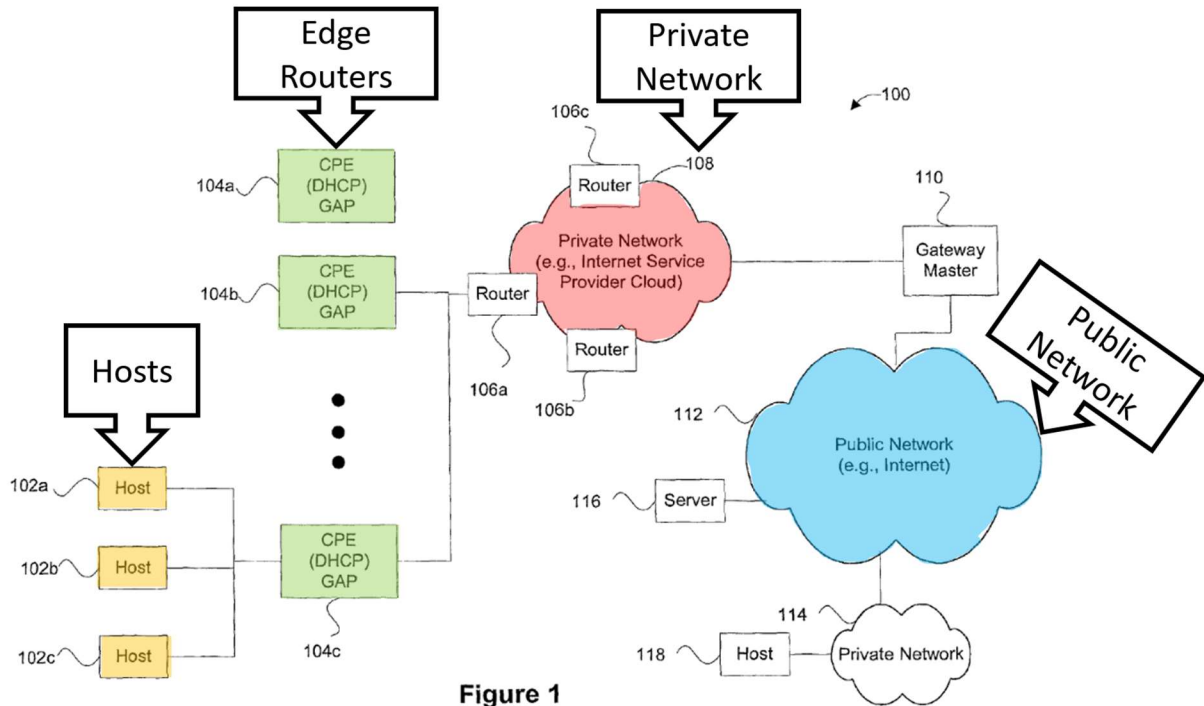


Figure 1

Id., Fig. 1 (colors and annotations added).

70. Network **108** (**red**) is a private network containing multiple intermediary routers **106** that are further connected to edge routers **104** (**green**) that service multiple hosts **102** (**orange**). *Id.*, 5:43-6:24. A gateway master **110** handles communication between the private network **108** and public network **112** (**blue**). *Id.* The network configuration can be used by host **102** to contact other hosts through the public network, like host **118** or server **116**. *Id.*

71. Each host (*e.g.*, hosts **102a-c**) obtain a global address and global port range from their corresponding edge router (*e.g.*, **104c**) using a DHCP process. *Id.*,

6:41-60, 7:49-12:19, Figs. 3A-8. In one embodiment, edge router **104c** has a global address of 172.1.1.1 and a global port range of 10000 to 15000. *Id.*, 6:61-7:7. “When host **102a** makes a request for a [global address] and [global port range], edge router **104c** may then assign the [global address] 172.1.1.1 and a portion of its available [global port range] to host **102a**.” *Id.* For instance, edge router **104c** might assign the port range 10000 to 10100 to host **102a**. *Id.* A POSTIA would have understood that edge router **104c** might further assign the next port range—for example, port range 10101 to 10200—to host **102b**. Edge router **104c** tracks the global port ranges that it assigns to the hosts so that incoming data packets can be sent to the correct host. *Id.*

2. Kumar (EX1023)

72. U.S. Patent No. 7,394,809 (“Kumar”) was filed on March 31, 2003 and granted on July 1, 2008. EX1023.

73. Kumar discloses a packet classifier that can apply various filters or rules to incoming data packets. *Id.*, 7:14-38. If the rule applies, then the router can take a pre-defined action associated with that rule. *Id.* These rules may be represented by bit masks. *Id.*, 7:38-57.

74. One example of a mask described in Kumar is a mask that defines a range of port numbers. *Id.*, 7:14-63. For instance, Figure 7B depicts an embodiment

that applies a port mask depicted at **712e** (yellow) to determine whether a port number in the destination port number field **702e** (red) falls between 0 and 1023:

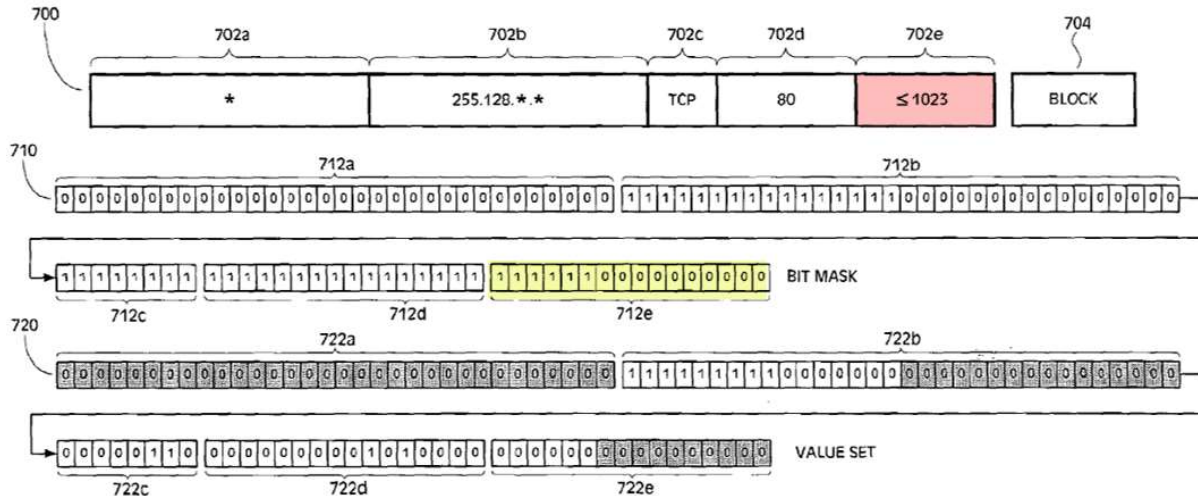


FIG. 7B

Id., Fig. 7B (colors added); *see also id.*, 8:20-9:19, Fig. 8. Indeed, the port mask shown in field **712e** has the value 1111110000000000, such that when logical AND operations are performed with the port mask and the destination port number in the IP packet the result will be 0 if the destination port number is within the assigned range (0-1023), and 1 when the destination port number is outside the assigned range.

75. For example, a POSITA would have known that if the destination port number is 1111000000010000 (*e.g.*, 61,456, which is outside the assigned range), the destination port number would be ANDed with the port mask, 1111110000000000. This operation would produce the result 1111000000000000.

This value is compared to zero, and since it is not equal this port number is *not* within the defined range.

76. On the other hand, a POSITA would have known that if the destination port number is 0000000000011101 (*e.g.*, 29, which is inside the assigned range), the destination port number would be ANDed with the port mask, 1111110000000000. This operation would produce the result 0000000000000000. Again, this value is compared to zero, and since it is equal to zero this port number *is* within the defined range.

3. The Biswas-Kumar Combination

77. In the Biswas-Kumar combination, in my opinion Biswas discloses an edge router that implements a method for configuring a piece of terminal equipment connected to a telecommunications network, including by assigning a piece of terminal equipment a shared primary address, a range of port numbers dedicated to it, and a routing identifier. Although Biswas does not provide the implementation detail of using a port mask to define the range of port numbers assigned to the terminal equipment, in my opinion Kumar's teachings supply this additional detail by disclosing port masks that define a range of port numbers. Thus, in the Biswas-Kumar combination that I discuss below, Biswas would continue to assign a range of port numbers to a piece of terminal equipment but would use port masks from

Kumar to define the range. In my opinion, the Biswas-Kumar combination renders claims 7-14 and 16-17 obvious.

4. Motivations to Combine

78. I explain the multiple reasons to combine Biswas and Kumar in my analysis below.

5. Claim 7

- (a) 7[pre]: A method of configuring a piece of terminal equipment connected to a telecommunications network, comprising, on reception of a configuration request sent by said equipment, the following steps:

79. To the extent the preamble is limiting, in my opinion Biswas discloses limitation 7[pre]: “a method of configuring a piece of terminal equipment [*e.g.*, **host 102a**] connected to a telecommunications network [*e.g.*, **the network described in Figure 1**], comprising, on reception of a configuration request [*e.g.*, **a DHCP request**] sent by said equipment, the following steps.”

80. Figure 1 illustrates a telecommunications network that includes hosts (orange) that are connected to an Internet Service Provider Cloud (red) and the public Internet (blue) via Customer Premises Equipment (green):

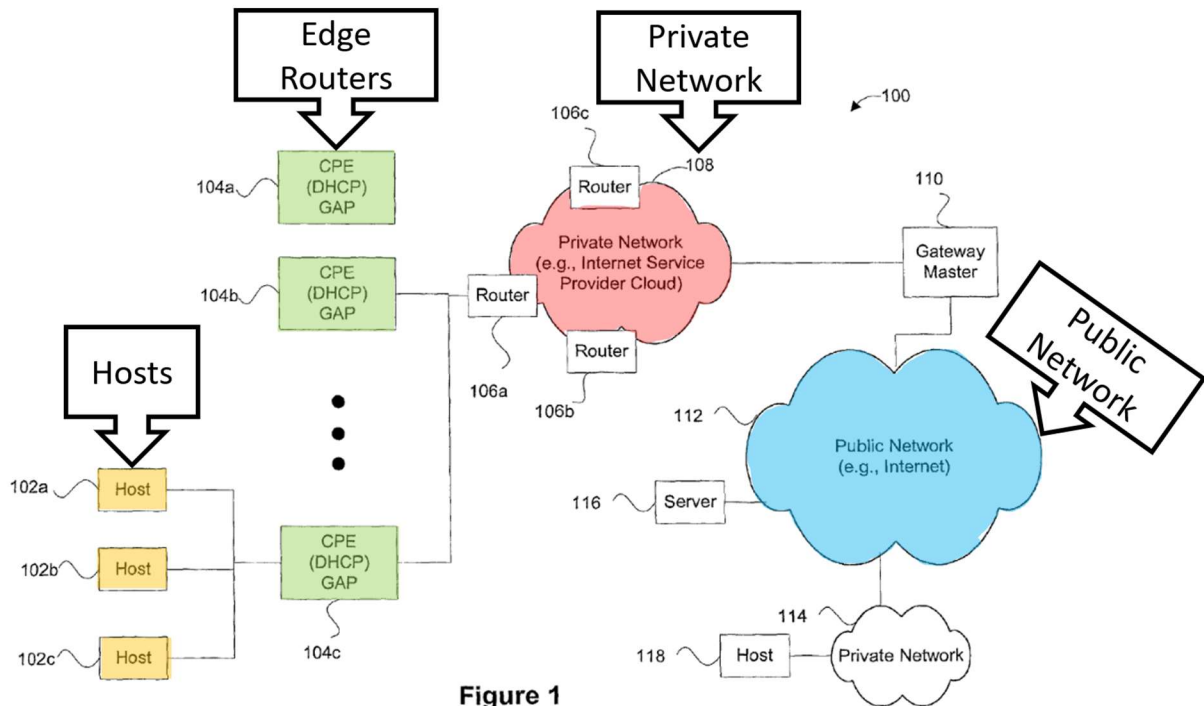


Figure 1

EX1022, Fig. 1 (colors and annotations added).

81. In my opinion, hosts **102** correspond to “a piece of terminal equipment connected to a telecommunication network.” Indeed, the ’369 patent states that “terminal equipment” can be “telephones or personal computers.” EX1001, 8:5-11. Similarly, Biswas discloses that host **102** may be “a personal computer or workstation.” EX1022, 12:54-58.

82. In my view, Biswas further discloses a method of configuring a piece of terminal equipment (e.g., **host 102a**) that comprises “reception of a configuration request” (e.g., **DHCP request**) sent by said equipment. For example, each host **102** “is operable to obtain from its corresponding edge router a global address (GA) and optionally a global port range (GPR).” *Id.*, 2:23-33. Host **102** may use “any suitable

mechanism” for requesting the GA and GPR, for example “a global address or a DHCP (Dynamic Host Configuration Protocol) request.” *Id.*, 6:50-60, 2:47-3:57, 7:9-12:19. A POSITA would understand that a DHCP request sent by a host **102** is a configuration request. Indeed, the ’369 patent discloses the configuration request may be a “DHCP” request. EX1001, 9:42-54 (“a configuration request ... may be, for example, a DHCP request.”), 11:30-35. Thus, in my opinion, Biswas discloses limitation 7[pre].

(b) 7[a]: assigning to said piece of terminal equipment a primary address shared with a plurality of pieces of terminal equipment;

83. In my opinion, Biswas also discloses limitation 7[a]: “assigning [*e.g.*, **via edge router 104**] to said piece of terminal equipment [*e.g.*, **host 102a**] a primary address [*e.g.*, **a global address**] shared with a plurality of pieces of terminal equipment [*e.g.*, **other hosts 102b-c**].”

84. Biswas discloses that after receiving a configuration request (*e.g.*, **a DHCP request**) from a piece of terminal equipment (*e.g.*, **hosts 102**), an edge router **104** responds with a DHCP reply that includes a local address, global address (GA), and global port range (GPR) for the terminal equipment. EX1022, 7:62-8:15, 6:50-60, 2:25-28.

85. In my opinion, Biswas further discloses how the piece of terminal equipment (*e.g.*, **host 102a**) is assigned a primary address (*e.g.*, **the global address**)

that is shared with other hosts (*e.g.*, **hosts 102b-c**). Specifically, each edge router **104** “has a GA [global address] and GPR [global port range] that may be apportioned among its corresponding hosts.” *Id.*, 6:61-7:7. For instance, “edge router **104c** may have GA 172.1.1.1 and GPR 10000 through 15000” to assign to hosts **102a-c**. *Id.* “When host **102a** makes a request for a GA and GPR, edge router **104c** may then assign the GA 172.1.1.1 and a portion of its available GPR to host **102a**,” for example it may assign “GPR 10000 through 10100” to host **102a**. *Id.* Correspondingly, a POSITA would have understood that the edge router **104c** could then assign a subsequent GPR, for example 10101 through 10200, to another host, for example host **102b**. Thus, in my opinion, Biswas discloses that a shared global address is assigned to multiple hosts (**102a-c**) with each host also being assigned a range of port numbers to “distinguish its GA from other hosts which use the same GA.” *Id.*, 11:50-54, 1:42-45, 6:61-63.

86. In my opinion, the “global address” in Biswas corresponds to the “primary address” in the ’369 patent. For instance, the ’369 patent discloses that an example of a “primary address is advantageously a public address.” EX1001, 3:44-46. The “global address” is therefore a public address, in my opinion, because it is used to communicate over the public network. EX1022, 6:41-49.

- (c) 7[b]: assigning to said piece of terminal equipment a port mask defining a range of numbers dedicated to it and a routing identifier; and

87. In my opinion, Biswas and Kumar render obvious limitation 7[b]: “assigning to said piece of terminal equipment [*e.g.*, **Biswas’s host 102a**] a port mask [*e.g.*, **Kumar’s port mask**] defining a range of numbers dedicated to it [*e.g.*, **Biswas’s global port range**] and a routing identifier [*e.g.*, **Biswas’s local address**].”

88. In my view, Biswas discloses assigning hosts (*e.g.*, **host 102a**) a routing identifier (*e.g.*, **a local address**). Biswas explains that hosts **102** “send[] a DHCP request for a local address to its corresponding edge router **104**,” which edge router then “respond[s] with a DHCP reply having the local address as well as the GA (and GPR) for the querying host.” EX1022, 6:50-60. In my opinion, the local address of Biswas corresponds to the “routing identifier” in the ’369 patent. Indeed, the ’369 patent explains that a “routing identifier” may be a “secondary destination address” (EX1001, 3:47-50, 14:29-31), such as a “private address” (*id.*, 3:50-52, 9:9-11). Similarly, Biswas teaches that a host’s local address is “only used within that local group” (EX1022, 1:32-33), such that a POSITA would have understood it is a private address.

89. Further, in my opinion, Biswas also discloses assigning each host (*e.g.*, **host 102a**) a range of port numbers dedicated to it. EX1022, 6:37-7:7, 7:49-61, Figs. 3A-3E. Like the port numbers disclosed in the ’369 patent, which can be used for

different connections, like “P2P (Peer to Peer), FTP (File Transfer Protocol), web browsing, telephone, etc. applications,” (EX1001, 7:22-27), in my opinion Biswas’s port numbers in the range of port numbers can also be used for these connections. Indeed, a POSITA would have understood that the port numbers in Biswas and the ’369 patent are typical implementations of port numbers.

90. Although Biswas does not provide the implementation detail of using a port mask to define the range of port numbers, in my opinion assigning a port mask defining that range of port numbers would have been obvious to a POSITA in view of Kumar. For instance, Kumar discloses using port masks that are similar to those disclosed in the ’369 patent to define a range of port numbers. Indeed, the ’369 patent depicts examples of 16-bit port masks, in which the range of port numbers is defined by the bits marked with an “x”:

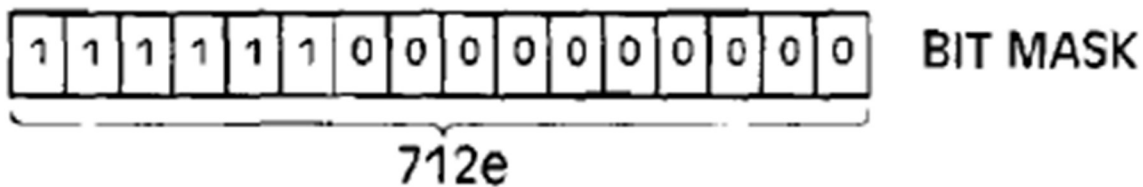
1	1	1	x	x	x	x	x	x	x	x	x	x	x	x	x
1	1	1	1	x	x	x	x	x	x	x	x	x	x	x	x
1	1	1	1	1	1	1	1	1	1	1	1	x	x	x	x
1	1	1	1	1	1	1	1	1	1	1	x	x	x	x	x
1	1	1	1	1	1	1	1	1	1	1	1	x	x	x	x
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	x
x	x	x	x	1	1	1	1	1	1	1	1	1	1	1	1
x	x	x	x	x	1	1	1	1	1	1	1	1	1	1	1

FIG. 2A

EX1001, Figs. 2A & 2B, 7:49-67. Similarly, Kumar discloses 16-bit port masks in which the range of port numbers is defined by the bits marked with a “0,” as I explained above. EX1023, Fig. 7B, 7:38-8:64; *see supra* § VI.A.2.

91. Kumar expressly teaches that its port masks may define “a range” of port numbers (EX1023, 7:31-38), and provides various examples of port masks (*id.*, Figs. 7C-7I, 8, 10A-10C).

92. For instance, Figure 7B of Kumar illustrates an exemplary port mask in which the last ten bits of the mask are marked with a “0” to specify a port range of 0-1023:



Id., Fig. 7B, 8:34-63. Kumar also explains that to the extent a port range cannot be represented by a single port mask, multiple masks can be used to encompass the desired range. *Id.*, 8:34-63.

93. For example, a POSITA would have known that if the destination port number is 1111000000010000 (*e.g.*, 61,456, which is outside the assigned range), the destination port number would be ANDed with the port mask, 1111100000000000. This operation would produce the result 1111000000000000.

This value is compared to zero, and since it is not equal this port number is *not* within the defined range of 0-1023.

94. On the other hand, a POSITA would have known that if the destination port number is 0000000000011101 (*e.g.*, 29, which is inside the assigned range), the destination port number would be ANDed with the port mask, 1111110000000000. This operation would produce the result 0000000000000000. Again, this value is compared to zero, and since it is equal to zero this port number *is* within the defined range of 0-1023. In this way, Kumar's port masks define a range of port numbers from 0-1023.

95. Thus, in the combined Biswas-Kumar system the edge router **104** would continue to assign to each host **102** a range of port numbers dedicated to it (as disclosed in Biswas), but would use a port mask to define the range of port numbers (as disclosed in Kumar).

96. In my opinion, a POSITA would have been motivated to combine the teachings of Biswas and Kumar in this manner.

97. As a threshold matter, Biswas and Kumar are analogous art because the references are in the same field of endeavor as each other and the '369 patent, *i.e.*, computer networking and routing data packets. EX1022, 1:7-10; EX1023, 1:7-24, 2:57-65; EX1001, 1:15-36. For instance, Biswas discloses an edge router for configuring hosts and routing data packets to those hosts (EX1022, 1:7-10), Kumar

discloses that its teachings “are generally applicable to any device, system, and/or circumstance where classification of packets or other communications is needed” (EX1023, 2:57-65), and further explains that it discloses a “routing technique” to route packets in a computer network (*id.*, 1:7-24), and the ’369 patent explains that its “field of invention is that of telecommunications networks,” including “rout[ing] data packets sent by pieces of terminal equipment to their final destination” (EX1001, 1:15-36).

98. Further, Biswas does not disclose the details of how edge router **104** determines whether a destination port number is within one of its stored port ranges. EX1022, 7:1-7. In my opinion, a POSITA would have been aware that masks could be used to determine whether a number lies within a range. *See supra* § III.C. Masks in general were well known in the prior art for decades. *Id.* And the use of masks to determine whether a number falls within a range was ubiquitous in computer networking. *Id.* For example, in my opinion, a POSITA would have been aware that networks routinely used masks to determine whether the destination address in an incoming data packet fell within the range of addresses in the network. *Id.* In my opinion, a POSITA would have further been aware that masks were used in the prior art to classify incoming port numbers—and determine whether those incoming port numbers fall within a specified range—as well. *Id.* Thus, in my opinion, a POSITA would be motivated to look to references, like Kumar, that discuss

classifying packets based on their port numbers, and, in my opinion, a POSITA would have been particularly interested in references, like Kumar, that use the common and well-known technique of masking to make these classifications. Indeed, a POSITA would have found combining Biswas and Kumar obvious because Kumar teaches that its disclosures “are generally applicable to any device, system, and/or circumstance where classification of packets or other communications is needed.” EX1023, 2:57-65.

99. Moreover, in my opinion, a POSITA would have been motivated to combine the teaching of these two references because, by the time of the alleged invention of the '369 patent, it was well-known that bit masks, such as port masks, as used in the '369 patent, could be used to optimize performance. For example, a POSITA would have recognized that Kumar's port masks are computationally efficient because they use only bitwise operations, like logical ANDs. Thus, an inclusion in the range can be efficiently computed with one logical operation and a comparison to zero.

100. Additionally, in my opinion, the combination would have involved the application of a known technique (*i.e.*, the use of port masks) to a known device (*i.e.*, Biswas's edge router which is equipped to assign port ranges) to yield predictable results (*i.e.*, a network device that uses port masks to define a range of port numbers). Indeed, Kumar was already using port masks to define ranges of port numbers in its

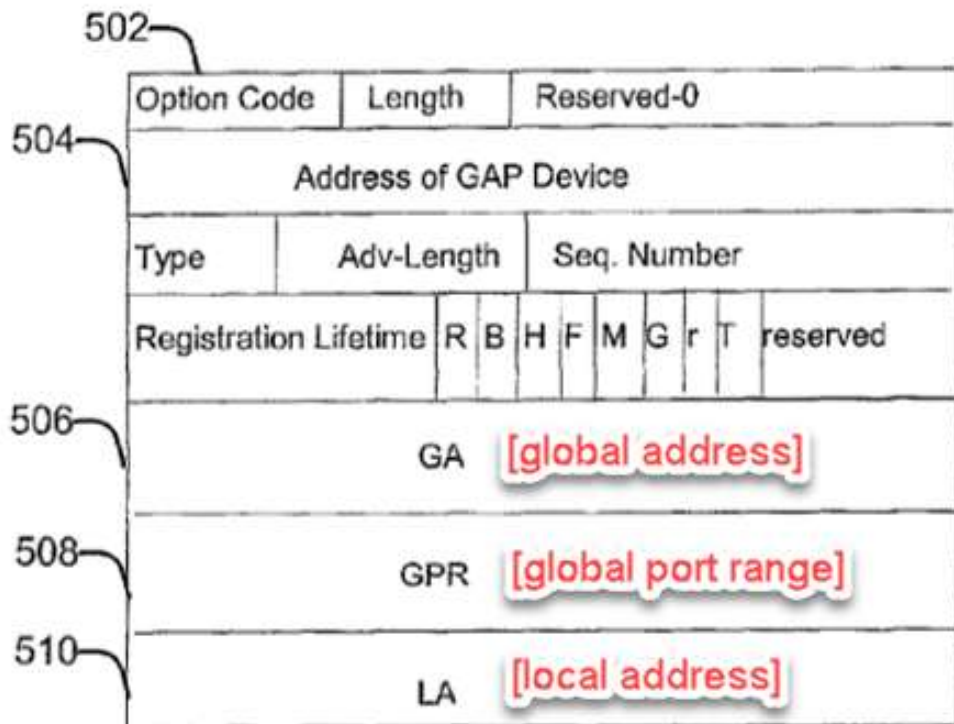
own invention. *See supra* § VI.A.2. And Kumar further disclosed using these port masks on a router in a network to help with typical network activities, like routing data packets. *Id.* So not only would the combination apply a known technique to a known device to yield a predictable result, but Kumar was *already* applying this known technique to the same or a similar known device to yield the same or a similar result.

101. And it is my opinion that a POSITA would have had a reasonable expectation of success in combining Biswas and Kumar because the combination merely involves the straightforward application of Kumar's port masks to define the range of port numbers already assigned by Biswas. As discussed above, Kumar already discloses an embodiment that is similar to the proposed combination; Kumar discloses a router that uses port masks to represent a range of port numbers, the router further using that port mask to assist with typical network operations, like routing data packets. *See supra* § VI.A.2. Indeed, this reasonable expectation of success is echoed by Kumar, which is "generally applicable to any device, system, and/or circumstance where classification of packets or other communications is needed." For at least these reasons, in my opinion, a POSITA would have been motivated to combine Biswas and Kumar as described above.

- (d) 7[c]: sending to said piece of terminal equipment a configuration message comprising said primary address, said port mask, and said routing identifier.

102. In my opinion, Biswas and Kumar render obvious limitation 7[c]: “sending to said piece of terminal equipment [e.g., **Biswas’s host 102**] a configuration message [e.g., **Biswas’s DHCP reply**] comprising said primary address [e.g., **Biswas’s global address**], said port mask [e.g., **Kumar’s port mask**], and said routing identifier [e.g., **Biswas’s local address**].”

103. Biswas discloses sending to the piece of terminal equipment (e.g., **hosts 102**) a configuration message. For instance, Figure 5 illustrates an embodiment of “the reply to the host’s DHCP request” and the global address **506**, the global port range **508**, and the local address **510** for host **102** that is included in the reply:



EX1022, Fig. 5 (red text added), 10:22-58.

104. As discussed in connection with limitations 7[a] and 7[b], in my view, the global address and the local address in the DHCP Reply correspond to the “primary address” and “routing identifier” in Biswas. *See supra* § VI.A.5.b-c. As also discussed in connection with limitation 7[b], in my opinion a POSITA would have found it obvious to combine Biswas and Kumar to implement Biswas’s global port range—which is a range of port numbers assigned to host **102**—using Kumar’s port mask representing a range of ports, and the POSITA would have been motivated to do so. *See supra* § VI.A.5.c.

6. **Claim 8: The method according to claim 7 of configuring a piece of terminal equipment, comprising a step of assigning to said piece of terminal equipment an identifier of a routing device adapted to route a data packet comprising said primary address as the destination address to said piece of terminal equipment, and the configuration message further comprising said routing device identifier.**

105. In my opinion, Biswas further discloses the additional limitation of claim 8: “assigning to said piece of terminal equipment [*e.g.*, **host 102**] an identifier of a routing device adapted to route a data packet [*e.g.*, **gateway master 110**] comprising said primary address as the destination address to said piece of terminal equipment [*e.g.*, **the global address that is used by gateway master 110**], and the configuration message [*e.g.*, **the DHCP reply 500**] further comprising said routing device identifier.”

106. As discussed, Biswas describes assigning a global address that is shared between hosts **102**, and the DHCP reply in Biswas contains that global address. *See supra* § VI.A.5. Biswas explains that “Gateway Master **110** translates local addresses of data received from a private network **108** into global addresses of data being output from the Gateway Master **110** to public network **112**, and vice versa. The Gateway Master **110** also translates global addresses of data received from public network **112** into local addresses of data being output from the Gateway Master **110** to private network **108**, and vice versa.” EX1022, 5:52-6:24. In my opinion, a POSITA would have known that gateway master **110** is a routing device since it routes incoming and outgoing data packets to their destinations. *Id.*, 5:52-6:24. As Biswas explains, “gateway master **110** is operable to handle communication between the ISP network **108** and public network **112**.” *Id.* Gateway master **110** can also act as a NAT device, which, in my view, a POSITA would have understood is a routing device. *Id.*

107. In my further opinion, a POSITA would have also known that the global address is an “identifier of a routing device” (*e.g.*, an identifier of gateway master **110**) because the disclosed network routes data packets containing that global address to gateway master **110**. In other words, the global address identifies gateway master **110** on the public network. Devices on the public network use this identifier (*i.e.*, the global address) to communicate with gateway master **110** by sending data

packets to the gateway master. Thus, the global address identifies gateway master **110** and is therefore an “identifier of a routing device.”

7. **Claim 9: The configuration method according to claim 7, wherein said configuration message is further sent to a routing device that routes to said piece of terminal equipment a data packet containing said primary address as the destination address.**

108. In my opinion, Biswas further discloses the additional limitation of claim 9: “wherein said configuration message [*e.g.*, **DHCP reply**] is further sent to a routing device [*e.g.*, **edge router 104**] that routes to said piece of terminal equipment [*e.g.*, **host 102**] a data packet containing said primary address [*e.g.*, **global address**] as the destination address.”

109. Biswas discloses embodiments where the “edge router **104** may be in the form of a customer premises equipment (CPE), such as a cable modem.” EX1022, 7:9-10. As Biswas explains, the disclosed CPE is “operable as a DHCP relay.” *Id.*, 8:16-27. Meaning, when host **102** requests a global address and global port range, it first sends that request to edge router **104**, which is acting as a DHCP relay. *Id.* Edge router **104**, then “forwards the DHCP request to” the device that constructs and sends the DHCP reply, which contains the global address and global port range assignments. *Id.* On the DHCP reply’s return path, it is sent to edge router **104**, acting as DHCP relay, and then to host **102**. *Id.* Figure 3B of Biswas

illustrates this embodiment in which the edge router (labeled CPE 206) is separate from the DHCP server (labeled DHCP/GAP 208) and acts as a relay:

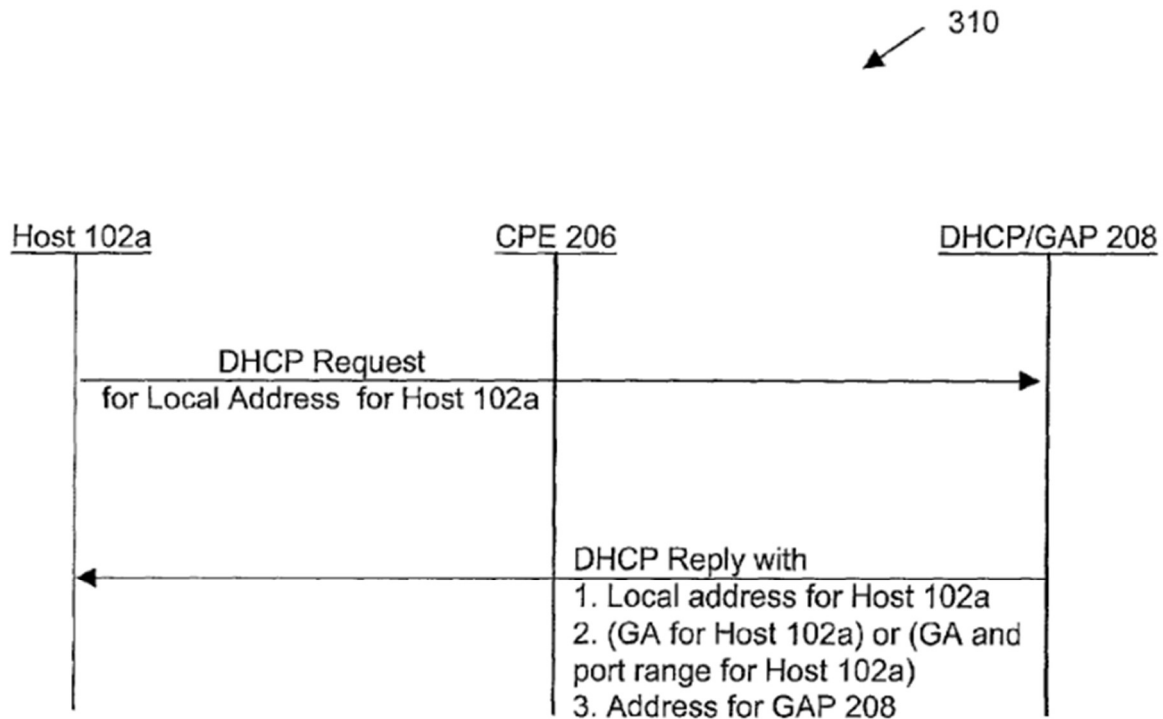


Figure 3B

Id., Fig. 3B. As I discussed above, edge router **104** routes data packets containing the primary address to the piece of terminal equipment. *See supra* § VI.A.5. Thus, in my opinion, Biswas and Kumar render obvious claim 9.

8. Claim 10

- (a) 10[pre]: A configuration server in a telecommunications network, wherein, on reception of a configuration request sent by a piece of terminal equipment, comprising:

110. To the extent the preamble is limiting, in my opinion Biswas teaches limitation 10[pre]: “a configuration server in a telecommunications network [*e.g.*,

edge router 104]” that performs the claimed steps. The ’369 patent discloses that the configuration server can be “a DHCP configuration server.” EX1001, 9:45-53. As discussed, Biswas describes edge routers **104** that can serve as DHCP servers. *See supra* § VI.A.5; *see also* EX1022, 7:18-26. Edge routers **104** receive configuration requests from hosts **102**. *See supra* § VI.A.5.a. Thus, in my opinion, Biswas teaches limitation 10[pre].

- (b) 10[a]: a processor that assigns a primary address to said piece of terminal equipment, said primary address being shared with a plurality of pieces of terminal equipment;

111. In my opinion, Biswas teaches limitation 10[a]. As I discuss above, Biswas teaches the claimed steps, performed on an edge router. *See supra* § VI.A.5.b. Biswas discloses that the edge router would have included a “processor” (EX1022, 3:62-64, 13:42-44), and a POSITA would have also understood that the edge router uses a processor to perform its functions. Thus, in my opinion, the edge router in Biswas uses a processor to perform the steps in this limitation.

- (c) 10[b]: the processor assigns to said piece of terminal equipment a port mask defining a range of numbers dedicated to it and a routing identifier; and

112. In my opinion, Biswas and Kumar render obvious limitation 10[b]. As discussed above, in my view, Biswas and Kumar render obvious the claimed steps, performed on an edge router. *See supra* § VI.A.5.c. In my opinion, POSITA would

have known that the edge router uses processors to perform these steps. *See supra* § VI.A.8.b.

- (d) 10[c]: a communication unit that sends to said piece of terminal equipment a configuration message comprising said primary address, said port mask, and said routing identifier.

113. In my opinion, Biswas and Kumar render obvious limitation 10[c]. As discussed above, in my view, Biswas and Kumar render obvious the claimed step, performed on an edge router. *See supra* § VI.A.5.d. In my opinion, Biswas also discloses that a POSITA would have known that the edge router performing this step uses a communication unit to perform its functions. *See supra* § VI.A.8.b. The '369 patent explains that an “implementation of the invention with reference to FIG. 5” includes a “telecommunications means **340** for communicating with the network **1**.” EX1001, 8:37-43, 10:57-63. The '369 patent does not further define what exactly this telecommunications means **340** is, but the patent does explain that it is an “element[] that [is] conventionally found in a conventional computer.” *Id.* In my opinion, a POSITA would have understood that the edge router in Biswas also has such a communication unit, which enables it to communicate with hosts both on the internal, private network and on the external, public network. Indeed, Biswas discloses a router that contains components necessary to “handle[] communications.” EX1022, 12:61-14:8. And Figure 9 of Biswas discloses a “router

10” containing a communication unit. *Id.*, Fig. 9 (“interfaces 68”). Thus, in my opinion, Biswas and Kumar render obvious limitation 10[c].

9. Claim 11

- (a) 11[pre]: A method of configuring a piece of terminal equipment connected to a telecommunications network, wherein, on reception of a configuration message comprising configuration data comprising a primary address, a port mask defining a range of port numbers that is dedicated thereto, and a routing identifier, said method comprises the following steps:

114. To the extent the preamble is limiting, in my opinion Biswas and Kumar render obvious limitation 11[pre]: “a method of configuring a piece of terminal equipment connected to a telecommunications network [*e.g.*, **Biswas’s host 102**], wherein, on reception of a configuration message [*e.g.*, **Biswas’s DHCP reply 500**] comprising configuration data comprising a primary address [*e.g.*, **Biswas’s global address**], a port mask [*e.g.*, **Kumar’s port mask**] defining a range of port numbers that is dedicated thereto [*e.g.*, **Biswas’s global port range**], and a routing identifier [*e.g.*, **Biswas’s local address**].” *See supra* §§ VI.A.5, VI.A.8.

- (b) 11[a]: storing said configuration data; and

115. In my opinion, Biswas discloses limitation 11[a]: “storing said configuration data [*e.g.*, **Biswas’s host stores the local address, global address, and global port ranges**].”

116. A POSITA would have known that the host **102** stores the configuration data. Biswas explains that, after receiving the configuration message, the host does

not need to contact any external device unless “it requires an additional GPR.” EX1022, 8:28-45, 10:53-56, 11:67-12:2. Additionally, Biswas explains that once the host receives its assigned port range, it can “simply use[] the next available port selected from the GPR that was previously obtained from its edge router.” *Id.*, 11:50-57. A POSITA would understand that the host remembers its port range (*e.g.*, by storing the port range in memory) so that it can continue to use the port range without having to further contact the DHCP device. In fact, a POSITA would have recognized that it would have been extremely inefficient and wasteful to not have host **102** store the configuration data. If host **102** did not store the configuration data, it would have to send a request to edge router **104** or some other DHCP device every time it needed to send a data packet, to remind itself of its assigned port range. Not only would it be inefficient, but it would also simply not be possible for the host **102** to send data because it would not be able to “remember” what address and port number to use, even if it had just received its configuration data, since it never stores that data. Therefore, a POSITA would have known that host **102** stores the configuration data upon receipt.

117. Indeed, Biswas explains that its hosts “may each be implemented” on “a personal computer or workstation” and Biswas further discloses computers that have a memory block **61** for “caching and/or storing data.” *Id.*, 12:40-13:17. “The memory or memories may also be configured to store received packets, identifiers

to track each session or flow and the number of such sessions or flows, application type and their corresponding data formats, *a local address, a global address, one or more global port ranges*, an address for a GAP device, etc.” *Id.*, 13:51-56 (emphasis added). As discussed, the emphasized terms correspond to the configuration data. *See supra* § VI.A.9.a. In my opinion, a POSITA would have found it obvious to implement this same memory and store this same information on host **102** to the extent that Biswas does not already explicitly disclose this. Thus, in my opinion, a POSITA would have known to have host **102** store the configuration data, and Biswas and Kumar render obvious limitation 11[a].

- (c) 11[b]: before sending a data packet into the telecommunications network, selecting a port number in the range of port numbers defined by the port mask, said data packet comprising as source address the primary address of said piece of terminal equipment and as source port number the selected port number.

118. In my opinion, Biswas and Kumar render obvious limitation 11[b]: “before sending a data packet into the telecommunications network [*e.g.*, **the network described in Figure 1 of Biswas**], selecting a port number [*e.g.*, **a port number assigned to a host 102 in Biswas**] in the range of port numbers defined by the port mask [*e.g.*, **Kumar’s port masks**], said data packet comprising as source address the primary address of said piece of terminal equipment [*e.g.*, **the global address for host 102**] and as source port number the selected port number.”

119. Biswas depicts host **102**’s process for sending data in Figure 8:

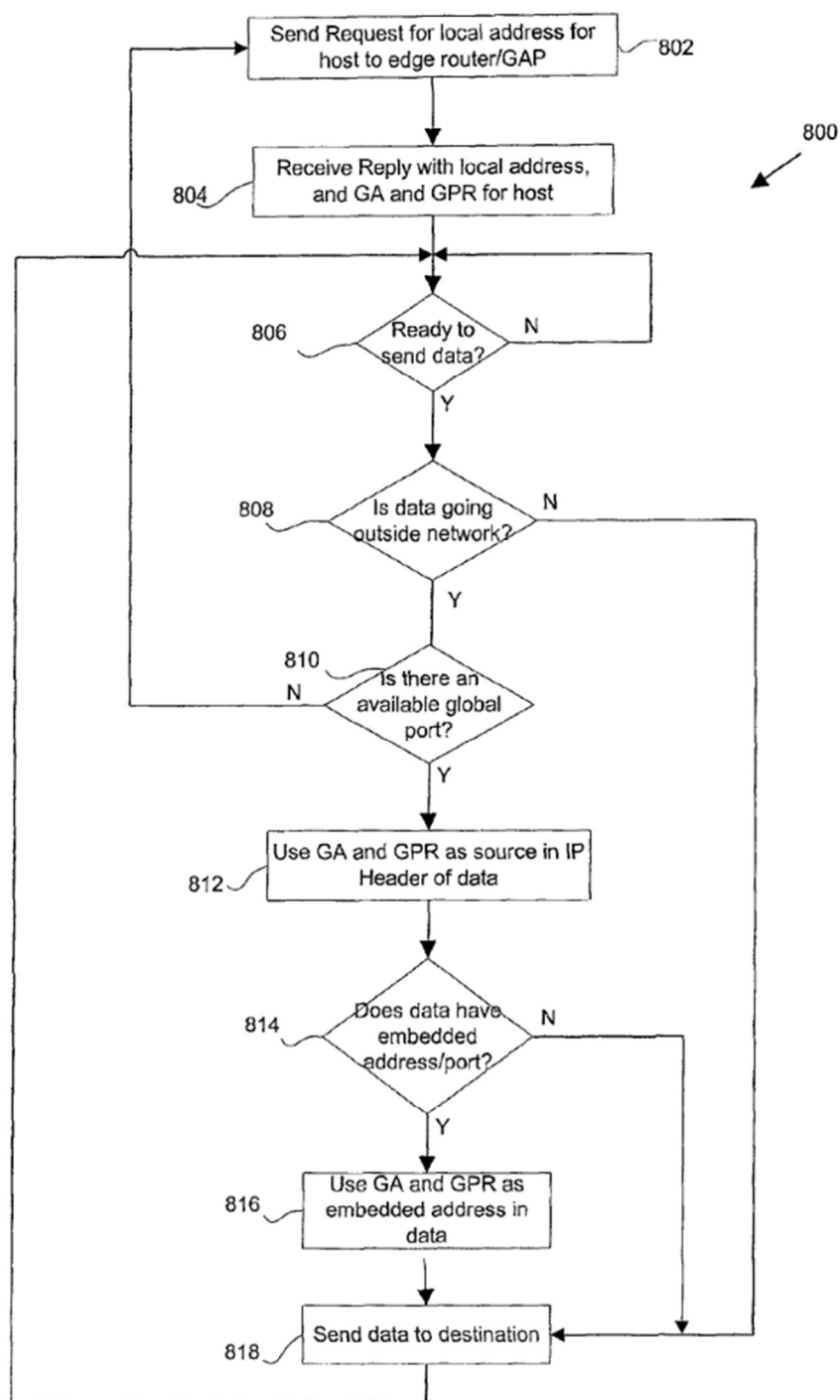


Figure 8

Id., Fig. 8. At step **812**, host **102** selects a global address and a port number in the global port range as the source address and source port number in the IP header of

the data packet. *Id.*, Fig. 8, 11:25-12:28. As discussed, in my opinion, a POSITA would have found it obvious to combine Biswas with Kumar to represent the port range as a port mask, and would have been motivated to do so. *See supra* § VI.A.5.c. After using said global address and port number in the global port range as the source information of the data packet, host **102** sends the data packet to its destination. EX1022, Fig 8, 11:25-12:28. Thus, in my opinion, Biswas and Kumar render obvious limitation 11[b].

10. Claim 12: The configuration method according to claim 11, wherein, once an identifier of a routing device adapted to route a data packet comprising said primary address as the destination address to said piece of terminal equipment has been received, said method further comprises a step of sending the configuration data to said routing device.

120. In my opinion, Biswas discloses claim 12: “once an identifier of a routing device adapted to route a data packet comprising said primary address as the destination address to said piece of terminal equipment has been received [*e.g.*, **Biswas’s global address**], said method further comprises a step of sending the configuration data [*e.g.*, **Biswas’s DHCP reply 500**] to said routing device [*e.g.*, **Biswas’s gateway master 110**].”

121. As discussed, Biswas discloses assigning a primary address (*e.g.*, a **global address**) to host **102**. *See supra* § VI.A.5.b. In my opinion, this global address corresponds to the “identifier of a routing device” in claim 12. In particular, the primary address is an identifier of gateway master **110**. As Biswas explains,

gateway master **110** can “translate[] local address of data received from a private network **108** into global addresses of data being output from the Gateway Master **110** to public network **112**, and vice versa.” EX1022, 6:12-24. In my opinion, a POSITA would have understood that this global address is an identifier of gateway master **110** because the gateway master intercepts incoming data packets that use the global address as a destination address.

122. Biswas further discloses that the gateway master **110** is “adapted to route a data packet comprising said primary address as the destination address to said piece of terminal equipment.” In particular, Biswas teaches that incoming data packets that include the global address as the destination address can be routed to the corresponding host **102**. EX1022, 6:61-7:8.

123. Biswas also teaches this method “further compris[ing] a step of sending the configuration data to said routing device.” In my opinion, a POSITA would have known that the configuration data is sent to gateway master **110**. In particular, a POSITA would have found it obvious that gateway master **110** routes incoming data packets that include the global address to the correct edge router **104** and host **102**. In my opinion, a POSITA would have therefore known that gateway master **110** receives and stores configuration data so that it knows which global address and global port range is assigned to which host **102** and edge router **104**. If gateway master **110** did not receive the configuration data, it would not know where to send

incoming data packets. For example, if gateway master **110** receives a data packet with destination address 172.1.1.1 and destination port number 10000, but it does not have the information that this global address and global port number is assigned to edge router **104c** and host **102a** (versus some other edge router or host), then gateway master **110** would accordingly not have the information as to where to send the incoming data packet. Thus, in my opinion, a POSITA would have known that the configuration message is sent to the routing device (*e.g.*, **gateway master 110**) once it is received by the terminal equipment (*e.g.*, **host 102**).

11. **Claim 13: The configuration method according to claim 11, wherein, on reception of a data packet comprising a destination address, a port number, and a routing identifier, said method further comprises a step of verifying that the port number belongs to the range of port numbers defined by the port mask, and a step of rejecting said packet if result of the verification is negative.**

124. In my opinion, Biswas further discloses the additional limitation of claim 13: “on reception of a data packet [*e.g.*, **data packet received by edge router 104**] comprising a destination address [*e.g.*, **global address**], a port number [*e.g.*, **port number assigned to host 102**], and a routing identifier [*e.g.*, **host 102’s local address**], said method further comprises a step of verifying that the port number belongs to the range of port numbers defined by the port mask, and a step of rejecting said packet if result of the verification is negative.”

125. The '369 patent explains that “terminal equipment” can be a gateway. EX1001, 8:5-10. Here, the terminal equipment corresponds to Biswas’s edge router **104**. Biswas explains that “[e]ach edge router **104** preferably tracks its GPR assignments so that data that is destined for any of its hosts may be sent to the correct host.” EX1022, 7:1-8. Kumar teaches rules or filters that are associated with actions. EX1023, 7:14-38. Kumar explains that the router can use these rules to accept or block incoming data packets. *Id.*; *see also, e.g., id.*, 8:1-19, 9:1-2.

126. In my opinion, A POSITA would have found it obvious to apply the teachings of Kumar to Biswas such that Biswas’s edge router **104** or gateway master **110** would be able to block or reject data packets that contain a port number that does not belong to an assigned range of port numbers. For instance, when edge router **104** receives an incoming data packet, it could use Kumar’s “rules” or “filters” to evaluate whether the data packet contains a destination port number that is within an assigned port mask. If a rule applies, the associated action would be to “accept” the data packet and continue routing it to host **102** that was assigned the relevant port mask. Data packets that do not match any rule would be automatically rejected.

127. In my view, a POSITA would have been motivated to combine the teachings of Biswas and Kumar. Biswas does not explain what to do when an incoming data packet contains a destination port number that is not within an assigned port mask. In my opinion, a POSITA would have been motivated to look

for references that teach a method of handling data packets that do not comply with specific assignments, like Kumar's filters. A POSITA would have found combining Biswas and Kumar obvious because Kumar teaches that its disclosures "are generally applicable to any device, system, and/or circumstance where classification of packets or other communications is needed." EX1023, 2:57-65. Biswas itself explains that "it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. Therefore, the described embodiments should be taken as illustrative and not restrictive, and the invention should not be limited to the details given herein." EX1022, 14:9-16.

128. Moreover, in my opinion, the combination would have been the application of a known technique (*i.e.*, Kumar's filters) to a known device (*i.e.*, Biswas's edge router **104** or gateway master **110**) to yield a predictable result (*i.e.*, classifying and handling data packets). Indeed, Kumar already implements this disclosure in this exact way. As discussed, Kumar teaches using its filters to block or accept incoming data packets. So not only would the combination have been of a known technique to a known device to yield a predictable result, but Kumar *already* implements this known technique to the same or a similar device to yield the same or a similar result.

129. In my opinion, a POSITA would also have had a reasonable expectation of success in combining Biswas and Kumar and there would have been no

unexpected results because the combination merely involves the straightforward application of Kumar's method of creating filters in a routing device to a known edge router **104** or gateway master **110**. Indeed, as discussed, Kumar already implements this exact process in its own invention, and applying it to Biswas would have involved merely applying the disclosure that Kumar implements on its router to the same or a similar device, edge router **104**, in Biswas.

130. To the extent claim 13 suggests that the host **102** must reject data packets outside of its port range (rather than the edge router **104**), Biswas discloses that as well. Biswas explains that the hosts **102** use only ports in their assigned global port range to communicate over the network. EX1022, 2:23-33, 2:46-65. For example, Biswas explains that hosts **102** must make additional DHCP requests (in which the DHCP device will assign an additional port range to host **102**) in order to use port numbers that are outside of their original port range. *Id.*, 3:6-14. In my opinion, a POSITA would have understood this disclosure to mean that host **102** in Biswas would not open connections on any ports or use any ports that are outside of its assigned port range. Thus, in my opinion, a POSITA would have known that host **102** would have rejected all incoming packets that contain a port number that is outside of the assigned port range.

131. Thus, Biswas and Kumar render obvious claim 13.

12. Claim 14

- (a) 14[pre]: A piece of client terminal equipment connected to a telecommunications network, wherein, on reception of a configuration message comprising configuration data comprising a primary address shared with a plurality of pieces of terminal equipment, a port mask defining a range of port numbers that is dedicated to the piece of client terminal equipment, and a routing identifier, the piece of client terminal equipment comprising:

132. To the extent the preamble is limiting, in my opinion Biswas and Kumar render obvious limitation 14[pre]. As discussed above, Biswas and Kumar render obvious the elements of this limitation, which occur on Biswas's host **102**. *See supra* § VI.A.9.a.

- (b) 14[a]: a memory that stores said configuration data;

133. In my opinion, Biswas and Kumar render obvious limitation 14[a]. As I discussed above, Biswas and Kumar render obvious storing the configuration data in memory on host **102**. *See supra* § VI.A.9.b.

- (c) 14[b]: before sending a data packet in the telecommunications network, a processor that selects a port number in the range of port numbers defined by the port mask, said data packet comprising as source address the primary address of said piece of client terminal equipment and as source port number the selected port number.

134. In my opinion, Biswas and Kumar render obvious limitation 14[b]. As I discussed above, Biswas and Kumar render obvious the steps of this limitation. *See supra* § VI.A.9.c. A POSITA would have found it obvious, in my opinion, to

use a processor to perform these steps. As discussed above, it is typical for computers to use processors to operate. *See supra* § VI.A.8.b. Host **102** is no different, it also uses a processor to perform its disclosed functions. *Id.* Thus, in my opinion, Biswas and Kumar render obvious limitation 14[b].

13. Claim 16: A non-transitory computer readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 7

135. In my opinion, Biswas and Kumar render obvious claim 16. As I discussed above, Biswas and Kumar render obvious claim 7. *See supra* § VI.A.5. Biswas also describes non-transitory computer readable mediums that execute instructions using a processor. *E.g.*, EX1022, 3:59-4:4, 13:58-14:16, 17:63-18-21.

14. Claim 17: A non-transitory computer-readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 11.

136. In my opinion, Biswas and Kumar render obvious claim 17. As I discussed above, Biswas and Kumar render obvious claim 11. *See supra* § VI.A.9. Biswas also describes non-transitory computer readable mediums that execute instructions using a processor. *E.g.*, EX1022, 3:59-4:4, 13:58-14:16, 17:63-18-21.

B. Ground 2: Claims 1-3, 5-6, and 15 Are Obvious in View of Fangman and Kumar

137. In my opinion, Fangman in view of Kumar renders claims 1-3, 5-6, and 15 of the '369 patent obvious.

138. In particular, this ground asserts that Fangman discloses the '369 patent's methods, apparatuses, and computer-readable mediums that route incoming data packets to appropriate destination equipment based on the port number and IP address in the incoming data packets. Kumar further discloses representing the range of port numbers as a port mask, and routing data packets based on whether the destination port number corresponds to a port mask that is assigned to a destination equipment. In my opinion, Fangman in view of Kumar renders obvious claims 1-3, 5-6, and 15.

1. Fangman (EX1024)

139. U.S. Patent No. 7,068,647 ("Fangman") was filed on July 11, 2001 and issued on June 27, 2006.

140. Fangman describes methods and systems for routing IP packets in networks supporting IP telephones and "Voice over Internet Protocol" (or "VoIP" for short). EX1024, Abstract, 1:1-2, 1:17-22. Like the '369 patent, Fangman explains that the "popular growth on the Internet" has led to the "depletion of remaining available addresses" and the need for improved "NAT technology" that permits "a single public IP address to be used to support thousands of hosts using private (RFC 1918) addresses." *Id.*, 1:40-56. Fangman thus discloses a process where each host is assigned a range of port numbers. *Id.*, 8:45-57, 8:4-9; *see also id.*, 14:12-14, 10:66-67, 11:14-15.

141. Figure 3B (below) depicts an embodiment of Fangman's VoIP network:

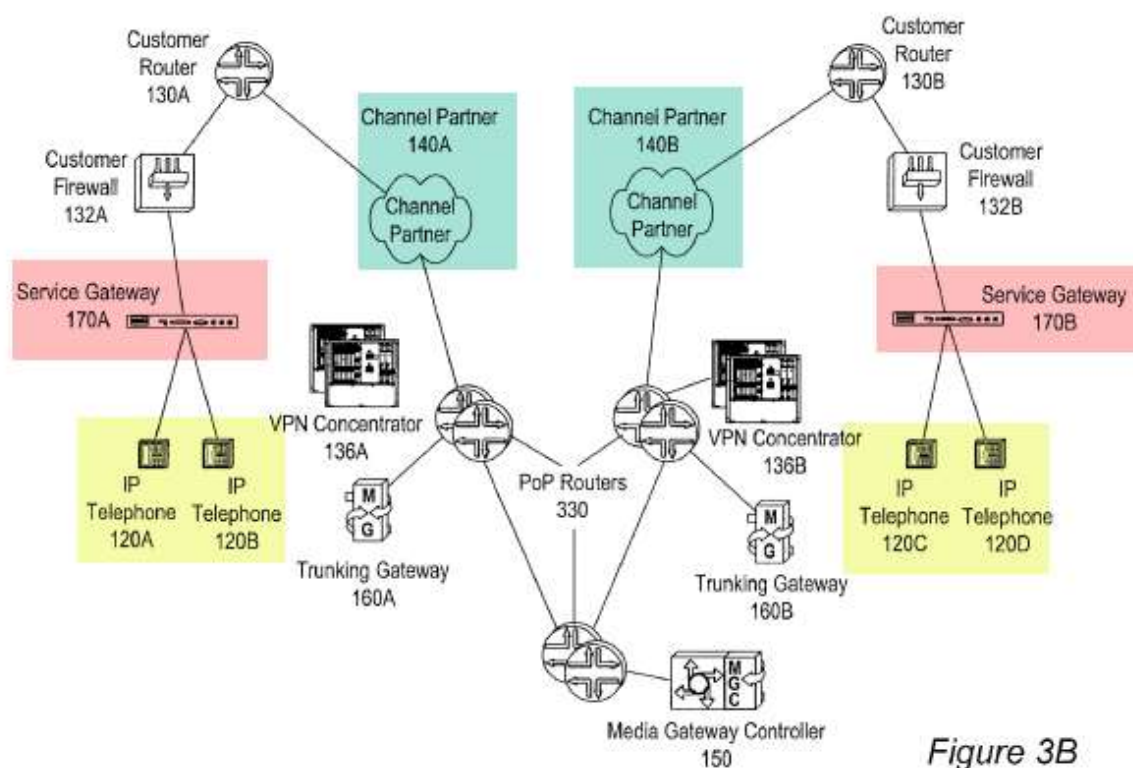


Figure 3B

Id., Fig. 3B (colors added). The IP telephones (yellow), also referred to as “internal hosts,” are connected to a service gateway at a customer premises (red). *Id.*, 12:2-4. The service gateway is in turn connected to “Internet Service Providers,” which are referred to as “Channel Partners” (green), via “customer routers.” *Id.*, 7:12-21.

142. Each internal host (e.g., IP telephones **120A** and **120B**) has its own “private IP address” for use within the private network. *Id.*, 12:1-10 (“[T]he internal hosts, or IP telephones, may use a private IP address.”). To reach the public network, Fangman's service gateways are equipped with its improved NAT functionality

(called “NAPPT”). *Id.*, 8:6-9. In particular, like conventional NAT processes each service gateway (*e.g.*, service gateway **170A**) has a “single, public IP address” for “all the internal hosts.” *Id.*, 8:21-31, 1:51-56. However, “[i]nstead of dynamically assigning ports to IP telephones,” the service gateway assigns each of the hosts that share this public address a semi-permanent “range of port numbers.” *Id.*, 8:21-32, 18:45-57. In this manner, the combination of a public IP address (shared by multiple hosts) and an assigned port range can “uniquely identify the IP telephone.” *Id.*, 18:37-46, 4:17-25.

143. To perform Network Address Persistent Port Translation (“NAPPT”), the service gateway also maintains a table that contains mappings between the public IP address and assigned port range for an internal host and the private IP address for that internal host. *Id.*, 8:49-56. Thus, when service gateway **170A** “receives a data packet” that is “destined for the IP telephone” **120A**, the packet can then be routed to its destination using the private IP address of telephone **120A**. *Id.*, 18:31-47.

2. The Fangman-Kumar Combination

144. In the Fangman-Kumar combination, in my opinion, Fangman discloses an edge router that implements a method for configuring a piece of terminal equipment connected to a telecommunications network, including by assigning a piece of terminal equipment a shared primary address, a range of port numbers dedicated to it, and a routing identifier. Although Fangman does not provide the

implementation detail of using a port mask to define the range of port numbers assigned to the terminal equipment, in my opinion Kumar's teachings supply this additional detail by disclosing port masks that define a range of port numbers. Thus, in the Fangman-Kumar combination, in my view, Fangman would continue to assign a range of port numbers to a piece of terminal equipment but would use port masks to define the range. In my opinion, the Fangman-Kumar combination renders claims 1-3, 5-6, and 15 obvious.

3. Motivations to Combine

145. I explain the multiple reasons to combine Fangman and Kumar in my analysis below.

4. Claim 1

- (a) 1[pre]: A method of routing an IP data packet in a telecommunications network to a destination equipment, said packet comprising a primary destination address and a destination port number, said method comprising, on reception of said packet, the following steps:

146. In my opinion, to the extent the preamble is limiting, Fangman discloses limitation 1[pre]: “a method of routing an IP data packet [*e.g.*, **data packet received at service gateway 170**] in a telecommunications network [*e.g.*, **network of Figure 3B**] to a destination equipment [*e.g.*, **IP telephones 120**], said packet comprising a primary destination address [*e.g.*, **public destination IP address**] and a destination port number [*e.g.*, **destination port number**].”

147. Fangman discloses a method of routing “IP packets” in a telecommunication network to IP telephones **120**. EX1024, Abstract, 13:55-58, 18:31-47; *see also id.*, 1:1-2 (“system and method for routing IP packets”). Figure 3B (reproduced below) depicts an embodiment of the network in which IP telephones (yellow) are connected to service gateways (red). The service gateways connect the IP telephones to “Internet Service Providers,” which are referred to as “Channel Partners” (green), via “customer router” **130**. *Id.*, 7:12-21, 7:47-54.

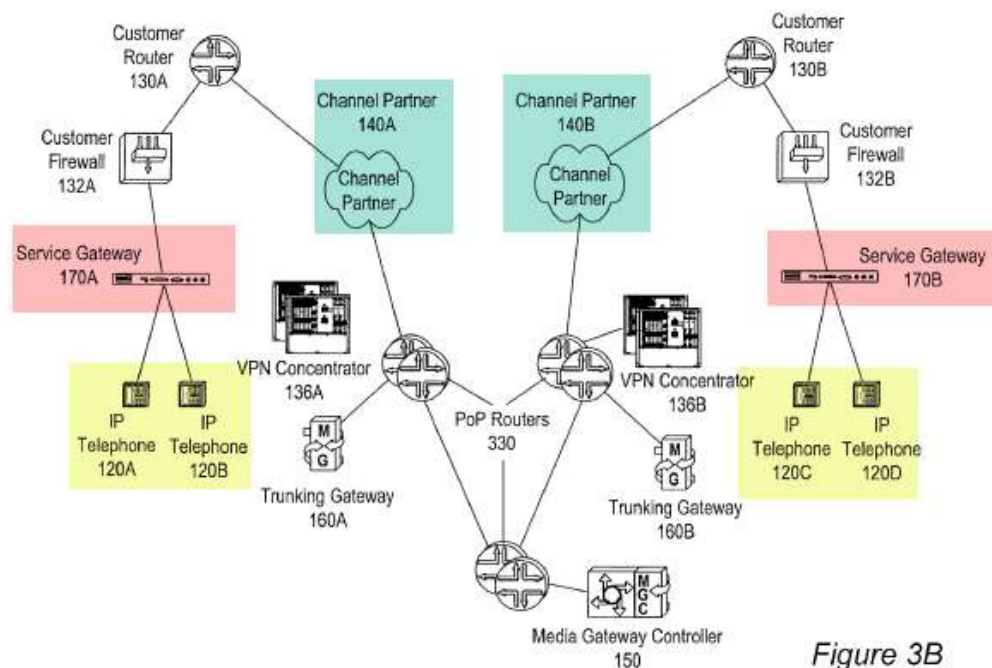


Figure 3B

Id., Fig. 3B (colors added).

148. In my view, Fangman’s IP telephones **120** correspond to the “destination equipment” in the ’369 patent. Indeed, the ’369 patent states that the

destination equipment, which it also calls the “terminal equipment,” can be “telephones or personal computers.” EX1001, 8:5-11.

149. Fangman also discloses that service gateways **170** route an “IP packet” to an IP telephone that comprises a “primary destination address” and a “destination port number.” EX1024, 4:17-33, 18:30-47, Abstract. For instance, Fangman states that “service gateways may mediate IP communications between the IP telephone and an IP device, such as another IP telephone.” *Id.*, 3:65-4:3. Fangman further teaches that this involves “SG 170 receiv[ing] a data packet from the IP device destined for the IP telephone **120**,” and that “the data packet may include a public destination IP address [and] a destination port number ... where the destination port number is in the assigned range of port numbers for the IP telephone **120**.” *Id.*, 3:65-4:3, 4:17-33, 18:30-47, Abstract; *see also* Fig. 10B (box 1064, showing that “SG 2” receives a packet having “Dest. IP” that is equal to “Phone 2 Public” and “Dest. Port” that is equal to “Phone 2 port.”).

150. In my opinion, the “public destination IP address” in Fangman corresponds to the “primary address” in the ’369 patent. For instance, like the “public destination IP address” in Fangman, the ’369 patent discloses that an example of a “primary address is advantageously a public address.” EX1001, 3:44-46. The “public destination IP address” is also a public address, in my opinion, because it is used to communicate over the public network. EX1022, 6:41-49.

151. Like the port numbers disclosed in the '369 patent, which can be used for different connections, like "P2P (Peer to Peer), FTP (File Transfer Protocol), web browsing, telephone, etc. applications," (EX1001, 7:22-27), in my opinion Fangman's port numbers in the range of port numbers can also be used for these connections. Indeed, a POSITA would have understood that the port numbers in Fangman and the '369 patent are typical implementations of port numbers.

- (b) 1[a]: determining a port mask assigned to the destination equipment, the port mask defining a range of port numbers to which the destination port number belongs;

152. In my opinion, Fangman in view of Kumar render obvious limitation 1[a]: "determining a port mask [*e.g.*, **Kumar's port mask**] assigned to the destination equipment [*e.g.*, **Fangman's IP telephones 120**], the port mask defining a range of port numbers [*e.g.*, **Fangman's range of port numbers**] to which the destination port number belongs."

153. As Fangman explains, each of the IP telephones is assigned a range of port numbers by service gateway **170**. EX1024, 3:14-25, 8:45-49, 17:21-25. When service gateway **170** receives an IP data packet destined for IP telephone **120**, the service gateway must perform "NAPPT on the data packet" to "change the public destination IP address to a private destination IP address" for the IP telephone. *Id.*, 4:17-33, 18:30-47. In particular, Fangman explains that to perform NAPPT on received data packets, the service gateway "maintain[s] a table" that "map[s]" the

port range assigned to an IP telephone to its internal (or “private”) IP address. *Id.*, 8:45-58, 10:66-67, 11:14-15. Thus, in my opinion, a POSITA would have understood that the service gateway **170** consults its mapping table to determine “the assigned range of port numbers” to which the “destination port number” in the IP packet belongs, and then replaces the public IP address in the received packet with the private IP address for the IP telephone that is associated with that range of port numbers. Indeed, Fangman explicitly teaches that “[p]erforming a NAPPT on the data packet may include using the public destination IP address and the destination port number to uniquely identify the IP telephone **120**.” *Id.*, 18:31-47, 4:17-33. In my opinion, a POSITA would have known that the service gateway **170** would consult its mapping table to perform NAPPT and determine the assigned port range that includes the destination port number.

154. For instance, in the case of a packet that is received at service gateway **170A** and destined for IP telephone **120A**, the service gateway determines that the destination port number in the IP packet “is in the assigned range of port numbers for the IP telephone” **120A** by consulting its mapping table, and then replaces the public IP address of the packet with the private IP address for IP telephone **120A**. *Id.*, 18:31-47; *see also id.*, Fig. 10B (box 1064: “SG 2 performs NAPPT” involving changing “Dest. IP” from “Phone 2 Public changed to Phone 2 private”), 30:12-23.

155. Although Fangman does not provide the implementation detail that the service gateway uses a port mask to define the range of port numbers in the mapping table, a POSITA would have found it obvious to do so. Indeed, as I already explained above, Fangman's service gateway maintains a table of port ranges that have been assigned to the IP telephones and determines the range of port numbers to which a destination port number in a received data packet belongs. Also discussed above, Kumar discloses using a port mask to make this determination. *See supra* § VI.A.5.c. Kumar discloses port masks that are similar to those disclosed in the '369 patent, and expressly teaches that its port masks may define "a range" of port numbers. *Id.*; EX1023, 7:31-38, Fig. 7B.

156. In my opinion, a POSITA would have been motivated to combine the teachings of Fangman and Kumar.

157. As a threshold matter, Fangman, Kumar, and the '369 patent are analogous art because they are in the same field of endeavor, *i.e.*, computer networking and routing data packets. EX1024, 1:1-2, 8:33-43; EX1023, 1:7-24, 2:57-65; EX1001, 1:15-36. For instance, Fangman discloses a service gateway in an IP communications network that configures hosts and routes data packets to those hosts (EX1024, 1:1-2, 8:33-43), Kumar discloses that its teachings "are generally applicable to any device, system, and/or circumstance where classification of packets or other communications is needed" (EX1023, 2:57-65), and further explains

that it discloses a “routing technique” to route packets in a computer network (*id.*, 1:7-24), and the ’369 patent explains that its “field of invention is that of telecommunications networks,” including “rout[ing] data packets sent by pieces of terminal equipment to their final destination” (EX1001, 1:15-36).

158. Further, Fangman does not disclose the details of how service gateway
170 determines whether a destination port number is within one of its stored port ranges. EX1024, 4:17-33, 8:45-58, 18:31-47. In my opinion, a POSITA would have been aware that masks could be used to determine whether a number lies within a range. *See supra* § III.C. Masks in general were well known in the prior art for decades. *Id.* And the use of masks to determine whether a number falls within a range was ubiquitous in computer networking. *Id.* For example, in my opinion, a POSITA would have been aware that networks routinely used masks to determine whether the destination address in an incoming data packet fell within the range of addresses in the network. *Id.* In my opinion, a POSITA would have further been aware that masks were used in the prior art to classify incoming port numbers—and determine whether those incoming port numbers fall within a specified range—as well. *Id.* Thus, in my opinion, a POSITA would be motivated to look to references, like Kumar, that discuss classifying packets based on their port numbers, and, in my opinion, a POSITA would have been particularly interested in references, like Kumar, that use the common and well-known technique of masking to make these

classifications. Indeed, a POSITA would have found combining Fangman and Kumar obvious because Kumar teaches that its disclosures “are generally applicable to any device, system, and/or circumstance where classification of packets or other communications is needed.” EX1023, 2:57-65.

159. Moreover, in my opinion, a POSITA would have been motivated to combine the teaching of these two references because, by the time of the alleged invention of the '369 patent, it was well-known that bit masks, such as port masks, as used in the '369 patent, could be used to optimize performance. For example, a POSITA would have recognized that Kumar's port masks are computationally efficient because they use only bitwise operations, like logical ANDs. Thus, an inclusion in the range can be efficiently computed with one logical operation and a comparison to zero.

160. Further, in my opinion, a POSITA would have found combining Fangman and Kumar obvious because Kumar teaches that its disclosures “are generally applicable to any device, system, and/or circumstance where classification of packets or other communications is needed.” EX1023, 2:57-65. Fangman itself explains that “numerous variations and modifications will become apparent to those skilled in the art once the above disclosure is fully appreciated” and that “[i]t is intended that the following claims be interpreted to embrace all such variations and modifications.” EX1024, 32:28-34.

161. Additionally, in my opinion, the combination would have been of a known technique (*i.e.*, Kumar’s port mask rules) to a known device (*i.e.*, Fangman’s service gateway **170**) to yield predictable results (*i.e.*, a service gateway that can use port masks to determine whether a destination port number falls within an assigned port range). Indeed, Kumar was already using port masks to define ranges of port numbers in its own invention. *See supra* § VI.A.2. And Kumar further disclosed using these port masks on a router in a network to help with typical network activities, like routing data packets. *Id.* So not only would the combination apply a known technique to a known device to yield a predictable result, but Kumar was *already* applying this known technique to the same or a similar known device to yield the same or a similar result.

162. Moreover, it is my opinion that a POSITA would have had a reasonable expectation of success in combining Fangman and Kumar because the combination merely involves the straightforward application of Kumar’s port masks to the service gateway of Fangman to define a port range. As discussed above, Kumar already discloses an embodiment that is similar to the proposed combination; Kumar discloses a router that uses port masks to represent a range of port numbers, the router further using that port mask to assist with typical network operations, like routing data packets. *See supra* § VI.A.2. Indeed, this reasonable expectation of success is echoed by Kumar, which is “generally applicable to any device, system,

and/or circumstance where classification of packets or other communications is needed.” For at least these reasons, in my opinion, a POSITA would have been motivated to combine Fangman and Kumar as described above.

- (c) 1[b]: selecting at least one identifier of the destination equipment of the packet from a plurality of equipment identifiers associated with said primary destination address based on the port mask; and

163. In my opinion, Fangman in view of Kumar renders obvious limitation 1[b]: “selecting at least one identifier [*e.g.*, **Fangman’s private IP address**] of the destination equipment [*e.g.*, **Fangman’s IP telephone 120**] of the packet from a plurality of equipment identifiers [*e.g.*, **Fangman’s private IP addresses for IP telephones 120A-D**] associated with said primary destination address [*e.g.*, **Fangman’s public IP address**] based on the port mask [*e.g.*, **Kumar’s port mask**].”

164. Fangman discloses a plurality of equipment identifiers (*e.g.*, **private IP addresses**) associated with said primary destination address (*e.g.*, **a public IP address**). Fangman explains that network address port translation is a technique that “allows a single public IP address to be used to support thousands of hosts using private (RFC 1918) addresses.” EX1024, 1:54-56. Consistent with this, Fangman discloses that service gateways (*e.g.*, service gateway **170A**) have a “single, public IP address” to provide network address persistent port translation support to multiple

internal hosts (*e.g.*, IP telephones **120A** and **120B**), each of which is assigned a private IP address. *Id.*, 8:20-31, 12:7-13.

165. In my opinion, a POSITA would have understood that a “private IP address” in Fangman is an “equipment identifier.” Indeed, the ’369 patent also teaches that an example of an equipment “identifier” is a “secondary destination address” (EX1001, 3:47-50, 14:29-31), such as a “private address” (*id.*, 3:50-52, 9:9-11). And as I already explained in connection with limitation 1[pre], a POSITA would have understood that Fangman’s public IP address is a “primary destination address.” *See supra* § VI.B.4.a.

166. In my opinion, Fangman also teaches selecting at least one identifier from the plurality of equipment identifiers based on the port range. To perform NAPPT, service gateways **170** maintain a table that maps the “external” (*i.e.*, public) IP address and assigned port range for a host to a private IP address for the host:

NAT/NAPT/NAPPT

Instead of dynamically assigning ports to IP telephones, the **SG 170 may allocate a range of port numbers for each IP telephone 120** as it acquires its lease during a DHCP process, described below with reference to FIGS. 5A and 5B. **The SG 170 may maintain a table of semi-permanent mappings of the external IP address and ports to the internal hosts and ports. The SG 170 may continue to replace the internal or private source IP address with the NATed external source IP address.** It may not, however, modify the port information, though it may validate it to ensure the correct internal host is using its assigned port range. Such Network Address Translation

may be referred to as Network Address Persistent Port Translation (NAPPT).

EX1024, 8:49-52. Thus, when a packet “destined for the IP telephone” (e.g., IP telephone **120A**) is received, the service gateway **170** will (1) consult its mapping table to determine “the assigned range of port numbers” to which the “destination port number” in the IP packet belongs, and then (2) based on the matching port range in the table, the service gateway will replace the public IP address in the received packet with the private IP address for the IP telephone to which the packet is to be routed:

Conversely, when the SG 170 receives a data packet from the IP device destined for the IP telephone 120, the data packet may include a public destination IP address, a destination port number; and source information associated with the IP device, where the destination port number is in the assigned range of port numbers for the IP telephone 120. In one embodiment, the public destination IP address and the destination port number may be used to uniquely identify the IP telephone 120. Performing a NAPPT on the data packet may include using the public destination IP address and the destination port number to uniquely identify the IP telephone 120, and changing the public destination IP address to a private destination IP address while leaving the destination port number unchanged. Note that in this embodiment, the private IP address may be an IP address of the IP telephone 120. After NAPPTing the data packet, the SG 170 may send the data packet to the IP telephone 120.

Id., 18:39-47, 4:17-33, Abstract; *see also id.*, 8:52-56 (when performing NAPPT, service gateway “may validate” the port number in the IP packet “to ensure the correct internal host is using its assigned port range.”).

167. As discussed in connection with limitation 1[a], in the combined system of Fangman in view of Kumar, the service gateway would determine a port mask defining a range of port numbers to which the destination port number belongs, such that the service gateway would determine the private IP address for the IP telephone based on the port mask that defines the range of port numbers to which the destination port number belongs. As I discussed in connection with limitation 1[a], a POSITA would have found it obvious to combine Fangman and Kumar in this manner and would have been motivated to do so.

(d) 1[c]: routing the packet to the destination equipment based on said identifier.

168. In my opinion, Fangman discloses limitation 1[c]: “routing the packet [e.g., **IP data packet received by the service gateway 170**] to the destination equipment [e.g., **IP telephone 120**] based on said identifier [e.g., **the private IP address of IP telephone 120**].”

169. As I explained in connection with limitation 1[b], service gateway **170** “[p]erform[s] a NAPPT on the data packet” that “change[s] the public destination IP address to a private destination IP address” for the IP telephone **120**. EX1024, 18:31-42. Fangman further teaches that “[a]fter NAPPTing the data packet, the SG

170 may send the data packet to the IP telephone **120**” using the private destination IP address. *Id.*, 18:46-47, Abstract. For instance, Figure 10B of Fangman illustrates a service gateway routing the packet to “Phone 2” (yellow) after performing a NAPPT operation that changes the destination IP address of the packet from “Phone 2 Public... to Phone 2 private” (red):

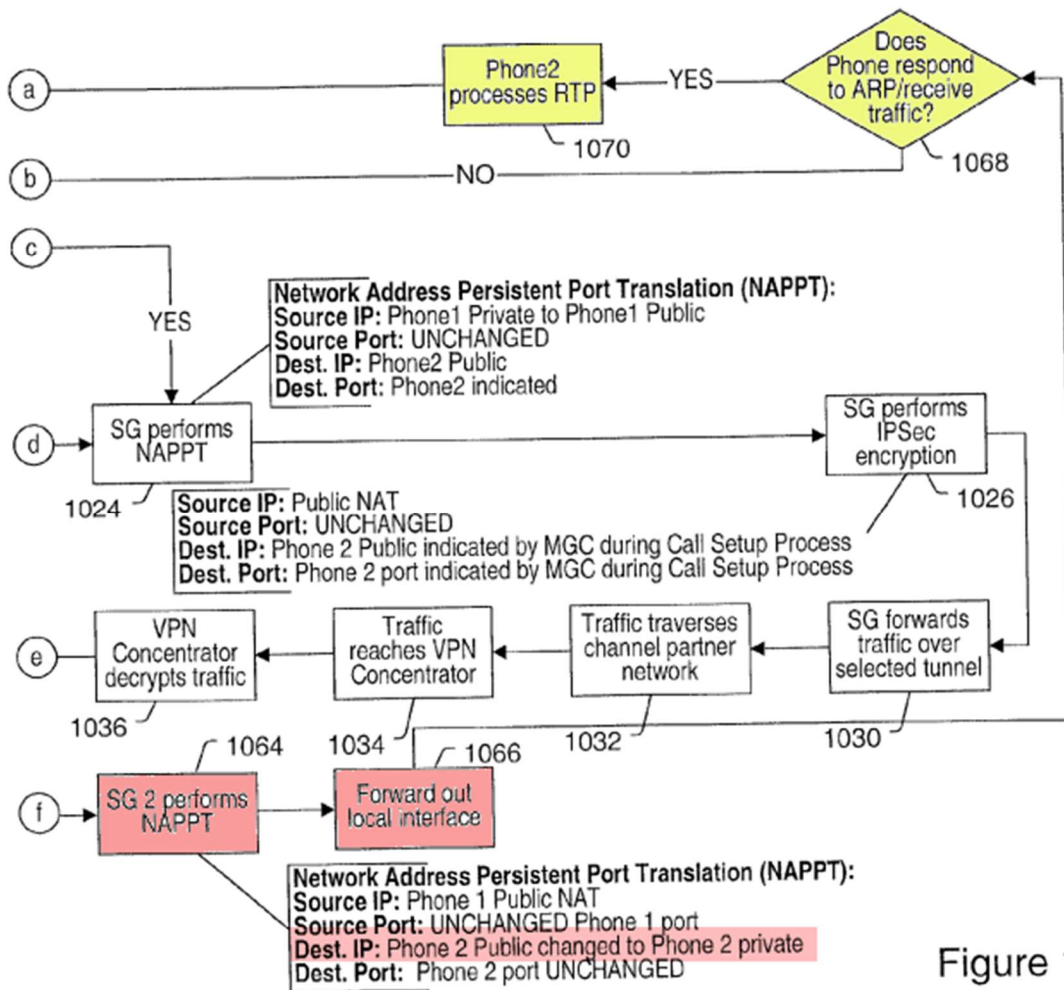


Figure 10B

Id., Fig. 10B (colors added), 30:12-41.

5. Claim 2: The method according to claim 1 of routing an IP data packet, wherein said at least one identifier is a secondary destination address of the destination equipment.

170. In my opinion, Fangman discloses the additional limitation of claim 2: “routing an IP data packet [*e.g.*, **IP data packet received by the service gateway 170**], wherein said at least one identifier is a secondary destination address [*e.g.*, **Fangman’s private IP address**] of the destination equipment [*e.g.*, **IP telephone 120**].” For instance, Fangman teaches that the IP packet is routed using the private destination address:

Conversely, when the SG 170 receives a data packet from the IP device destined for the IP telephone 120, the data packet may include a public destination IP address, a destination port number; and source information associated with the IP device, where the destination port number is in the assigned range of port numbers for the IP telephone 120. In one embodiment, the public destination IP address and the destination port number may be used to uniquely identify the IP telephone 120. **Performing a NAPPT on the data packet may include** using the public destination IP address and the destination port number to uniquely identify the IP telephone 120, and **changing the public destination IP address to a private destination IP address while leaving the destination port number unchanged**. Note that in this embodiment, the private IP address may be an IP address of the IP telephone 120. **After NAPPTing the data packet, the SG 170 may send the data packet to the IP telephone 120.**

Id., 18:39-47, 4:17-33, Abstract. As the ’369 patent explains, a “secondary address” is merely the private IP address of the destination equipment in one embodiment.

EX1001, 3:50-51. Similarly, Fangman uses the private IP address of the IP telephone as the identifier. *See supra* § VI.B.4.c.

6. Claim 3: The method according to claim 2 of routing an IP data packet, comprising, before the routing step, a step of transforming the packet by adding said secondary address to the packet, and routing the packet based on said secondary destination address.

171. In my opinion, Fangman discloses the additional limitation of claim 3: “routing an IP data packet [*e.g.*, **IP data packet received by the service gateway 170**], comprising, before the routing step, a step of transforming the packet by adding said secondary address to the packet [*e.g.*, **changing the public destination IP address to a private destination IP address**], and routing the packet based on said secondary destination address.” Fangman teaches transforming the packet before routing it. In particular, Fangman explains that the service gateway **170**, upon receiving an incoming data packet, “chang[es] the public destination IP address to a private destination IP address” before it “send[s] the data packet to the IP telephone **120**.” EX1024, 18:31-47. Similarly, the ’369 patent explains that “the transformation step” can be “add[ing] the secondary address of the destination equipment to a field of the packet.” EX1001, 4:1-3.

7. Claim 5

- (a) 5[pre]: A device for routing an IP data packet in a telecommunications network to a destination equipment, said packet comprising a primary destination address and

a destination port number, wherein said device comprises, on reception of said packet:

172. As discussed in connection with Ground 2, Claim 1[pre], Fangman discloses that **service gateway 170** routes an IP data packet in a telecommunications network to a destination equipment, said packet comprising a primary destination address and a destination port number. *See supra* § VI.B.4.a. Thus, in my opinion, Fangman discloses limitation 5[pre].

- (b) 5[a]: a processor that determines a port mask assigned to the destination equipment, the port mask defining a range of port numbers to which the destination port number belongs;

173. As I discussed in connection with Ground 2, Claim 1[a], Fangman and Kumar render obvious that **service gateway 170** determines a port mask assigned to the destination equipment, the port mask defining a range of port numbers to which the destination port number belongs. *See supra* § VI.B.4.b. A POSITA would have understood that the service gateway uses a processor to perform this operation. EX1024, 32:15-20. In particular, a POSITA would have known that routing devices, like the service gateway **170**, use processors to perform functions, like the steps claimed in this limitation. Additionally, Fangman explains that its disclosed computer systems “can be broadly defined to encompass any device having at least one processor which executes instructions from a memory medium.” *Id.*, 32:15-20.

- (c) 5[b]: the processor selects an identifier of the destination equipment of the packet from a plurality of equipment

identifiers associated with said primary destination address based on the port mask; and

174. As I discussed in connection with Ground 2, Claim 1[b], Fangman and Kumar render obvious that **service gateway 170** selects an identifier of the destination equipment of the packet from a plurality of equipment identifiers associated with said primary destination address based on the port mask. *See supra* § VI.B.4.c. As discussed above, a POSITA would have understood the service gateway uses a processor to perform this operation. EX1024, 32:15-20; *see supra* § VI.B.7.b.

(d) 5[c]: a communication unit that routes the packet to the destination equipment based on said identifier.

175. As discussed in connection with Ground 2, Claim 1[c], Fangman discloses that **service gateway 170** routes the packet to the destination equipment based on said identifier. *See supra* § VI.B.4.d. A POSITA would have understood that the service gateway uses a communication unit to route the packet. EX1024, 30:23-24, Fig. 10B (box 1066, showing communication unit of service gateway “forward[ing]” packet “out local interface” using “Phone 2[’s] private” IP address).

8. Claim 6

(a) 6[pre]: Telecommunications network equipment adapted to receive an IP data packet comprising a primary

destination address and a destination port number,
comprising at least one routing device comprising:

176. As I discussed in connection with Ground 2, Claim 1[pre], Fangman discloses telecommunications network equipment, such as **service gateway 170**, that is adapted to receive and route an IP data packet comprising a primary destination address and a destination port number. *See supra* § VI.B.4.a.

- (b) 6[a]: a processor that determines a port mask assigned to a destination equipment, the port mask defining a range of port numbers to which the destination port number belongs;

177. As discussed in connection with Ground 2, Claim 5[a], Fangman and Kumar render obvious this limitation. *See supra* § VI.B.7.b.

- (c) 6[b]: the processor selects an identifier of the destination equipment of the packet from a plurality of equipment identifiers associated with said primary destination address based on the port mask; and

178. As discussed in connection with Ground 2, Claim 5[b], Fangman and Kumar render obvious this limitation. *See supra* § VI.B.7.c.

- (d) 6[c]: a communication unit that routes the packet to the destination equipment based on said identifier.

179. As discussed in connection with Ground 2, Claim 5[c], Fangman discloses this limitation. *See supra* § VI.B.7.d.

9. Claim 15: A non-transitory computer readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 1.

180. Fangman discloses and, in my opinion, a POSITA would have understood that service gateway includes a non-transitory computer readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 1. EX1024, 4:34-46, 31:62-32:20.

C. Ground 3: Claims 1-3, 5-6, and 15 Are Obvious in View of King and Kumar

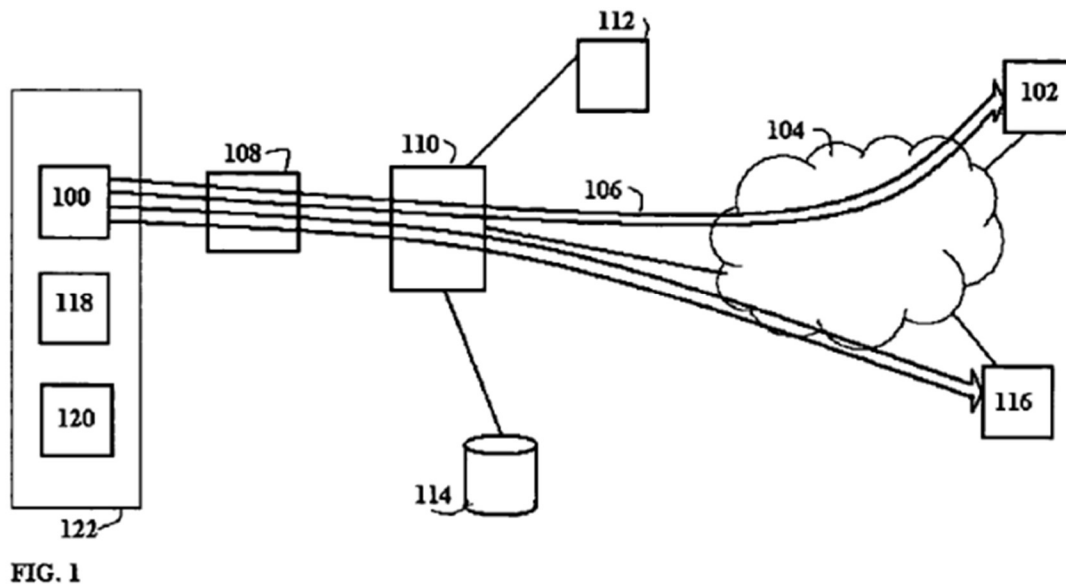
181. In my opinion, King in view of Kumar renders claims 1-3, 5-6, and 15 of the '369 patent obvious.

182. In particular, this ground asserts that King discloses the '369 patent's methods, apparatuses, and computer-readable mediums that route incoming data packets to appropriate destination equipment based on the port number and IP address in the incoming data packets. Kumar further discloses representing the range of port numbers as a port mask, and routing data packets based on whether the destination port number corresponds to a port mask that is assigned to a destination equipment. In my opinion, King in view of Kumar renders obvious claims 1-3, 5-6, and 15.

1. King (EX1025)

183. U.S. Patent No. 8,032,639 ("King") was filed on May 23, 2006 and granted on October 4, 2011. EX1025.

184. King describes a network in which user devices **100**, **118**, and **120** belong to a “community of source devices” **122**. *Id.*, 1:34-44, 2:49-51. These user devices send data packets over the Internet **104** to remote devices **102** and **116**. *Id.*, 1:45-59. Several intermediary devices assist in routing the data packet from the user devices to the remote devices, like the customer premises equipment **108** and the aggregation device **110**. *Id.*



Id., Fig. 1.

185. King improves on PAT by assigning ranges of port numbers to individual user devices. For example, Figure 7 shows that the range of port numbers 1024-1039 is assigned to user device **100**, while the range of port numbers 1040-1055 is assigned to user device **118**. *Id.*, 5:23-32

SOURCE ADDRESS	TCP PORT	USER DEVICE
IPCPE	1024-1039	IP1'
IPCPE	1040-1055	1P2'

FIG. 7

Id., Fig. 7. Incoming packets (*i.e.*, packets that are sent from a remote device to a user device) “can then be classified” based on the assigned port range. *Id.*, 5:36-42. For example, when the aggregation device receives a data packet that contains (1) the customer premises equipment’s IP address and (2) port number 1024, the aggregation device can determine that port number 1024 belongs to the range of port numbers associated with user device **100**. *Id.*, 5:36-57.

2. The King-Kumar Combination

186. In the King-Kumar combination, in my opinion King discloses intermediary devices that assign user devices a shared primary address, a range of port numbers dedicated to it, and a routing identifier. Although King does not provide the implementation detail of using a port mask to define the range of port numbers assigned to the terminal equipment, Kumar’s teachings supply this additional detail by disclosing port masks that define a range of port numbers. Thus, in the King-Kumar combination, in my view, King would continue to assign a range of port numbers to a piece of terminal equipment but would use port masks from

Kumar to define the range. In my opinion, the King-Kumar combination renders claims 1-3, 5-6 and 15 obvious.

3. Reasons to combine King and Kumar

187. I explain the multiple reasons to combine King and Kumar in my analysis below.

4. Claim 1

- (a) 1[pre]: A method of routing an IP data packet in a telecommunications network to a destination equipment, said packet comprising a primary destination address and a destination port number, said method comprising, on reception of said packet, the following steps:

188. To the extent the preamble is limiting, in my opinion King teaches limitation 1[pre]: “a method of routing an IP data packet [*e.g.*, **returning traffic**] in a telecommunications network to a destination equipment [*e.g.*, **user device 100**], said packet comprising a primary destination address [*e.g.*, **the overloaded IP address**] and a destination port number [*e.g.*, **destination TCP port number**].”

189. King discloses a “method [that] is implemented using one or more computer programs running on a network element such as a *router device*.” EX1025, 7:29-35. Particularly, a customer premises equipment (“CPE”) device **108** and an “aggregation device **110**.” *Id.*, 1:34-49, 2:62-3:41, 5:36-56, Fig. 4. King teaches that “returning traffic” is sent from, for example, remote device **102** through aggregation device **110** and CPE **108** to user device **100**. *Id.*, 3:2-6, Fig. 5. In my opinion, a POSITA would have understood that a user device (*e.g.*, “user device

100”) is “a destination equipment” in the return path because it is the destination where the data sent from the remote device to the user device is to be routed.

190. King discloses that the “returning traffic” contains a “translated overloaded IP address and TCP port” in the destination address and TCP destination port fields, respectively. *Id.*, 3:2-6, Figs. 2 & 5. For instance, a data packet sent by remote device **102** to user device **100** is received with the IP address (*i.e.*, IPCPE) and TCP port number (*i.e.*, 1024) that was inserted as part of the outbound translation process. *Id.*

191. In my opinion, the “translated overloaded IP address” corresponds to the “primary address” of the ’369 patent. The ’369 patent discloses that an example of a “primary address” is a public IP address that can be “shared with a plurality of pieces of terminal equipment.” EX1001, 3:44-46, 1:37-40. Similarly, the “overloaded IP address” of the CPE **108** “serv[es] multiple user devices.” EX1025, 2:55-61. Indeed, King refers to the address as “overloaded” because it is shared by multiple devices. In my opinion, a POSITA would have also understood that King’s “overloaded IP address” is a public IP address because it can traverse the public Internet (*e.g.*, Internet **104** in Figure 1 of King).

192. In my opinion, the “TCP port” number in the TCP destination port field of the packet corresponds to the “destination port number” of the ’369 patent. Like the port numbers disclosed in the ’369 patent, which can be used for different

connections, like “P2P (Peer to Peer), FTP (File Transfer Protocol), web browsing, telephone, etc. applications,” (EX1001, 7:22-27), in my opinion King’s port numbers in the range of port numbers can also be used for these connections. Indeed, a POSITA would have understood that the port numbers in King and the ’369 patent are typical implementations of port numbers.

- (b) 1[a]: determining a port mask assigned to the destination equipment, the port mask defining a range of port numbers to which the destination port number belongs;

193. In my opinion, King and Kumar render obvious limitation 1[a]: “determining a port mask [*e.g.*, **Kumar’s port mask**] assigned to the destination equipment [*e.g.*, **King’s user device 100**], the port mask defining a range of port numbers [*e.g.*, **King’s port range assigned to user device 100**] to which the destination port number [*e.g.*, **King’s destination TCP port number**] belongs.” To start, King teaches the “range of port numbers” in the ’369 patent. In Figure 7, King discloses assigning port ranges to user devices and storing those assignments in a database.

SOURCE ADDRESS	TCP PORT	USER DEVICE
IPCPE	1024-1039	IP1’
IPCPE	1040-1055	IP2’

FIG. 7

EX1025, Fig. 7, 5:36-57. For example, “the CPE may assign TCP port numbers 1024 to 1039 to data sessions associated with the first user or source device **100** and TCP port numbers 1040 to 1055 to data sessions associated with the second user or source device **118**.” *Id.*, 5:28-32. This assignment is stored by both CPE **108** and aggregation device **110**. *Id.*, 4:23-24, 5:36-65. “As a result, ... translation is carried out to separate port ranges per host device.” *Id.*, 5:32-35.

194. In my opinion, King, in combination with Kumar, teaches “determining a port mask assigned to the destination equipment ... to which the destination port number belongs.” King explains, on receipt of the data packet, that “incoming packets can then be classified ... based on source port range.” *Id.*, 5:26-46. “In particular on receipt of a packet with (translated) source address IPCPE [*i.e.*, **the primary destination address**] and (translated) TCP port in the range 1024 to 1039 [*i.e.*, **the destination port number**] the aggregation device derives corresponding source device information.” *Id.*, 5:42-46, 9:39-62 10:43-44. “Similarly if the port address is in the range 1040 to 1055 then the user device address is identified as IP2 or another mappable identifier/IP2.” *Id.*, 5:49-51. As I discussed above, Kumar teaches using a port mask to represent a port range. *See supra* §§ VI.A.2, VI.A.5.c.

195. In my opinion, a POSITA would have found it obvious to apply the teachings of Kumar to King such that King’s aggregation device **110** would determine port masks defining a range of port numbers to which the destination port

number belongs. Upon receipt of the incoming data packet, the aggregation device would need to determine which destination device the data packet is intended for. Accordingly, the aggregation device would use a port mask to identify the destination device based on the destination port number.

196. A POSITA would have been motivated to combine the teachings of King and Kumar in this manner.

197. As a threshold matter, King and Kumar are analogous art in my opinion because the references are in the same field of endeavor as each other and the '369 patent, *i.e.*, computer networking and routing data packets. EX1025, 1:23-44, 7:29-8:10; EX1023, 1:7-24, 2:57-65; EX1001, 1:15-36. For instance, King discloses “communication” that pass through intermediary router devices, like a CPE and aggregation device, to user devices (EX1025, 1:23-44, 7:29-8:10), Kumar discloses that its teachings “are generally applicable to any device, system, and/or circumstance where classification of packets or other communications is needed” (EX1023, 2:57-65), and further explains that it discloses a “routing technique” to route packets in a computer network (*id.*, 1:7-24), and the '369 patent explains that its “field of invention is that of telecommunications networks,” including “rout[ing] data packets sent by pieces of terminal equipment to their final destination” (EX1001, 1:15-36).

198. Further, King does not disclose the details of how “incoming packets can then be classified ... based on source port range.” EX1025, 5:26-46. In my opinion, a POSITA would have been aware that masks could be used to determine whether a number lies within a range. *See supra* § III.C. Masks in general were well known in the prior art for decades. *Id.* And the use of masks to determine whether a number falls within a range was ubiquitous in computer networking. *Id.* For example, in my opinion, a POSITA would have been aware that networks routinely used masks to determine whether the destination address in an incoming data packet fell within the range of addresses in the network. *Id.* In my opinion, a POSITA would have further been aware that masks were used in the prior art to classify incoming port numbers—and determine whether those incoming port numbers fall within a specified range—as well. *Id.* Thus, in my opinion, a POSITA would be motivated to look to references, like Kumar, that discuss classifying packets based on their port numbers, and, in my opinion, a POSITA would have been particularly interested in references, like Kumar, that use the common and well-known technique of masking to make these classifications. Indeed, a POSITA would have found combining King and Kumar obvious because Kumar teaches that its disclosures “are generally applicable to any device, system, and/or circumstance where classification of packets or other communications is needed.” EX1023, 2:57-

65. King itself explains that “[a]ny appropriate communication protocol and mechanism can be adopted to implement this invention.” EX1025, 9:38-42.

199. Moreover, in my opinion, a POSITA would have been motivated to combine the teaching of these two references because, by the time of the alleged invention of the ’369 patent, it was well-known that bit masks, such as port masks, as used in the ’369 patent, could be used to optimize performance. For example, a POSITA would have recognized that Kumar’s port masks are computationally efficient because they use only bitwise operations, like logical ANDs. Thus, an inclusion in the range can be efficiently computed with one logical operation and a comparison to zero.

200. Additionally, in my opinion, the combination would have been of a known technique (*i.e.*, Kumar’s port mask rules) to a known device (*i.e.*, King’s network configuration) to yield predictable results (*i.e.*, a network that can route incoming data packets according to destination port numbers). Indeed, Kumar was already using port masks to define ranges of port numbers in its own invention. *See supra* § VI.A.2. And Kumar further disclosed using these port masks on a router in a network to help with typical network activities, like routing data packets. *Id.* So not only would the combination apply a known technique to a known device to yield a predictable result, but Kumar was *already* applying this known technique to the same or a similar known device to yield the same or a similar result.

201. And it is my opinion that a POSITA would have a reasonable expectation of success in combining King and Kumar and there would have been no unexpected results because the combination merely involves the straightforward application of Kumar's method of classifying data packets according to pre-defined rules in King's network. As discussed above, Kumar already discloses an embodiment that is similar to the proposed combination; Kumar discloses a router that uses port masks to represent a range of port numbers, the router further using that port mask to assist with typical network operations, like routing data packets. *See supra* § VI.A.2. Indeed, this reasonable expectation of success is echoed by Kumar, which is "generally applicable to any device, system, and/or circumstance where classification of packets or other communications is needed." For at least these reasons, in my opinion, a POSITA would have been motivated to combine King and Kumar as described above.

- (c) 1[b]: selecting at least one identifier of the destination equipment of the packet from a plurality of equipment identifiers associated with said primary destination address based on the port mask; and

202. In my opinion, King and Kumar render obvious limitation 1[b]: "selecting at least one identifier of the destination equipment [*e.g.*, **King's IP address of user device 100**] of the packet [*e.g.*, **King's returning traffic**] from a plurality of equipment identifiers associated with said primary destination address based on the port mask [*e.g.*, **Kumar's port mask**]."

203. In my opinion, King teaches the “at least one identifier of the destination equipment” of the ’369 patent. The ’369 patent states that an example of an “identifier” is a “secondary destination address,” like the private address of the destination equipment. EX1001, 3:47-50, 14:29-31, 3:50-52, 9:9-11. Similarly, King derives user “device identifier information” from the port mask. EX1025, 5:43-46. King provides several examples of user “device identifier information,” including “the IP address of” the user device. *Id.*, 5:46-49. Figure 7 shows how this information is stored as well as “how [user] device identifier information can be derived from a received packet.” *Id.*, 5:36-43.

SOURCE ADDRESS	TCP PORT	USER DEVICE
IPCPE	1024-1039	IP1’
IPCPE	1040-1055	IP2’

FIG. 7

Id., Fig. 7. This process is described in further detail in King’s Figure 8:

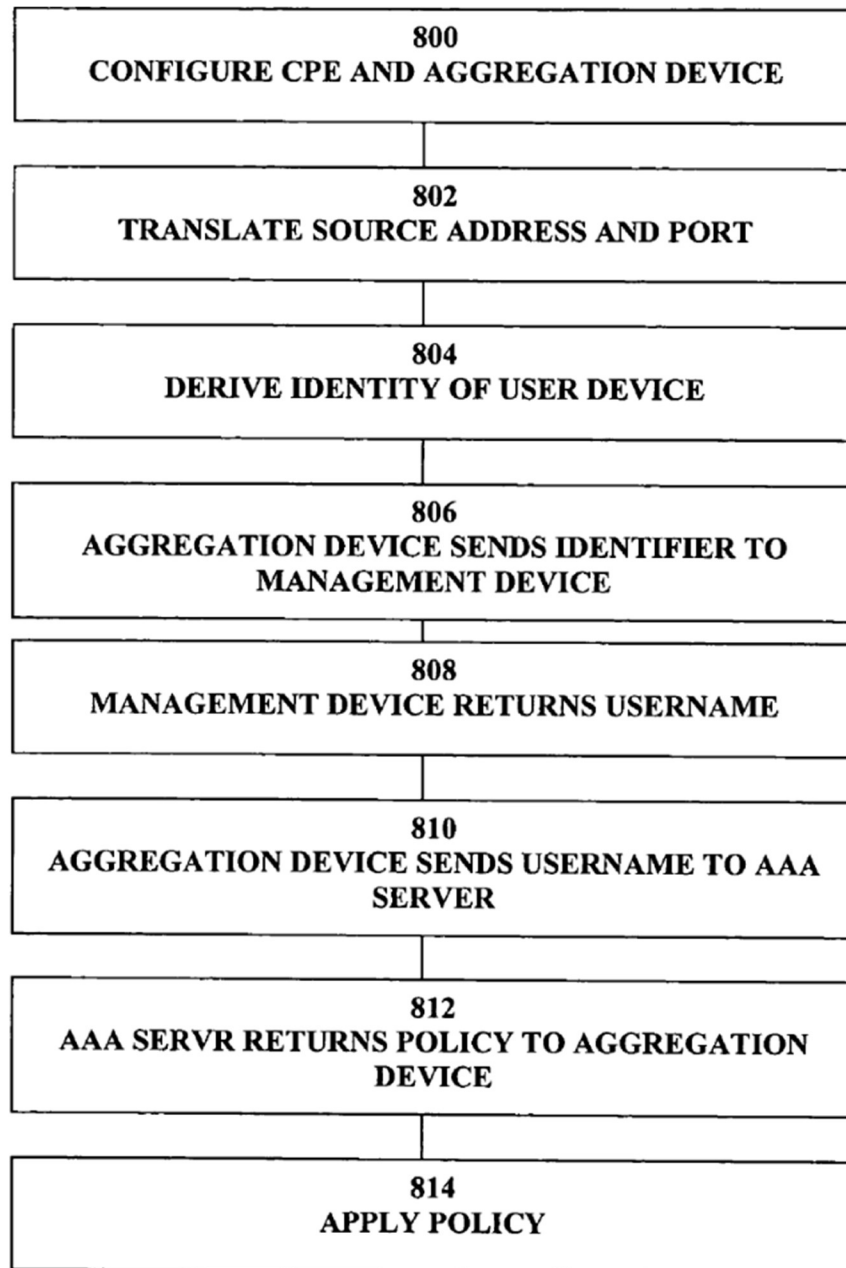


FIG. 8

Id., Fig. 8. In particular, “[a]t step **804** the aggregation device derives the data session [user] device information in the form of the original source or user device IP address or other identifier for example from the table at FIG. 7 based on the range

in which the received TCP port number falls and, in the event that the CPE may use multiple outside source addresses, the received [user] device identifier in combination.” *Id.*, 6:5-11.

- (d) 1[c]: routing the packet to the destination equipment based on said identifier.

204. In my opinion, King teaches limitation 1[c]: “routing the packet [*e.g.*, **returning traffic**] to the destination equipment [*e.g.*, **user device 100**] based on said identifier [*e.g.*, **IP address of user device 100**].” Figure 5 discloses the typical operations of a CPE that, as discussed above, “serves a plurality of user devices” and “acts as an ‘overloaded’ IP address serving multiple user devices.” EX1025, 2:49-61.

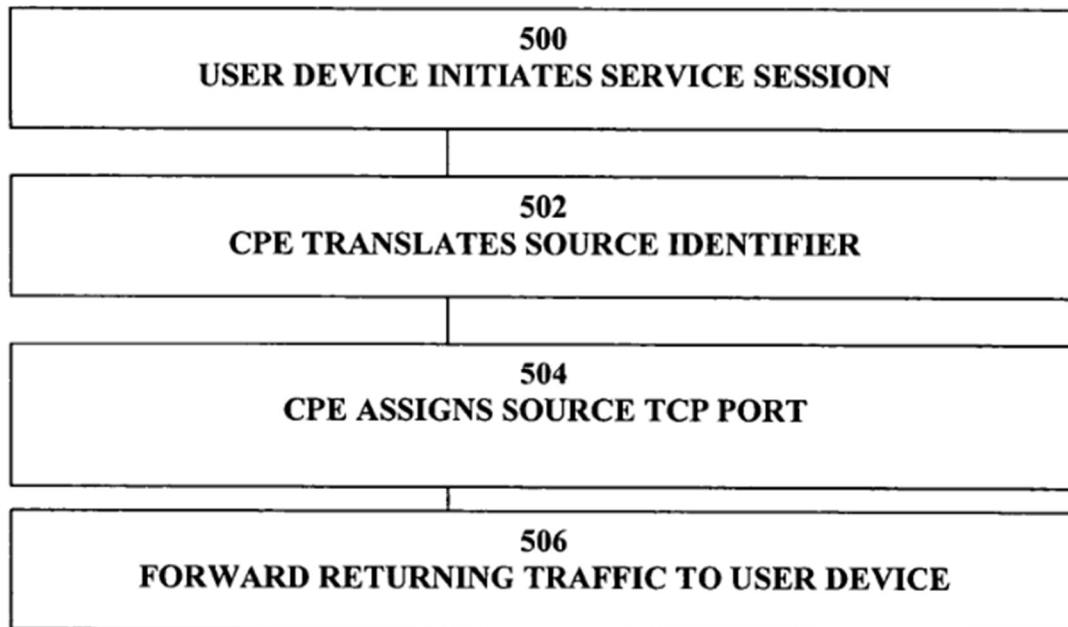


FIG. 5

Id., Fig. 5. At step **506**, the CPE “forwards returning traffic with the translated overloaded IP address and TCP port to the user device, reinstating the user device IP address as destination address and the user device assigned TCP port number.” *Id.*, 3:2-6. As discussed, the “user device IP address” corresponds to the identifier in the ’369 patent. *Id.*, 5:46-57, 6:5-11; *see supra* § VI.C.4.c.

5. Claim 2: The method according to claim 1 of routing an IP data packet, wherein said at least one identifier is a secondary destination address of the destination equipment.

205. In my opinion, King discloses the additional limitation of claim 2: “routing an IP data packet [*e.g.*, **returning traffic**], wherein said at least one identifier is a secondary destination address [*e.g.*, **IP address of user device 100**] of the destination equipment [*e.g.*, **user device 100**].” As the ’369 patent explains, a “secondary address” is merely the private IP address of the destination equipment. EX1001, 3:50-51. Similarly, as discussed above, King uses the private IP address of the user device, which it refers to as “IP1” or “IP2,” as the identifier. EX1025, 5:46-57, 6:5-11; *see supra* § VI.C.4.c.

6. Claim 3: The method according to claim 2 of routing an IP data packet, comprising, before the routing step, a step of transforming the packet by adding said secondary address to the packet, and routing the packet based on said secondary destination address.

206. In my opinion, King discloses the additional limitation of claim 3: “routing an IP data packet [*e.g.*, **returning traffic**], comprising, before the routing

step, a step of transforming the packet by adding said secondary address [e.g., **IP address of user device 100**] to the packet [e.g., **reinstating the user device IP address**], and routing the packet based on said secondary destination address.” For example, King teaches transforming the packet before routing it. In particular, King describes, upon receiving an incoming data packet, “reinstating the user device IP address as destination address and the user device assigned TCP port number” before “forward[ing] returning traffic ... to the user device.” EX1025, 3:2-6. Similarly, the ’369 patent explains that “the transformation step” can be “add[ing] the secondary address of the destination equipment to a field of the packet.” EX1001, 4:1-3. And as discussed above, King discloses routing the packet based on the secondary destination address. *See supra* § VI.C.4.

7. Claim 5

- (a) 5[pre]: A device for routing an IP data packet in a telecommunications network to a destination equipment, said packet comprising a primary destination address and a destination port number, wherein said device comprises, on reception of said packet:

207. To the extent it is limiting, in my opinion, King and Kumar render obvious limitation 5[pre]. As I discussed with respect to claim 1, King teaches devices—a CPE and an aggregation device—that perform the claimed steps. *See supra* § VI.C.4.a.

- (b) 5[a]: a processor that determines a port mask assigned to the destination equipment, the port mask defining a range

of port numbers to which the destination port number belongs;

208. In my opinion, King and Kumar render obvious limitation 5[a]. As I discussed with respect to claim 1, King teaches an aggregation device that performs the claimed steps. *See supra* § VI.C.4.b. A POSITA would know that an aggregation device uses a processor to operate. In particular, a POSITA would have known that routing devices, like the aggregation device, use processors to perform functions, like the steps claimed in this limitation. In fact, King discloses a “computer system **140** upon which the method may be implemented” that “includes a bus **142** or other communication mechanism for communicating information, and a processor **144** coupled with bus **142** for processing information.” EX1025, 7:30-51.

- (c) 5[b]: the processor selects an identifier of the destination equipment of the packet from a plurality of equipment identifiers associated with said primary destination address based on the port mask; and

209. In my opinion, King and Kumar render obvious limitation 5[b]. As I discussed with respect to claim 1, King teaches an aggregation device that performs the claimed steps. *See supra* § VI.C.4.c. A POSITA would have known that an aggregation device uses a processor to perform the claimed steps. *See supra* § VI.C.7.b.

- (d) 5[c]: a communication unit that routes the packet to the destination equipment based on said identifier.

210. In my opinion, King and Kumar render obvious limitation 5[c]. As discussed with respect to claim 1, King teaches a CPE that performs the claimed steps. *See supra* § VI.C.4.d. A POSITA would have known that the CPE uses a communication unit to route the packet. In fact, King explains that CPEs communicate with several devices in the network. EX1025, 1:22-33, 1:45-59, Figs. 1 & 5.

8. Claim 6

- (a) 6[pre]: Telecommunications network equipment adapted to receive an IP data packet comprising a primary destination address and a destination port number, comprising at least one routing device comprising:

211. As discussed in connection with Ground 3, Claim 1[pre], in my opinion King discloses telecommunications network equipment, such as CPE **108** and aggregation device **110**, that are adapted to receive and route an IP data packet comprising a primary destination address and a destination port number. *See supra* § VI.C.4.a.

- (b) 6[a]: a processor that determines a port mask assigned to a destination equipment, the port mask defining a range of port numbers to which the destination port number belongs;

212. As discussed in connection with Ground 3, Claim 5[a], in my opinion King and Kumar render obvious this limitation. *See supra* § VI.C.7.b.

- (c) 6[b]: the processor selects an identifier of the destination equipment of the packet from a plurality of equipment identifiers associated with said primary destination address based on the port mask; and

213. As discussed in connection with Ground 3, Claim 5[b], in my opinion King and Kumar render obvious this limitation. *See supra* § VI.C.7.c.

- (d) 6[c]: a communication unit that routes the packet to the destination equipment based on said identifier.

214. As discussed in connection with Ground 3, Claim 5[c], in my opinion King and Kumar render obvious this limitation. *See supra* § VI.C.7.d.

9. Claim 15: A non-transitory computer readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 1.

215. In my opinion, King and Kumar render obvious claim 1. *See supra* § VI.C.4. King also describes non-transitory computer readable mediums that execute instructions using a processor. EX1025, 12:4-9, 12:30-38. Thus, King and Kumar render obvious claim 15.

D. Ground 4: Claim 4 Is Obvious in View of Fangman, Kumar and RFC 791

1. RFC 791 (EX1026)

216. RFC 791 is the “Internet Protocol” specification. An RFC is a “Request For Comments” that are produced by the IETF to “describe the Internet's technical foundations, such as addressing, routing, and transport technologies.” *RFCs*, IETF, available at <https://www.ietf.org/standards/rfcs/> (last accessed Nov. 8, 2023). The

IETF is an “Internet Engineering Task Force” that was founded in 1986 to “make[] voluntary standards that are often adopted by Internet users, network operators, and equipment vendors.” *Introduction to the IETF*, IETF, available at <https://www.ietf.org/about/introduction/> (last accessed Nov. 8, 2023). The IETF has a “commitment to making [its] documents, [its] Working Group mailing lists, [its] attendance lists, and [its] meeting minutes publicly available on the Internet.” *Id.* The IETF makes its documents, like RFCs publicly available on its website. Indeed, “[w]hen they are published, RFCs are freely available online.” *RFCs*, IETF, available at <https://www.ietf.org/standards/rfcs/> (last accessed Nov. 8, 2023).

217. In my opinion, the IETF is a well-known, reputable organization and its website is routinely used and known by POSITAs. I often use the IETF website to review documents that the IETF publishes, including numerous RFCs, to stay up-to-date on developments in technical fields, like computer networking. Based on my personal experience, when documents, especially RFCs, that are published on the IETF website contain a date on the face of the publication, that is the date that the document was made publicly available.

218. As disclosed on the face of the document, RFC 791 was published in September 1981. EX1026, Cover Page. I personally accessed RFC 791 prior to the ’369 patent’s priority date of March 2008. Prior to the priority date of the patent, I accessed a public copy of RFC 791 online. I also read and reviewed a paper copy

of RFC 791 in the mid-1990s as well. After reviewing EX1026, I can confirm that the document attached to this petition as EX1026 is the same document that I had personally accessed and reviewed before the priority date of the patent. RFC 791 is a well-known RFC, as it describes the workings of the Internet that we use today. It is widely read and analyzed by POSITAs to understand how the Internet works, and I have reviewed it numerous times over the course of my own personal work. In particular, I can confirm that the disclosure of strict source routing is materially the same as I remember reading in the 1990s.

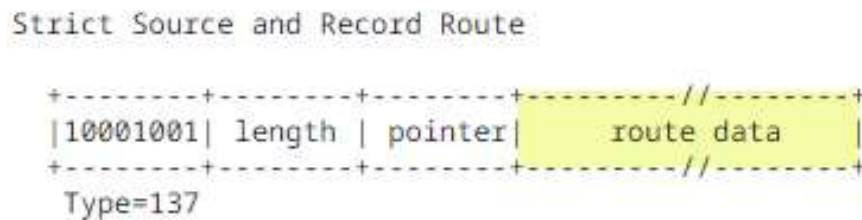
219. I have also downloaded a June 20, 2006 copy of RFC 791 (EX1029) from the Internet's Way Back Machine at the link <https://web.archive.org/web/20060720182319/http://www.ietf.org/rfc/rfc791.txt/>.

After reviewing EX1029, I can confirm that the document is the same as the RFC 791 document that I review before the priority date of the patent.

220. In fact, several U.S. patents that were filed and issued before the '369 patent's priority date discuss and cite to RFC 791. For example, U.S. Patent No. 5,014,221 ("Mogul"), filed on January 29, 1988 and published on May 7, 1991, says that "[t]he well known Internet Protocol (IP) will be described for use in the preferred embodiment" and then cites to RFC 791. EX1027, 3:50-61. Similarly, U.S. Patent No. 5,163,131 ("Row"), filed on September 8, 1989 and issued on November 10, 1992, explains that its Figure 1 depicts "[t]he internet protocol

standard” that “is specified in ... RFC 791.” EX1028, 6:5-23. It is therefore my opinion that RFC 791 was publicly accessible before the ’369 patent’s priority date, based on my personal experiences and based on citations in public documents that pre-date the ’369 patent.

221. RFC 791 discloses a “strict source routing” option (routing identifier) that specifies the routers that an IP packet should traverse on its way to the destination equipment in a “route data” (yellow) field:



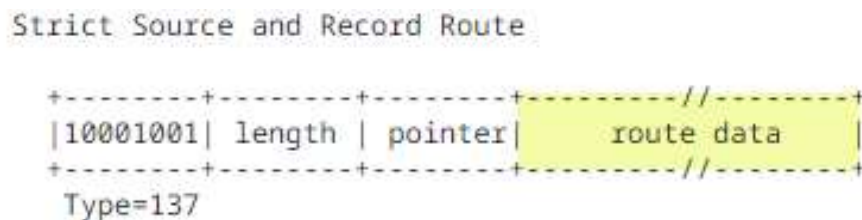
EX1026, 19-21 (colors added). The route data is composed of a “series of internet addresses” that specify the exact set of routers that a packet should traverse to reach its destination. *Id.*, 20; *see also* EX1031, 441-42 (“The Strict source routing option gives the complete path from the source to destination as a sequence of IP addresses.”).

2. **Claim 4: The routing method according to claim 1, wherein the at least one identifier is a route identifier specific to said destination equipment and the packet is routed based on said specific route identifier.**

222. As discussed above, in my opinion, Fangman and Kumar render obvious Claim 1 of the ’369 patent. *See supra* § VI.B.4. Claim 4 further recites “[t]he routing method according to claim 1, wherein the at least one identifier is a

route identifier specific to said destination equipment and the packet is routed based on said specific route identifier.” In my opinion, the additional limitation of claim 4 is obvious in view of Fangman and Kumar and the general knowledge of a POSITA, or in further view of RFC 791.

223. Fangman discloses that its system is an “IP-based data networks” and its devices operate in accordance with the “Internet Protocol.” EX1024, 1:14-15, 1:19-24, 6:22-25. In my opinion, a POSITA at the time would have been well-aware of the Internet Protocol and RFC 791, which is the “Internet Protocol” specification. This includes the “strict source routing” option disclosed in the Internet Protocol specification, which specifies the routers that an IP packet should traverse on its way to the destination equipment in a “route data” (yellow) field:



Id., 19-21 (colors added). Thus, in view of the general knowledge of a POSITA and RFC 791, in my view, it would have been obvious for Fangman’s service gateway 170 to implement the strict source routing option. In the combined system, the service gateway would select the route data to route the IP packet to a piece of destination equipment (e.g., host 102a) when performing NAPPT. In my opinion,

the route data is “a route identifier specific to said destination equipment” because it specifies the exact path the packet should take to reach the destination equipment.

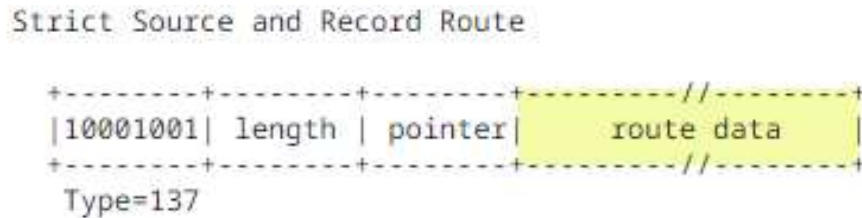
224. A POSITA would have been motivated to use strict source routing with the service gateway 170 of Fangman. EX1030, 1 (“There are probably many situations in which a source routing capability would be useful. Some possible uses are...”). Because strict source routing allows the service gateway 170 to specify the exact route to a host 102, the path can be optimized for reliability and bandwidth, for instance by routing packets around known bottlenecks or points of congestion. EX1030, 2 (one benefit of source routing is “restricting the route the a datagram may take” to avoid “some ‘trouble spot’”). In my opinion, a POSITA would have been particularly motivated to use source routing in Fangman because Fangman’s network is intended for IP telephony, and selecting a path that optimizes reliability and bandwidth would improve the quality of Fangman’s voice calls.

E. Ground 5: Claim 4 Is Obvious in View of King, Kumar and RFC 791

- 1. Claim 4: The routing method according to claim 1, wherein the at least one identifier is a route identifier specific to said destination equipment and the packet is routed based on said specific route identifier.**

225. King discloses an IP network with devices that operate in accordance with the “Internet Protocol.” EX1025, 1:21-33, claim 6. In my opinion, a POSITA would have thus understood King to disclose or render obvious that its network

devices may operate in accordance with RFC 791, which is the “Internet Protocol” specification. EX1026 (RFC 791). RFC 791 discloses a “strict source routing” option (routing identifier) that specifies the routers that an IP packet should traverse on its way to the destination equipment in a “route data” (yellow) field:



Id., 19-21 (colors added); *see also* EX1031, 441-42 (“The *Strict source routing* option gives the complete path from the source to destination as a sequence of IP addresses.”). Thus, in my opinion, it was obvious in view of the general knowledge of a POSITA to implement the strict source routing option such that the IP packet is routed to the terminal equipment based on the route (“a route identifier specific to said destination equipment”).

226. In my opinion, a POSITA would have been motivated to use strict source routing. EX1030, 1 (“There are probably many situations in which a source routing capability would be useful. Some possible uses are...”). For instance, in my view, a POSITA would have understood that specifying the exact path to a piece of terminal equipment would allow the network to be optimized for reliability and bandwidth. EX1030, 2 (one benefit of source routing is “restricting the route the a datagram may take” to avoid “some ‘trouble spot’”).

VII. CONCLUSION

227. For the reasons stated above, it is my opinion that the Challenged Claims would have been obvious at the time of the invention.

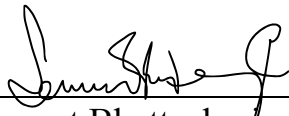
228. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

* * *

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. I further declare that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001.

Respectfully submitted,

Date: November 9, 2023



Samrat Bhattacharjee, Ph.D