

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

<i>In re</i> patent of: Mohamed BOUCADAIR	§	Attorney Docket: T4172-00012
	§	
U.S. Patent: 8,693,369	§	Customer No.: 39290
	§	
Issue Date: 2014-04-08	§	
	§	
Filing Date: 2010-09-28	§	
	§	Real Party in Interest:
For: METHOD OF ROUTING A DATA	§	
PACKET IN A NETWORK AND	§	Unified Patents, LLC
AN ASSOCIATED DEVICE	§	

**REQUEST FOR *EX PARTE* REEXAMINATION OF
U.S. PATENT 8,693,369**

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

Dear Commissioner:

Pursuant to 35 U.S.C. §§ 301-307, Unified Patents, LLC (“Requester”) hereby requests an *ex parte* reexamination of Claims 1-3 and 5-17 of U.S. Patent No. 8,693,369 (the “’369 Patent” (EX-1001)). The ’369 Patent issued April 8, 2014, from U.S. Patent Application No. 12/935,040, filed September 28, 2010,

which is a national stage entry of PCT/FR09/50548 filed March 31, 2009.¹ The named inventor is Mohamed Boucadir.

This Request presents prior art references and analyses that were not considered by the Examiner during the original prosecution of the '369 Patent, and demonstrates that Claims 1-3 and 5-17 (the "Challenged Claims") are not patentable over these references. Requester therefore requests that an order for reexamination and an Office Action rejecting the Challenged Claims be issued.

¹ Because the effective filing date is before March 16, 2013, the '369 Patent is subject to the pre-AIA provisions of 35 U.S.C. et seq.

Ex Parte Patent Reexamination Filing Requirements

Pursuant to 37 C.F.R. § 1.510(b)(1), statements pointing out at least one substantial new question of patentability based on material, non-cumulative references for Claims 1-3 and 5-17 of the '369 Patent are provided in Section III of this Request.

Pursuant to 37 C.F.R. § 1.510(b)(2), reexamination of Claims 1-3 and 5-17 is requested, and a detailed explanation of the pertinence and manner of applying the cited references to Claims 1-3 and 5-17 is provided in Section IV of this Request. The material and analysis in this Request is fully supported by the expert testimony of Thomas La Porta Ph.D. (EX-1003). Additionally, the charts at Exhibits AA and BB comparing the Challenged Claims to the cited references provide further support for the issues analyzed in this Request, including more fulsome reproductions of the cited portions of the references relied upon herein.

Pursuant to 37 C.F.R. § 1.510(b)(3), copies of every patent or printed publication relied upon or referred to in the statement pointing out each substantial new question of patentability, or in the detailed explanation of the pertinence and manner of applying the cited references, are provided as Exhibits 1001-1007 of this Request.

Pursuant to 37 C.F.R. § 1.510(b)(4), a copy of the '369 Patent is provided as EX-1001 of this Request, along with a copy of any disclaimer, certificate of correction, and reexamination certificate issued corresponding to the patent.

Pursuant to 37 C.F.R. § 1.510(b)(5), the attached Certificate of Service indicates that a copy of this Request, in its entirety, has been served on the Patent Owner at its correspondence address of record in the patent file of the '369 Patent, in accordance with 37 C.F.R. § 1.33(a) and (c):

NOBLITT & NEWSON, PLLC (Acacia)
Daniel J. Noblitt
8777 NORTH GAINES CENTER DRIVE, STE. 175
Scottsdale, AZ 85258
UNITED STATES

Also submitted herewith is the fee set forth in 37 C.F.R. § 1.20(c)(2).

Pursuant to 37 C.F.R. § 1.510(b)(6), Requester hereby certifies that the statutory estoppel provisions of 35 U.S.C. § 315(e)(1) and 35 U.S.C. § 325(e)(1) do not prohibit Requester from filing this *ex parte* patent reexamination request.

TABLE OF CONTENTS

	Page
I. SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY	1
II. OVERVIEW	1
A. Summary of the '369 Patent	1
1. Purported Problem/Solution	2
2. Disclosed Method of Routing IP Packets	5
3. Disclosed Method of Configuring the Routing Device and Terminal Equipment	13
B. Prosecution History	19
C. Claim Construction	21
D. Priority Date of the Challenged Claims	22
E. Person of Ordinary Skill in the Art	22
F. State of the Art	23
1. Conserving Public Addresses	23
2. Dynamic Host Configuration Protocol	25
III. SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY	28
A. Prior Art	29
1. <i>Biswas</i> (EX-1004)	29
2. <i>Fangman</i> (EX-1005)	30
B. Ground 1: Anticipation and/or obviousness over <i>Biswas</i> Presents Substantial New Questions of Patentability (Claims 1- 3, 5-17)	30
1. The <i>Biswas</i> Reference	30

C.	Ground 2: Anticipation and/or obviousness over <i>Fangman</i> Presents Substantial New Questions of Patentability (Claims 1- 3, 5-8, 10, 11, 13-17).....	35
1.	The <i>Fangman</i> Reference.....	35
IV.	IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE	40
A.	Proposed Rejections	40
B.	Proposed Rejection 1: Claims 1-3 and 5-17 are anticipated by or obvious over <i>Biswas</i>	40
C.	Proposed Rejection 2: Claims 1-3, 5-8, 10, 11, and 13-17 are anticipated by or obvious over <i>Fangman</i>	54
D.	Secondary Considerations	73
V.	DISCLOSURE OF CONCURRENT LITIGATION AND ADMINISTRATIVE PROCEEDINGS.....	74
VI.	CONCLUSION	74

Requester's Exhibit List

<i>Exhibit #</i>	<i>Description</i>
1001	U.S. Patent 8,693,369 (the “’369 Patent”)
1002	Prosecution history of the ’369 Patent (“File History”)
1003	Declaration of Requester’s Expert, Thomas La Porta Ph.D.
1004	U.S. Patent 7,624,195 (“ <i>Biswas</i> ”)
1005	U.S. Patent 8,363,647 (“ <i>Fangman</i> ”)
1006	Z. Zhen et al., <i>Saving Public Addresses in Mobile IP</i> , International Conference on Networking, International Conference on Mobile Communications and Technologies in 2006, (“Zhen”)
1007	Dynamic Host Configuration Protocol, IETF Request for Comments 2131, March 1997.
AA	Claim Charts - Claims anticipated/obvious over <i>Biswas</i>
BB	Claim Charts - Claims anticipated/obvious over <i>Fangman</i>

I. SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

Prior to describing the substantial new questions of patentability presented in this Request, provided below is an overview of the '369 Patent, its prosecution history, a discussion of claim construction, a summary of the prior art used in the present Request, and a summary of the state of technology relevant to the '369 Patent.

II. OVERVIEW

The Challenged Claims are unpatentable as anticipated or obvious over the prior art. The claims are directed to IP telecommunications networks in which packets of data are transported from source equipment to destination equipment identified by a destination address, all of which was well known in the art. EX-1003 ¶ 38. At least the prior art references *Biswas* (EX-1004) and *Fangman* (EX-1005), as discussed in detail below, anticipate or render obvious each of the Challenged Claims.

A. Summary of the '369 Patent

The '369 Patent is titled “Method of Routing a Data Packet in a Network and an Associated Device” and is generally directed to “IP telecommunications networks in which packets of data are transported from source equipment to destination equipment identified by a destination address.” '369 Patent 1:15-18. More specifically, the '369 Patent states that “[t]he invention relates to a

mechanism for allocating addresses and port numbers enabling the same primary address to be assigned to a plurality of pieces of terminal equipment of the telecommunications network,” and that “the invention applies to any type of public or private addressing, but it applies especially to public IP addresses defined by Internet Protocol version 4 (IPv4).” ’369 Patent 1:37-43.

The ’369 Patent includes seventeen claims with Claims 1, 5, 6, 7, 10, and 14 being independent claims.

1. Purported Problem/Solution

The ’369 Patent identifies that “[i]t is commonly accepted in the IP service provider community that exhaustion of public IPv4 addresses is inevitable” and describes the dual NAT (Network Address Translation) or Operator NAT solution that has been implemented. ’369 Patent 1:65-2:1. FIG. 1 diagrammatically shows a telecommunications network implementing the prior art Operator NAT function:

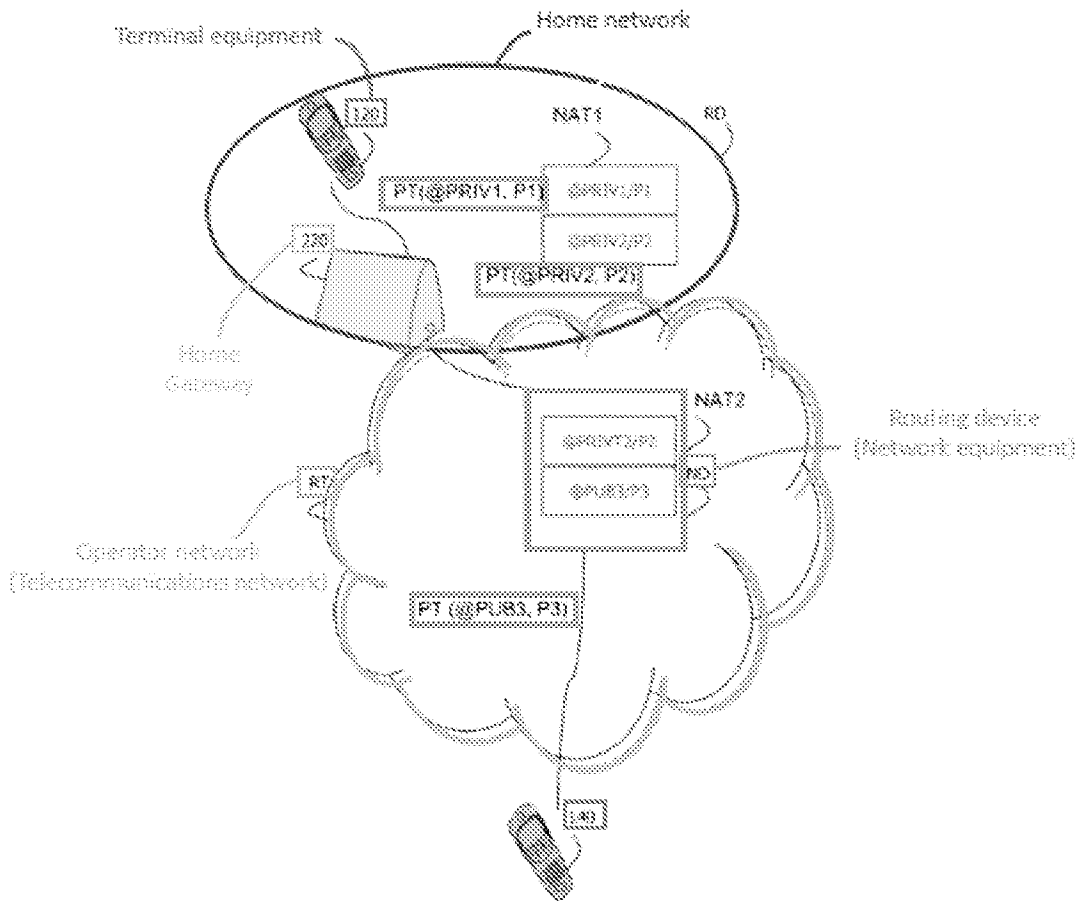


FIG. 1

Terminal equipment (TE) 120 (red) in a home network RD (purple) is connected to home gateway 220 (orange) between TE 120 and telecommunications network RT (green). Home gateway 220 implements a first NAT function NAT1 (gold) that translates a first private address pair (@PRIV1, P1) of data packet PT sent by TE120 into a second private address pair (@PRIV2, P2). Home gateway 220 then sends the translated packet PT in the network RT where it is received by network equipment NO (blue). Network equipment NO executes Operator NAT function NAT2 (gold) that translates second private

address pair (@PRIV2, P2) into third public address pair (@PUB3, P3), thus translating private addresses of home gateways to public addresses. '369 Patent 2:4-18.

The '369 Patent identifies several drawbacks to the prior art Operator NAT solution, including the added complexity of second level translation and the need to adapt application or application level gateway signaling protocols. '369 Patent 2:19-41. The '369 Patent purports to alleviate these drawbacks by providing a new solution to economizing the use of public IP addresses:

The invention addresses this need by way of a method of routing a data packet in a telecommunications network, said packet including a primary destination address and a destination port number, said method including, on reception of said packet, the following steps:

- determining a port mask defining a range of port numbers to which the destination port number belongs;
- selecting a routing identifier of a destination piece of equipment of the packet from a plurality of terminal equipment routing identifiers associated with said destination address on the basis of the determined port mask; and
- routing the packet to the destination equipment on the basis of said identifier.

* * *

Thus the invention is based on an entirely novel and inventive approach to routing a data packet that relies on a unique combination consisting of the destination address of the packet, the port mask defining a range of port numbers that includes the destination port number of the received packet and a routing identifier of the

destination terminal equipment. The invention thus makes it possible to assign the same routable primary address in the telecommunications network to a plurality of pieces of terminal equipment connected to that network and thus to economize on the use of public IP addresses without having recourse to the Operator NAT solution.

'369 Patent 2:51-64, 3:11-23.

2. Disclosed Method of Routing IP Packets

The '369 Patent states that “[t]he general principle of the invention relies on assigning the same primary address to a plurality of pieces of terminal equipment in a telecommunications network, these pieces of terminal equipment being uniquely identified by a routing identifier and a port mask defining a range of port numbers that is dedicated to them.” '369 Patent 7:12-18. A telecommunications network RT of an operator on which a service provider has deployed an IP connectivity or access service architecture is described with reference to FIG. 3 which diagrammatically shows a plurality of pieces of terminal equipment connected to a telecommunications network of an operator:

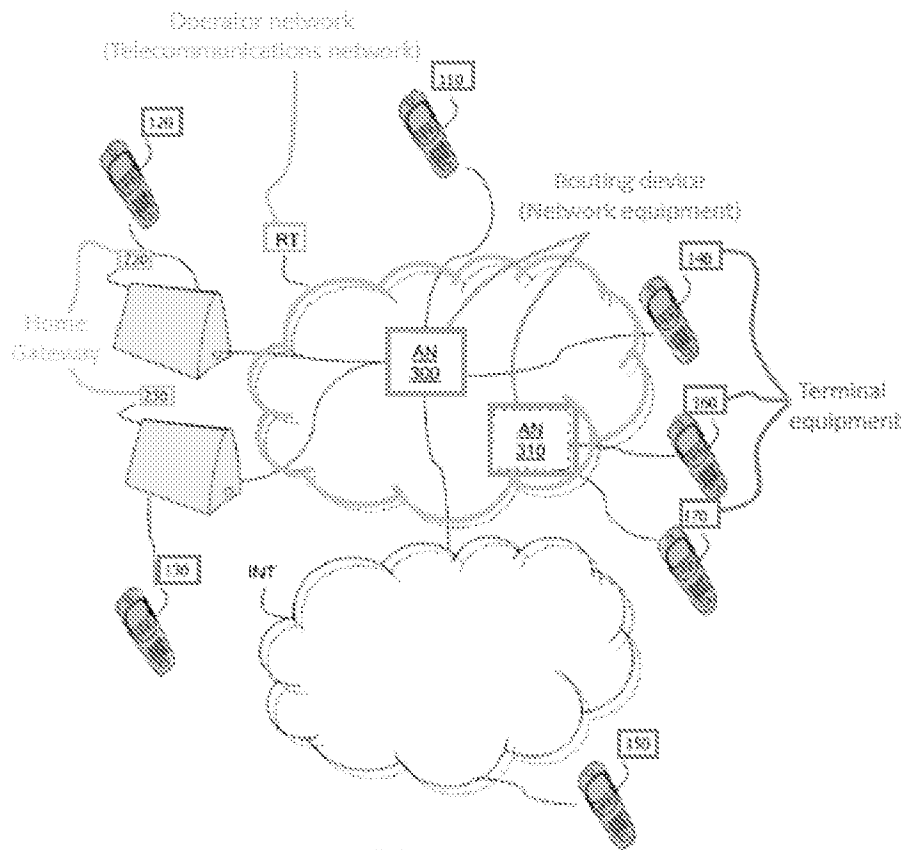


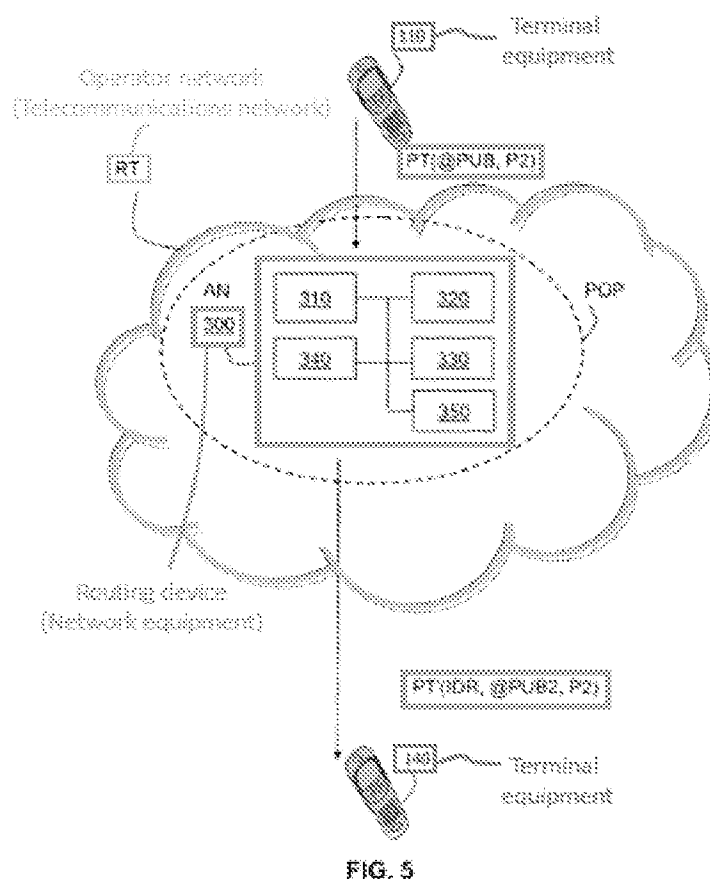
FIG. 3

A plurality of pieces of terminal equipment (TE)(red) have access to network RT (green). The pieces of terminal equipment 110, 120, 130, 140, 160, and 170 (e.g., telephones or PCs) are connected directly to the network RT (TE 110, 140, 160, 170) or to a home gateway 220, 230 (orange) between a home network and the network RT (TE 120, 130). '369 Patent 8:1-11.

The home gateway 220, 230 includes a translation table or NAT table that correlates a private address and a first port number of a piece of terminal equipment of its private network (TE 120 or TE 130 respectively) to at least the

public address of the home gateway and a second port number. '369 Patent 8:12-15.

The telecommunications network RT includes at least one routing device AN 300, 310 (blue) that implements the data packet routing method. '369 Patent 8:16-20. With reference to FIG. 5, the '369 Patent explains that the routing device AN 300 includes elements found in a conventional computer, namely, a processor 310, a random-access memory 320, a read-only memory 330, and telecommunications means for communicating with the network. '369 Patent 8:37-42.



The routing device AN 300 includes memory 350 containing a database in which it stores the association between the public address @PUB, the port mask MP uniquely assigned to each piece of terminal equipment, and the routing identified IDR unique to each piece of terminal equipment. '369 Patent 8:44-48.

The primary address that may be shared by a plurality of pieces of terminal equipment is a public address @PUB and is announced by the routing device AN 300 by conventional protocols. '369 Patent 9:1-8.

In one embodiment, the IDR is a private address, also known as a secondary address, of the piece of terminal equipment, and such address is not announced by the routing device. '369 Patent 9:9-17.

In a second embodiment, the IDR is a route identifier that uniquely designates a route that serves a piece of terminal equipment. '369 Patent 9:18-23.

The '369 Patent explains that the main function of the routing device AN 300 according to the invention is maintaining a table of the correspondence between the routing identifier IDR and the pair (public IP address @PUB and port mask MP) “so as to be able to determine unambiguously which piece of terminal equipment the data packet containing the destination address @PUB shared by a plurality of pieces of terminal equipment must be transmitted.” '369 Patent 8:57-63.

The read-only memory 330 of the routing device AN 300 stores a computer program including instructions for executing the steps of the routing method described with reference to FIG. 4:

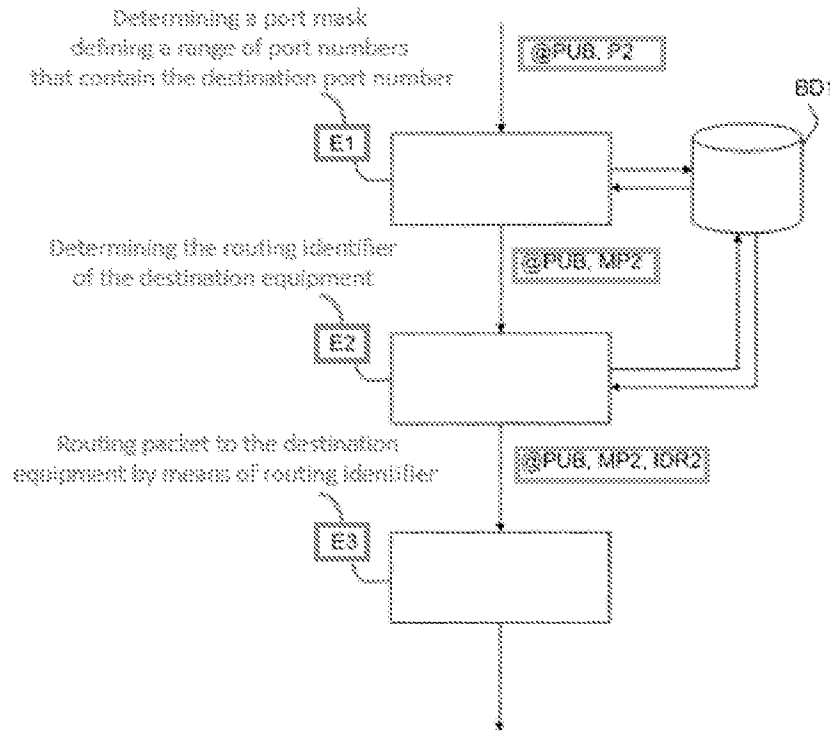


FIG. 4

According to the routing method, upon receipt of a data packet PT containing a destination public address @PUB and a destination port number P2, routing device AN 300 executes step E1 of determining a port mask defining a range of port numbers that contains the destination port number P2. The port mask assigned to each piece of terminal equipment may be stored in database BD1. '369 Patent 8:22-28.

In step E2, the port mask MP is used to determine the routing identifier IDR of the destination equipment of the packet PT from among the plurality of pieces

of terminal equipment having the same public address @PUB. '369 Patent 8:28-32.

In step E3, the packet is routed to the destination equipment by means of its routing identifier IDR. If the routing device AN 300 has no entry in its routing tables corresponding to the destination port number, the packet is eliminated. '369 Patent 8:32-36.

The '369 Patent discloses that the packet PT may be transformed in various ways. In one embodiment, the packet is encapsulated in a packet PT' containing the secondary address @PRIV2 of the destination terminal equipment 120 as the destination address. '369 Patent 12:58-62.

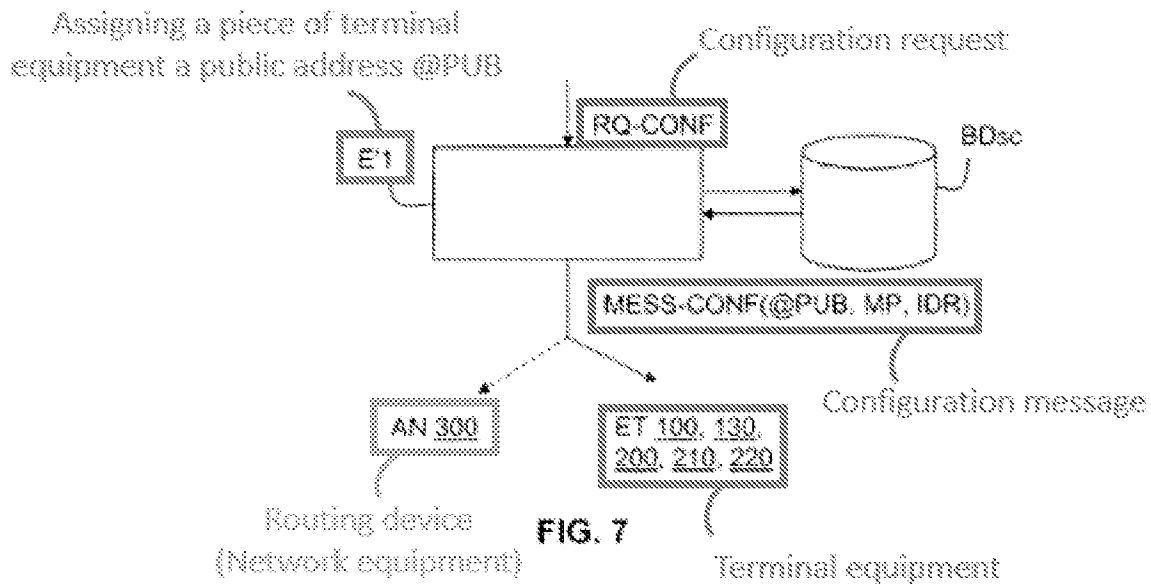
Independent Claims 1, 5, and 6 are directed to routing an IP data packet in a telecommunications network to a destination equipment according the method described above. Claim 1 is directed to the method, Claim 5 is directed to a processor performing the method, and Claim 6 is directed to network equipment comprising the processor. A side-by-side comparison of the claims is provided below:

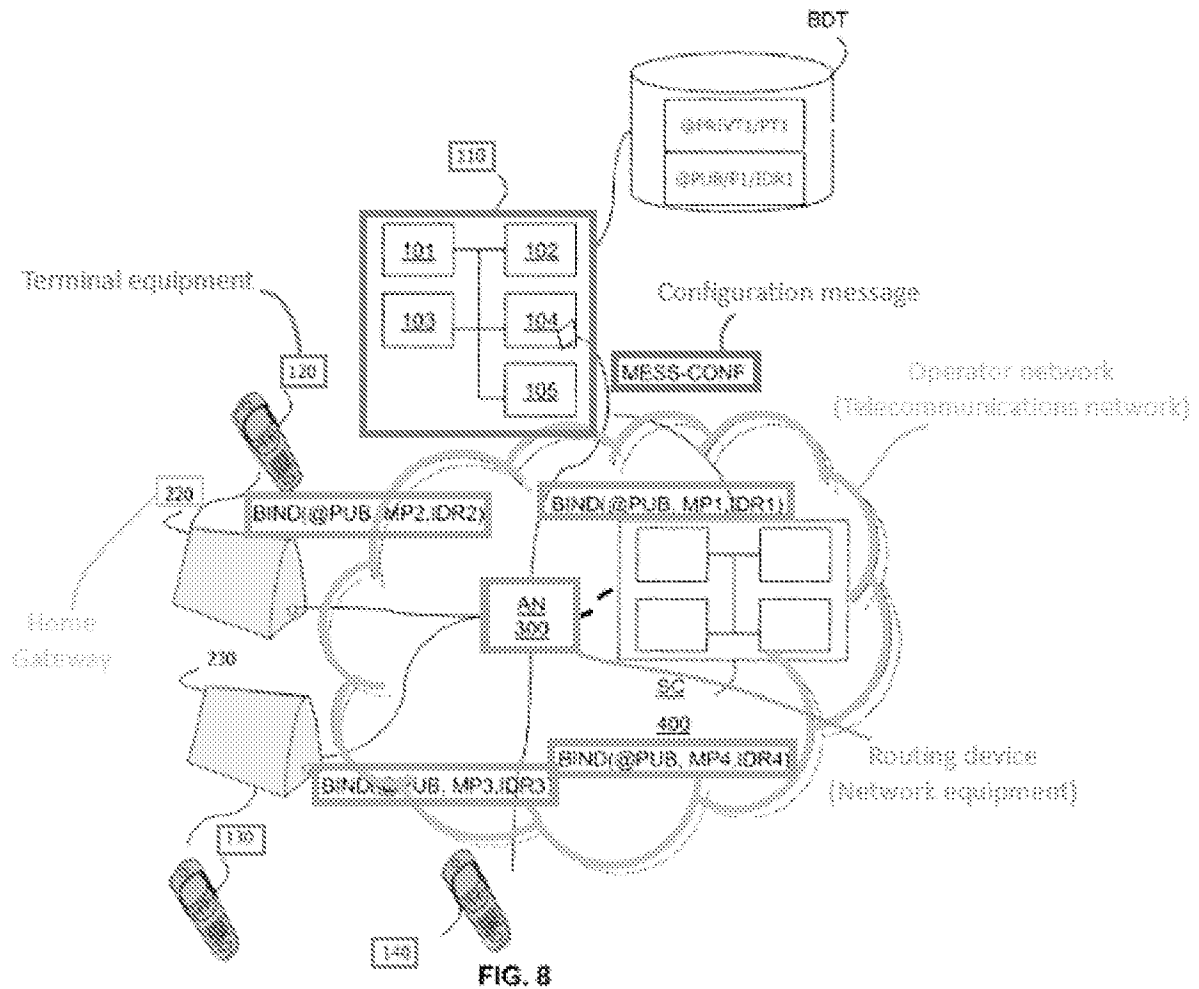
Claim 1	Claim 5	Claim 6
1. A method of routing an IP data packet in a telecommunications network to a destination equipment,	5. A device for routing an IP data packet in a telecommunications network to a destination equipment,	6. Telecommunications network equipment

said packet comprising a primary destination address and a destination port number,	said packet comprising a primary destination address and a destination port number,	adapted to receive an IP data packet comprising a primary destination address and a destination port number,
said method comprising, on reception of said packet, the following steps:	wherein said device comprises, on reception of said packet:	comprising at least one routing device comprising:
[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;	[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;	[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;
[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	[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	[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
[1.c] routing the packet to the destination equipment based on said identifier.	[5.c] a communication unit that routes the packet to the destination equipment based on said identifier.	[6.c] a communication unit that routes the packet to the destination equipment based on said identifier.

3. Disclosed Method of Configuring the Routing Device and Terminal Equipment

The '369 Patent discloses methods and apparatus for configuring the routing device AN and the pieces of terminal equipment. The method of configuring a piece of terminal equipment is described with reference to FIGs. 7 and 8:





When a piece of terminal equipment (100, 130, 200, 210, 220) connects to the network RT of an operator (for example, upon powering up), the terminal equipment sends a configuration request RQ-CONF to the IP connectivity service of the service provider according to known protocols. '369 Patent 9:35-42. The DHCP is specifically identified as an example: "It [RQ-CONF] may be, for example, a DHCP request DHCP_DISCOVER() broadcast to the telecommunications network of the IP service provider." '369 Patent 9:45-47.

The configuration request RQ-CONF is received by a configuration server SC 400 that responds at step [E'1] by assigning to the piece of terminal equipment a public address @PUB that is shared with a plurality of pieces of terminal equipment. '369 Patent 9:55-58. At step [E'2] (not shown), the configuration server SC also responds to the configuration request RQ-CONF by assigning to the piece of terminal equipment a port mask MP defining a range of port numbers dedicated to the piece of terminal equipment and a routing identifier IDR. '369 Patent 9:58-60. The configuration data including the public address @PUB, the routing identifier IDR, and the port mask MP, are sent to the piece of terminal equipment in a configuration message MESS-CONF. '369 Patent 9:60-63. The '369 Patent specifically identifies DHCP as an example: "If configuration is effected by a DHCP server, the configuration message is a DHCP_OFFER() type offer that contains the IP configuration data relating to the configuration of the terminal equipment that requested it." '369 Patent 10:4-7.

The configuration server includes a memory containing a database in which it stores the configuration data for each piece of terminal equipment that it manages, namely the public address @PUB, the port mask MP, and the routing identifier. '369 Patent 10:65-11:2.

In one embodiment, the configuration server SC designates an attachment routing device AN 300 for the piece of terminal equipment and sends the

configuration message MESS-CONF to the routing device AN 300. '369 Patent 9:64-10:3.

Independent Claims 7 and 10 are directed to configuring a piece of terminal equipment connected to a telecommunications network described above wherein the configuration server receives the configuration request RQ-CONF, assigns the configuration data, and sends the configuration message MESS-CONF to the piece of terminal equipment. Claim 7 is directed to the method and Claim 10 is directed to the configuration server. A side-by-side comparison of Claims 7 and 10 is provided below:

Claim 7	Claim 10
7. 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:	10. A configuration server in a telecommunications network, wherein, on reception of a configuration request sent by a piece of terminal equipment, comprising:
[7.a] assigning to said piece of terminal equipment a primary address shared with a plurality of pieces of terminal equipment;	[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;
[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	[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
[7.c] sending to said piece of terminal equipment a configuration message comprising said primary address, said port mask, and said routing identifier.	[10.c] a communication unit that sends to said piece of terminal equipment a configuration message comprising said

The flowchart illustrates the message processing method in a network equipment. It begins with a 'Configuration message' (MESS-CONF[@PUB, MP, IDR2]) being received by a central processing block. This block is connected to a 'BDT' (Base Data Table) and a 'Routing device (Network equipment)'. The central block also receives input from 'Terminal equipment selects port number'. The flow proceeds through several steps: E*1 (receiving the configuration message), E*2 (routing the message to the routing device), E*3 (receiving the message from the routing device), and E*4 (receiving the message from the routing device). The message is then processed by a block that outputs 'PT(@PRIV, P1)' and 'PT(@PUB, P2)'. The flow then reaches a decision point (E*5) which can either reject the message ('REJ') or accept it ('ACC').

FIG. 9

17

terminal equipment selects (at step E'3) a port number (for example, P2) from the range of port numbers defined by the port mask MP assigned to it, and assigns to the data packet PT a source port corresponding to port P2. 369 Patent 11:14-18.

Independent Claims 11 and 14 are directed to terminal equipment connected to a telecommunications network receiving a configuration message as described above. Claim 11 is directed to the method and Claim 14 is directed to the piece of terminal equipment. A side-by-side comparison of Claims 11 and 14 is provide below:

Claim 11	Claim 14
11. A method of configuring a piece of terminal equipment connected to a telecommunications network	14. 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, a port mask defining range of port numbers that is dedicated thereto, and a routing identifier,	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,
said method comprises the following steps:	the piece of client terminal equipment comprising:
[11.a] storing said configuration data; and before sending a data packet into the telecommunications network,	[14.a] a memory that stores said configuration data;
[11.b] selecting a port number in the range of port numbers defined by the port mask,	[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,

[11.c] 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.	[14.c] 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.
--	---

B. Prosecution History

The Challenged Claims were allowed following several rejections with the Examiner stating as the basis for allowance of independent Claims 1, 5, and 6:

Allowable Subject Matter

10. Independent Claims 1, 5 and 6 are allowable.

The following is a statement of reasons for the indication of allowable subject matter: The following limitation from Claims 1, 5 and 6 is allowable, as the prior art does not teach or suggest:

“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;

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;”

Claims 2-4 depend on Claim 1, thus they are allowable for the same reason.

EX-1002 72-73 (Office Action May 20, 2013)

During prosecution, Applicant overcame a rejection based on cited references *Baum* (US2011/0067119) and *Patek* (US2003/0088694) by arguing that the '369 Patent uses the plain and ordinary meaning of the terms “port” and “port number” as follows:

¹ The present application uses the ordinary and customary meanings of “port” and “port number.” Application, p. 13, ln. 1–p. 14, ln. 11. For a description of “port” and “port number” as well known by one of ordinary skill in the art, see [http://en.sakmedia.org/wiki/Port_\(computer_networking\)](http://en.sakmedia.org/wiki/Port_(computer_networking)):

In computer networking a **port** is an application-specific or process-specific software construct serving as a communications endpoint in a computer's host operating system. A port is associated with an IP address of the host, as well as the type of protocol used for communication. In plain English, the purpose of ports is to uniquely identify different applications or processes running on a single computer and thereby enable them to share a single physical connection to a packet-switched network like the Internet.

The protocols that primarily use ports are the Transport Layer protocols, such as the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) of the Internet Protocol Suite. **A port is identified for each address and protocol by a 16-bit number, commonly known as the port number.** The port number, added to a computer's IP address, completes the destination address for a communications session. That is, data packets are routed across the network to a specific destination IP address, and then, upon reaching the destination computer, are further routed to the specific process bound to the destination port number.

EX-1002 133-34 fn 1 (Amendment Nov. 28, 2012)

Applicant then argued that neither *Baum* nor *Patek* disclosed the “destination port number” and “port mask” recited in the claims:

First, the Ethernet frame disclosed in *Baum*, which has an IP destination address, cannot be equated to a “data packet comprising . . . a destination port number” as required by claim 1 (emphasis added). *Baum* discloses edge routers that interface between the Ethernet LANs and the IP network, and “the edge routers . . . include routines for responding to requests to identify a router port corresponding to an IP or MAC address supplied as part of a port information request.” *Baum*, ¶ [0082] (emphasis added). In *Baum*, when an edge router receives an Ethernet frame including an IP destination address, the edge router determines, within the Ethernet LAN, which MAC address is uniquely associated with this IP destination address. *Baum*, ¶¶ [0034]–[0035]. The edge router then forwards the Ethernet frame to a terminal having this MAC address via the router's output port to which this terminal is connected. *Baum*, ¶ [0091].

As it is well known in the art, an IP or MAC address is distinct from a port number.¹ Thus, the IP destination address in *Baum* is not interchangeable with the “port number” recited

in amended claim 1. Furthermore, while the “ports” discussed in Baum are interfaces of a router, the “ports” disclosed in the present application are interfaces of a destination or terminal equipment. Accordingly, Baum does not disclose, teach, or suggest a “said packet including a primary destination address and a destination port number” or “defining a range of port numbers to which the destination port number belongs” as required by amended claim 1 (emphasis added).

Second, Patek fails to disclose, teach, or suggest “determining a port mask to be assigned to the destination terminal” as recited in amended claim 1. Patek discloses a router for scheduling multicast frames in a switching network. When the router receives an incoming frame including a destination ID associated with a set of multicast destination terminals, the router forwards a copy of this frame to the output ports of the router. Patek, ¶¶ [0006] & [0030]. The “output port mask” in Patek refers to the selection of the router output ports associated with a given destination ID. Patek, ¶ [0006]. Patek’s “output port mask” is thus distinct from the “port mask to be assigned to the destination terminal” recited in amended claim 1. Similar to Baum, while the “output ports” discussed in Patek are interfaces of a router, the “ports” disclosed in the present application are interfaces of a destination or terminal equipment. Accordingly, Patek’s “output port mask” cannot be interpreted as the “port mask” recited in amended claim 1.

EX-1002 133-34.

Thus, to the extent that the scope of the terms “port” or “port number” could encompass a router port corresponding to an IP or MAC address, Applicant has disclaimed such scope. Moreover, prior art disclosing a “port” or “port number” as construed by Patent Owner was not relied upon by the Office during prosecution of the Challenged Claims.

C. Claim Construction

The claims must be given their “broadest reasonable interpretation consistent with the specification.” *See* MPEP § 2258; *In re Yamamoto*, 740 F.2d 1569, 222

USPQ 934 (Fed. Cir. 1984). This Request presents its claim analysis in a manner that is consistent with the broadest reasonable interpretation consistent with the specification.

Requester proposes that each claim term in the Challenged Claims be given its plain and ordinary meaning in this proceeding, and that no specific construction of any claim term is required because the prior art relied on in this Request meets each of the claim terms under any reasonable construction.

D. Priority Date of the Challenged Claims

The application that issued as the '369 Patent claims priority to International Patent Application number PCT/FR2009/050548, filed on March 31, 2009, which claims the benefit of French Application number 08 52108 filed March 31, 2008. Requester does not concede that the '369 Patent is entitled to the March 31, 2008, earliest possible priority date. Nonetheless, because all of the prior art relied on herein antedates Mar. 31, 2008, a priority analysis is not necessary to find the Challenged Claims unpatentable.

E. Person of Ordinary Skill in the Art

At the time of the purported invention of the '369 Patent, a POSA would have been familiar with telecommunications networks in which packets of data are transported from source equipment to destination equipment identified by a destination address. EX-1003 ¶ 69. A POSA would have had a working

knowledge of IP packet routing, Network address translation, IP networking technologies (e.g., NAT, DHCP), and network management. EX-1003 ¶ 69. A POSA would have gained knowledge of these concepts through a mixture of training and work experience, such as by having a Bachelor's degree in computer science, computer communications, electrical engineering, or equivalent degree, coupled with two years of experience; or by obtaining a Master's degree in computer science, computer communications, or electrical engineering, but having no experience; or by having no formal education but experience in computer science or computer communications of at least four years. EX-1003 ¶ 69.

F. State of the Art

The following section describes the state of conserving public addresses in telecommunications networks and common protocols for communicating configuration information to Internet hosts. The prior art references, and the discussions of what was known to a POSA, provide the factual support for the general description of the state of the art at the time of the invention and provide additional motivation to modify or combine the references.

1. Conserving Public Addresses

A publication titled SAVING PUBLIC ADDRESSES IN MOBILE IP by Z. Zhen et al. (*Zhen*)(EX-1006) was published in the Proceedings of the International Conference on Networking, International Conference on Mobile Communications

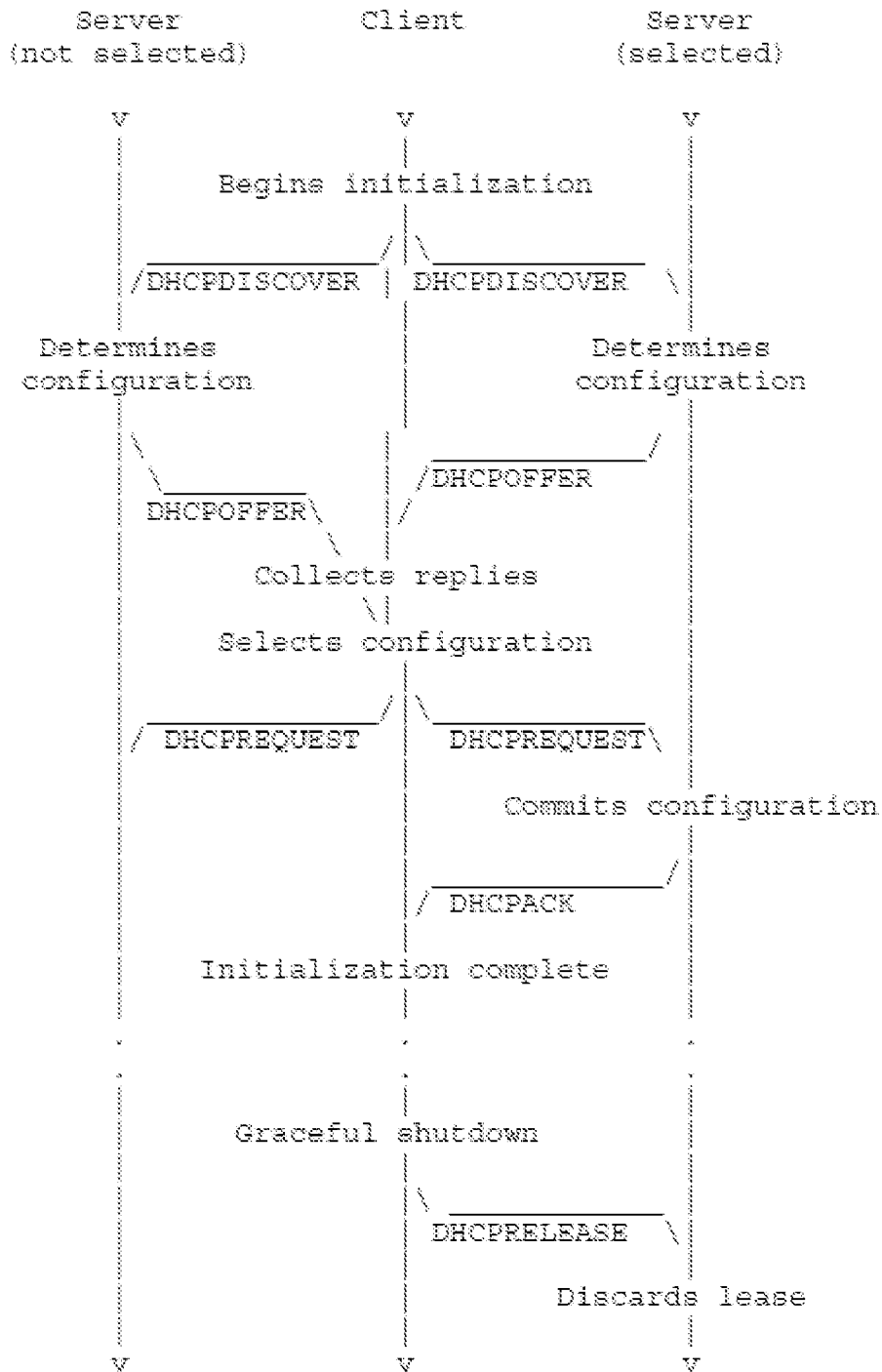
and Technologies in 2006. *Zhen* acknowledges the “deprivation of IPv4 address spaces” and the lag of adoptions of the IPv6 protocols. *Zhen* Abstract. *Zhen* discloses that “drawbacks of Mobile IPv4 is that it requires each mobile node (MN) to have a unique public home address and this causes a heavy demand for saving IPv4 addresses.” *Zhen* Abstract; EX-1003 ¶ 71.

Zhen discloses an address sharing technique that enables IP addresses to be reused among the nodes. *Zhen* Abstract. Specifically *Zhen* discloses using a common public IP address among several mobile nodes (MN), and assigning each of the MNs a range of port numbers. *Zhen* 3.1 ; EX-1003 ¶ 72.

The MN uses a preconfigured public address and an assigned port range to initiate a session. *Zhen* discloses the session address/port is then used as the destination address/port for packets received in the home network related to that session. The destination address/port and the source address/port subsequently uniquely identify the respective session. When a session packet is received, using the destination address/port and the session table, a virtual address/port which is an internal (private) address (i.e. the routing identifier or IDR) is determined, that enables the packet to be delivered to the specific application associated with the session. *Zhen* 3.4.1; EX-1003 ¶ 73.

2. Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol (“DHCP”) [RFC 2131] (EX-1007) has two components: a protocol for delivering host-specific configuration parameters from a DHCP server, and a mechanism for allocation of network addresses to a host EX-1007 2. A DHCP client is an Internet host that is using DHCP to obtain an address and configuration parameters. EX-1007 6. A DHCP server is an Internet host that returns configuration parameters to the client. EX-1007 6; EX-1003 ¶ 74.



The figure above shows the basic DHCP mechanism. A client broadcasts a DHCPDISCOVER message to find a DHCP server. The DHCPDISCOVER message may contain an identifier of the client or a device type in one of the

DHCP options. The server uses the information in the DHCPDISCOVER and any policies it has been configured with to offer the client an IP address along with other configuration parameters like a default gateway. EX-1007 14. The server provides this configuration information in a DHCPOFFER message sent to the client. If the client accepts the configuration, it replies with a DHCPREQUEST which is acknowledged by the server with a DHCPACK. There are other provisions for having one DHCP server serve multiple networks using DHCP relays, in which case, the DHCP server assigns addresses based on the gateway serving the network. EX-1007 27; EX-1003 ¶ 75.

The parameters in a DHCP message are shown below.

FIELD	OCTETS	DESCRIPTION
----	-----	-----
op	1	Message op code / message type. 1 = BOOTREQUEST, 2 = BOOTREPLY
htype	1	Hardware address type, see ARP section in "Assigned Numbers" RFC; e.g., '1' = 10mb ethernet.
hlen	1	Hardware address length (e.g. '6' for 10mb ethernet).
hops	1	Client sets to zero, optionally used by relay agents when booting via a relay agent.
xid	4	Transaction ID, a random number chosen by the client, used by the client and server to associate messages and responses between a client and a server.
secs	2	Filled in by client, seconds elapsed since client began address acquisition or renewal process.
flags	2	Flags (see figure 2).
ciaddr	4	Client IP address; only filled in if client is in BOUND, RENEW or REBINDING state and can respond to ARP requests.
yiaddr	4	'your' (client) IP address.
siaddr	4	IP address of next server to use in bootstrap; returned in DHCPOFFER, DHCPACK by server.
giaddr	4	Relay agent IP address, used in booting via a relay agent.
chaddr	16	Client hardware address.
sname	64	Optional server host name, null terminated string.
file	128	Boot file name, null terminated string; "generic" name or null in DHCPDISCOVER, fully qualified directory-path name in DHCPOFFER.
options	var	Optional parameters field. See the options documents for a list of defined options.

The yiaddr is used by the server to assign the IP address to the client. The siaddr is used by the client to send messages directly to the DHCP server. The giaddr is used if there is a relay (gateway) between the client and the DHCP server. The options fields include a client identifier and a vendor class identifier. EX-1007 36; EX-1003 ¶ 77.

III. SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

Requester submits that *Biswas* (EX-1004) and *Fangman* (EX-1005) cited herein raise a "substantial new question of patentability" because "the teaching of the (prior art) patents and printed publications is such that a reasonable examiner

would consider the teaching to be important in deciding whether or not the claim is patentable.” See MPEP 2242. For example, the references introduced and discussed in further detail below and in the attached charts, when considered by themselves or in view of the knowledge of a POSA, teach each of the elements recited in the claims.

Further, these references were never cited nor applied in an Office Action during prosecution of the ’369 Patent; the “same question of patentability as to the claim has not been decided by the Office in an earlier concluded examination or review of the patent” (MPEP 2242, Section I) at least because there is no evidence that the art referenced in this request was considered by the Office during prosecution of the ’369 Patent.

Further, to Requester’s knowledge, there has never been a prior post-grant proceeding challenging any claim of the ’369 Patent, much less based on the prior art references, *Fangman*, and *Biswas*, relied upon in this Request.

A. Prior Art

1. *Biswas* (EX-1004)

U.S. Patent No. 7,624,195 to Biswas et al. (“*Biswas*”) is titled METHOD AND APPARATUS FOR DISTRIBUTED NETWORK ADDRESS TRANSLATION PROCESSING. *Biswas* issued on November 24, 2009, from an application filed on May 8, 2003. *Biswas* qualifies as prior art under §102(e)(2)

(Pre-AIA). *Biswas* was not cited or applied by the Examiner during prosecution of the Challenged Claims.

2. *Fangman* (EX-1005)

U.S. Patent No. 8,363,647 to Fangman et al. (*Fangman*) is titled SYSTEM AND METHOD FOR CONFIGURING AN IP TELEPHONY DEVICE.

Fangman issued Jan. 13, 2013 from an application filed Jul. 11, 2001, and published Oct. 3, 2002 (US 2002/0141352). *Fangman* is prior art at least under § 102(b)(Pre-AIA). *Fangman* was not cited or applied by the examiner during prosecution of the Challenged Claims.

B. Ground 1: Anticipation and/or obviousness over *Biswas* Presents Substantial New Questions of Patentability (Claims 1-3, 5-17)

1. The *Biswas* Reference

Like the '369 Patent, *Biswas* identifies the “serious concern” of the depletion of IPv4 addresses, the known NAT solution to conserving public IP addresses, and discloses an improvement to the solution, including “methods and apparatuses for distributing network address translation functionally across one or more private network devices.” *Biswas* 1:13-37, 2:6-8. *Biswas* is thus analogous art to the '369 Patent. *Biswas* provides the following Abstract summarizing its invention:

Methods and apparatuses for distributing network address translation. By having a gateway inform inside devices of global addresses, the gateway can avoid performing many functions of a traditional NAT

box. Specifically, an inside device is informed of a global address shared by all devices on the inside device's network segment. Each device on that segment would be assigned a range of ports to distinguish messages from separate devices that use the same global address.

Biswas Abstract (emphasis added) ; EX-1003 ¶ 79.

Biswas provides FIG. 1 as a block diagram illustrating an exemplary environment in which its disclosed invention may be implemented. *Biswas* 42-43; EX-1003 ¶ 80.

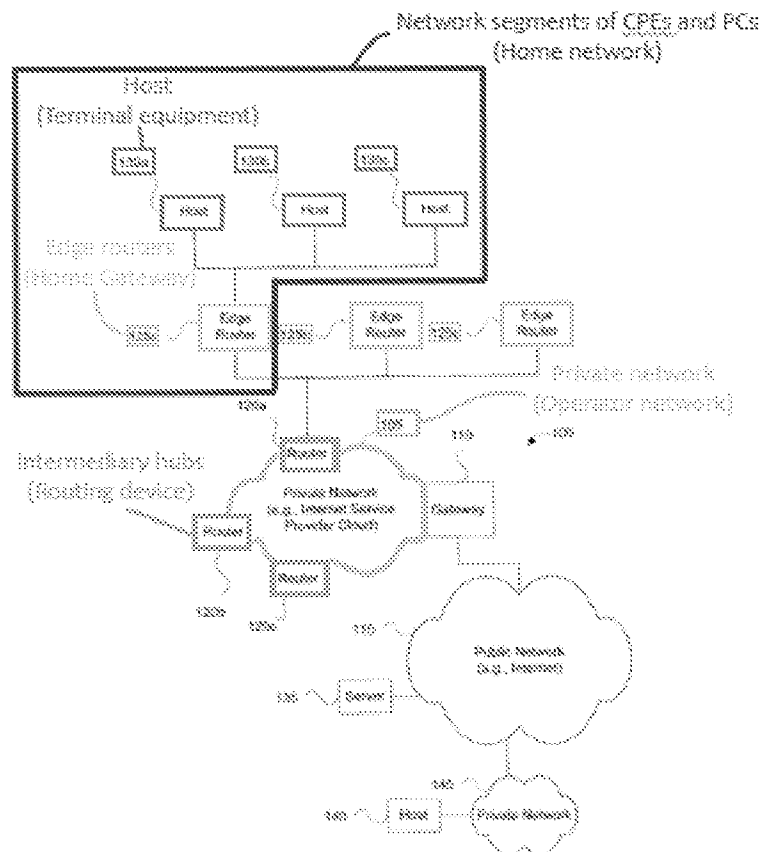


Figure 1

A private network 105 (green) [*operator network*]² such as an Internet Service provider (ISP) is coupled to a gateway 110 that allows connectivity with a public network 115 such as the Internet. *Biswas* 43-46. The private network 105 includes a plurality of intermediary hubs or routers 120a, 120b, 120c (blue) [*routing device*] that provide connectivity to a plurality of edge routers 125a, 125b, 125c (orange) [*home gateway*] that may be coupled to one or more hosts 130a, 130b, 130c (red), for example, PCs [*pieces of terminal equipment*] forming a network segment of CPEs and PCs (purple) [*home network*]. *Biswas* 3:46-59; EX-1003 ¶ 81.

Biswas explains that network addresses (IP addresses) associated with the devices 130a, 130b, 130c [*pieces of terminal equipment*] of the private network 105 and which are unique within the private network 105 are referred to as “inside” addresses with respect to the gateway 110 [*@PRIV or IDR*]; and network addresses used by devices of the public network 115 are referred to as “outside” addresses [*@PUB*]. *Biswas* 3:60-4:3; EX-1003 ¶ 82.

Biswas discloses that the plurality of routing devices 120a, 120b, 120c may share the same global or outside address [*@PUB*], and that these devices may be distinguished by the gateway 110 by assigning each routing device a disjoint port

² Corresponding terminology from the '369 Patent is shown in bracketed italics.

range [*port mask*] along with the public address. *Biswas* 4:51-57. The routing device maintains a mapping between the routers assigned public address/port range and its private address. *Biswas* 4:57-60; EX-1003 ¶ 83.

As with the routing devices 120, the edge routers 125a, 125b, 125c may have the same public address and the routing device would distinguish among the edge routers sharing the same public address by assigning a port range to each edge router. *Biswas* 7:23-26. The routing device 120 distinguishes packets addressed to the same public address based on the port range allocated to each edge router. *Biswas* 7:32-36. *Biswas* further discloses that the edge router may assign each PC a port range and provide the public address and assigned port range to the respective PC. *Biswas* 7:59-67; EX-1003 ¶ 84.

When the routing device 120 initiates a request for assignment of an inside (private) address, the routing device receives an assignment of the inside (private) address and outside (public) address. The routing devices 120 are responsible for the downstream devices – edge routers (CPEs) 125 and hosts 130 (PCs). *Biswas* 2:43-54. The routing device 120 ensures traffic from downstream devices uses the outside (public) address to communicate with outside devices by performing a NAT function or by passing the address data to the devices. *Biswas* 2:54-59; EX-1003 ¶ 85.

When an edge router 125 requests an assignment of an inside (private) address, the edge router is assigned an inside address, an outside (public) address, and a range of ports. *Biswas* 2:60-65. The edge router 125 ensures traffic from each host 130 uses the outside (public) address and a port from within the port range as an identifier to communicate with outside devices by performing NAT functions or passing the address/port range data to the PCs. *Biswas* 2:66-3:5; EX-1003 ¶ 86.

Biswas discloses that inside (private) addresses are assigned using DHCP and that a GAPP/RAPID server is responsible for assigning outside (public) addresses and/or port ranges. *Biswas* 5:28-30. Once the private and public addresses and or port ranges are assigned to a device, the configuration data is routed to the device. *Biswas* 5:52-54; EX-1003 ¶ 87.

Each of the limitations recited in Claims 1-3 and 5-17 is disclosed or rendered obvious by *Biswas* as demonstrated in the Proposed Rejection 1 below, and in the charts comparing *Biswas* to Claims 1-3 and 5-17 provided as Exhibit AA. EX-1003, ¶ 88.

C. Ground 2: Anticipation and/or obviousness over *Fangman* Presents Substantial New Questions of Patentability (Claims 1-3, 5-8, 10, 11, 13-17)

1. The *Fangman* Reference

Like the '369 Patent, *Fangman* acknowledges the “rapid depletion” of public IP addresses and the “severe restriction” placed on the allocation of such routable, public addresses, and the use of NAT technology to conserve addresses. *Fangman* 1:46-54. *Fangman* is directed to a method and system for configuring IP telephony devices and using NAPT technology to conserve public IP addresses in an IP telephone system. *Fangman* Abstract, 13:39-48. *Fangman* is thus analogous art to the '369 Patent. EX-1003 ¶ 89.

FIG. 2 illustrates an embodiment of the IP telephony system:

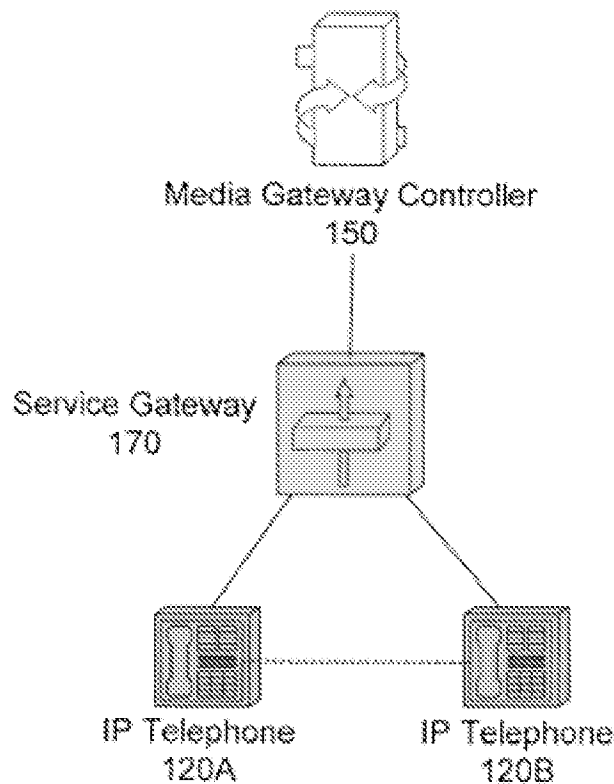


Figure 2

The IP telephony system includes IP telephones 120A, 120B (red) [terminal equipment] that are coupled to a Service Gateway (SG) 170 (blue) [routing device]. The SG 170 is also coupled to a Media Gateway Controller (MGC) 150 (gold). *Fangman* 6:29-43. The SG 170 may use a single public IP address [@PUB] that is shared among the IP telephones 120. *Fangman* 8:10-15. The SG 170 also allocates a range of port numbers [port mask MP] to each IP telephone. *Fangman* 8:30-33; EX-1003 ¶ 91.

Fangman describes the IP telephone initialization, configuration, and use with reference to a flowchart illustrated in FIG. 4B:

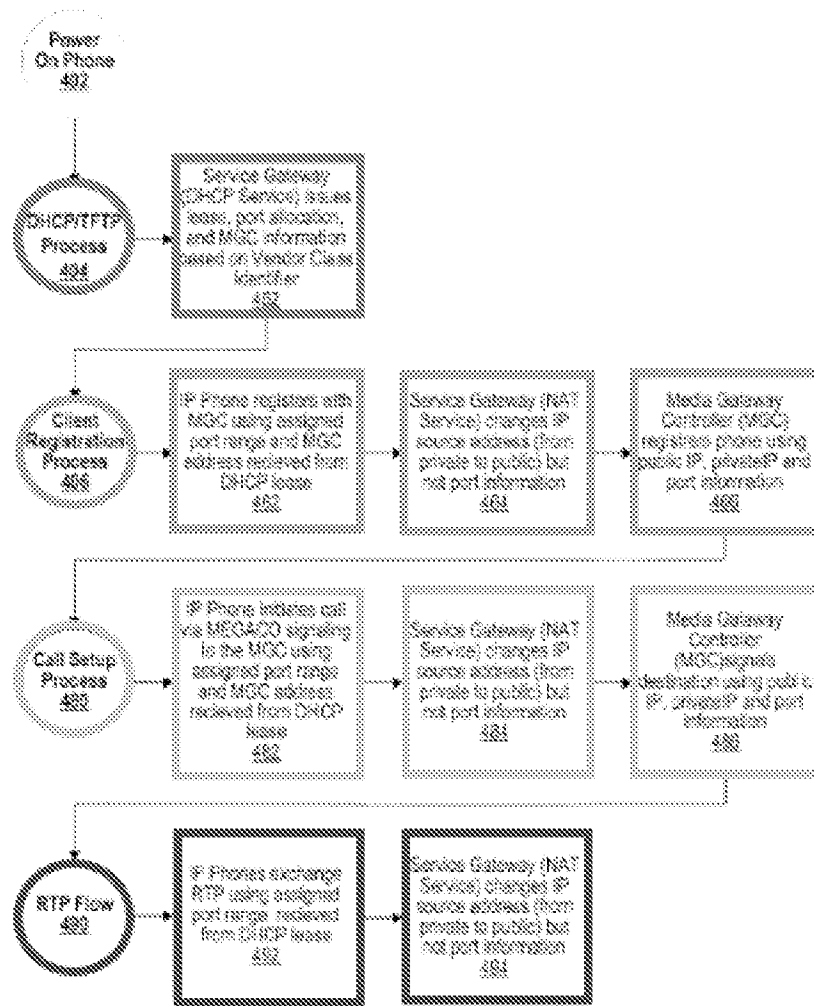


Figure 4B

EX-1003 ¶ 92

After powering up in Step 402, the IP telephone undergoes a DHCP/TFTP process in Step 404 and detailed in box 452 (red). The SG 170 receives an identifier from the IP telephone 120 such as a Vendor Class ID. Upon validating the IP telephone 120 based on the identifier, the SG 170 assigns a range of port numbers to the IP telephone 120 that may then be used by the IP telephone 120 to

send and receive IP communications. *Fangman* 16:12-19. The system may then provide DHCP lease information, the port range allocation and the MGC address to the IP telephone 120. *Fangman* 16:24-29. The initialization information may be downloaded to the IP telephone 120 via TFTP. *Fangman* 17:4-6. The SG 170 and IP telephone 120 may then each store this information. *Fangman* 16:37-40; EX-1003 ¶ 93.

The Client Registration Process of Step 406 is detailed in boxes 462, 464, and 466 (blue). The IP telephone 120 registers with the MGC 150 using the allocated port range and the MGC address provided in Step 404 (Box 462.) The SG 170 (as a NAT service) changes the source address from private to public. (Box 464). The MGC 150 then registers the IP telephone using the public IP address, the private IP address and the allocated port range. (Box 466). *Fangman* 17:7-25 EX-1003 ¶ 94.

The Call Setup Process of Step 480 is detailed in Boxes 482, 484, and 488 (green). The IP telephone 120 initiates a call using the port range and MGC address received in Step 404 (Box 482). The SG 170 (as a NAT service) changes the source address from private to public (Box 484). The MGC 150 then signals the call destination using the public IP address, the private IP address, and the port information. *Fangman* 17:26-38; EX-1003 ¶ 95.

The RTP flow related to the IP telephone call in Step 490 is detailed in Boxes 492 and 494 (purple). The IP telephones 120 exchange RTP using one or more ports from the respective allocated port ranges assigned in Step 404 (Box 492). The SG 170 (as a NAT service) changes the source address from private to public (Box 494). More specifically, the SG 170 performs NAPPT on the data packet and sends the NAPPTed data packet to the destination device. The data packet includes a private source IP address of the IP telephone 120, a source port selected from the allocated port range, and destination information related to the destination device. *Fangman* 17:38-59 ; EX-1003 ¶ 96.

Conversely, when the SG 170 receives an incoming data packet destined for IP telephone 120 including the public IP address and a port number from the assigned range of port numbers for the IP telephone 120, the SG 170 uses the public IP address and port number to uniquely identify the private IP address of the IP telephone 120. The SG 170 performs NAPPT on the packet and sends the NAPPTed packet to the private IP address of the IP telephone 120. *Fangman* 17:60-18:10 ; EX-1003 ¶ 97.

Each of the limitations recited in Claims 1-3, 5-8, 10, 11, and 13-17 is disclosed or rendered obvious by *Fangman* as demonstrated in the Proposed Rejection 2 below, and in the charts comparing *Fangman* to Claims 1-3, 5-8, 10, 11, and 13-17 provided as Exhibit BB. EX-1003, ¶ 98.

IV. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Proposed Rejections

Proposed Rejections	Claims	Basis	References
1	1-3 and 5-17	§§ 102/103	Anticipated by or obvious over <i>Biswas</i>
2	1-3, 5-8, 10, 11, and 13-17	§§ 102/103	Anticipated by or obvious over <i>Fangman</i>

B. Proposed Rejection 1: Claims 1-3 and 5-17 are anticipated by or obvious over *Biswas*

Claims 1-3 and 15-17 are anticipated by or obvious over U.S. Patent No. 7,624,195 (“*Biswas*”) under §§ 102/103. EX-1003 ¶ 99.

Claim 1³

Biswas anticipates or renders obvious **a method of routing an IP data packet in a telecommunications network to a destination equipment**, (*See Biswas* “A private network 105, such as an Internet Service Provider (ISP) is coupled with a gateway 110, which allows connectivity with a public network 115, such as the Internet. The private network 105 includes a plurality of intermediary hubs or routers 120a, 120b and 120c, such as aggregators that provide connectivity

³ Claim language in **Bold**

for a plurality of edge routers 125a, 125b and 125c. The edge routers 125a, 125b and 125c may be in the form of customer premises equipment (CPE), such as a cable modem, which may be coupled to one or more hosts 130a, 130b and 130c, such as PCs.” “The aggregator would then be able to route messages to the appropriate CPE based on the packets tuple.” 3:43-53, 7:37-38 ; EX-1003 ¶ 100)

said packet comprising a primary destination address and a destination port number, (See *Biswas* “Additionally, the edge router ensures that traffic from each responsible device uses the outside address [*primary destination address*] and a port within the port range [*destination port number*] as an identifier for itself to communicate with outside devices.” 2:66-3:2; EX-1003 ¶101)

said method comprising, on reception of said packet, the following steps: 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; (See *Biswas* “This can be achieved by giving a disjoint port-range [*port mask*] along with the outside address [*primary destination address*] to the aggregator. The gateway could then maintain a mapping between the aggregator’s assigned outside-address/port-range [*primary destination address/port mask*] and the aggregator’s inside-address [*identifier*].” 4:56-60. “When the gateway 110 received an outside packet [*IP data packet*], it could then route the packet to a selected aggregator based on both the outside address [*primary*

destination address] and the port number [*destination port number*].” 5:6-8; EX-1003 ¶102)

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; (*See Biswas* When multiple aggregators share a global address [*primary destination address*] “[t]he gateway could then maintain a mapping between the aggregator’s assigned outside-address/port-range [*primary destination address/port mask*] and the aggregator’s inside-address [*identifier*].” 4:57-60. “When the gateway 110 received an outside packet [*IP data packet*], it could then route the packet to a selected aggregator [*destination equipment*] based on both the outside address [*primary destination address*] and the port number [*destination port number*].” 5:6-8. “When the gateway 110 received an outside packet, it could either encapsulate (tunnel) the outside packet to the aggregator’s second inside address [*identifier*] or perform very basic header-only NAT on the outside packet such that the outside address is modified to the second inside address [*identifier*]. This second inside address is routable in this private domain 105.” 6:42-46. “Additionally, the aggregator includes some mechanism that allows it to distinguish between packets addressed to the same outside address. In a preferred embodiment, each CPE would be given a port range. Allocation of port ranges could be accomplished through the

aggregator, or some other device. The aggregator would then be able to route messages to the appropriate CPE based on the packet's tuple." 7:32-38; EX-1003 ¶103)

and routing the packet to the destination equipment based on said identifier. (See *Biswas* "When the gateway 110 received an outside packet [*IP data packet*], it could then route the packet to a selected aggregator [*destination equipment*] based on both the outside address and the port number." 5:6-8 . "When the gateway 110 received an outside packet, it could either encapsulate (tunnel) the outside packet to the aggregator's second inside address [*identifier*] or perform very basic header-only NAT on the outside packet such that the outside address is modified to the second inside address. This second inside address [*identifier*] is routable in this private domain 105" to the aggregator [*destination equipment*] 6:42-46; EX-1003 ¶104).

Claim 2

Biswas anticipates or renders obvious **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.** (See *Biswas* "When the gateway 110 received an outside packet [*IP data packet*], it could either encapsulate (tunnel) the outside packet to the aggregator's second inside address [*secondary destination address*] or perform very basic header-only NAT on the

outside packet such that the outside address is modified to the second inside address. This second inside address [*secondary destination address*] is routable in this private domain 105.” 6:42-46. “Network addresses (e.g. IP addresses) used by devices of the public network 115 are referred to as “outside” addresses with respect to the gateway 115.” 3:60-62; EX-1003 ¶xx). The second inside address is a secondary destination address. EX-1003 ¶ 105.

Claim 3

Biswas anticipates or renders obvious **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 address.** (See *Biswas* “When the gateway 110 received an outside packet [*IP data packet*], it could either encapsulate (tunnel) the outside packet to the aggregator’s second inside address [*secondary address*] or perform very basic header-only NAT on the outside packet such that the outside address is modified to the second inside address. This second inside address is routable in this private domain 105.” 6:42-46; EX-1003 ¶106).

Claim 15

Biswas anticipates or renders obvious **a non-transitory computer readable medium encoded with code program instructions executable by a microprocessor to perform the method according to claim 1.** (See *Biswas*

“Generally, the techniques of the present invention may be implemented on software and/or hardware. For example, they can be implemented in an operating system kernel, in a separate user process, in a library package bound into network applications, on a specially constructed machine, or on a network interface card. In a specific embodiment of this invention, the technique of the present invention is implemented in software such as an operating system or in an application running on an operating system. A software or software/hardware hybrid implementation of the techniques of this invention may be implemented on a general-purpose programmable machine selectively activated or reconfigured by a computer program stored in memory.” 8:1-15; EX-1003 ¶107).

Claim 5

Biswas anticipates or renders obvious Claim 5 for at least the reasons set forth above with respect to Claim 1.

Claim 6

Biswas anticipates or renders obvious Claim 6 for at least the reasons set forth above with respect to Claim 1.

Claim 7

Biswas anticipates or renders obvious **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: (See *Biswas* “A private network 105, such as an Internet Service Provider (ISP) is coupled with a gateway 110, which allows connectivity with a public network 115, such as the Internet.” 3:44-46. “When a CPE requests an inside address, the aggregator (or some device in concert with the aggregator) would reply with an inside DHCP address and the outside address and/or port ranges.” 7:27-31; EX-1003 ¶110).

assigning to said piece of terminal equipment a primary address shared with a plurality of pieces of terminal equipment; (See *Biswas* “Specifically, an inside device is informed of a global address [*primary address*] shared by all devices [*pieces of terminal equipment*] on the inside device’s network segment.” Abstract “The edge router then receives an assignment of the inside address, a range of useable ports and a notification of an outside address [*primary address*] that outside devices will use to communicate with the responsible devices [*pieces of terminal equipment*].” 2:60-65; EX-1003 ¶111).

assigning to said piece of terminal equipment a port mask defining a range of numbers dedicated to it and a routing identifier; (See *Biswas* “Specifically, an inside device is informed of a global address shared by all devices [*pieces of terminal equipment*] on the inside device’s network segment. Each device [*piece of terminal equipment*] on that segment would be assigned a range of ports [*port mask*] to distinguish messages from separate devices that use the same

global address.” Abstract. “As with the aggregator, the CPEs would need to be both alerted to outside packets requiring NAT functions and have access to the outside address and/or port-ranges in order to perform the NAT functions.

Therefore, just as the aggregators would be aware of their outside addresses and/or port-ranges, so would the CPEs. When a CPE requests an inside address [*routing identifier*], the aggregator (or some device in concert with the aggregator) would reply with an inside DHCP address [*routing identifier*] and the outside address and/or port-ranges. Additionally, the aggregator includes some mechanism that allows it to distinguish between packets addressed to the same outside address. In a preferred embodiment, each CPE would be given a port range [*port mask*].

Allocation of port ranges could be accomplished through the aggregator, or some other device. The aggregator would then be able to route messages to the appropriate CPE based on the packet’s tuple.” 7:23-38; EX-1003 ¶112).

sending to said piece of terminal equipment a configuration message comprising said primary address, said port mask, and said routing identifier.

(See *Biswas* “When a CPE requests an inside address [*routing identifier*], the aggregator (or some device in concert with the aggregator) would reply with an inside DHCP address [*routing identifier*] and the outside address [*primary address*] and/or port ranges [*port mask*].” 7:27-31. “Once the inside and outside addresses

and/or port ranges are assigned, data identifying both addresses must be routed to the same device.” 5:52-54; EX-1003 ¶113).

Claim 8

Biswas anticipates or renders obvious **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.** (See *Biswas* “When a CPE requests an inside address, the aggregator (or some device in concert with the aggregator) would reply with an inside DHCP address [*routing identifier*] and the outside address [*primary address*] and/or port ranges [*port mask*].” 3:3-5; EX-1003 ¶114).

Claim 9

Biswas anticipates or renders obvious **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.** (See *Biswas* “The edge router receives the configuration message, including the primary address, and forwards it downstream. The edge router can also ensure such traffic uses outside

addresses either by performing NAT functions or passing outside address information on to devices on the edge router's network segment." 3:3-5. "When a CPE requests an inside address, the aggregator (or some device in concert with the aggregator) would reply with an inside DHCP address [*routing identifier*] and the outside address [*primary address*] and/or port ranges [*port mask*]." 7:27-31; EX-1003 ¶115).

Claim 16

Biswas anticipates or renders obvious **a non-transitory computer readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 7.** (See *Biswas* "Generally, the techniques of the present invention may be implemented on software and/or hardware. For example, they can be implemented in an operating system kernel, in a separate user process, in a library package bound into network applications, on a specially constructed machine, or on a network interface card. In a specific embodiment of this invention, the technique of the present invention is implemented in software such as an operating system or in an application running on an operating system. A software or software/hardware hybrid implementation of the techniques of this invention may be implemented on a general-purpose programmable machine selectively activated or reconfigured by a computer program stored in memory." 8:1-15; EX-1003 ¶116).

Claim 10

Biswas anticipates or renders obvious Claim 10 for at least the reasons set forth above with respect to Claim 7.

Claim 11

Biswas anticipates or renders obvious **a method of configuring a piece of terminal equipment connected to a telecommunications network** (*See Biswas* “A private network 105, such as an Internet Service Provider (ISP) is coupled with a gateway 110, which allows connectivity with a public network 115, such as the Internet.” 3:44-46. “When a CPE requests an inside address, the aggregator (or some device in concert with the aggregator) would reply with an inside DHCP address and the outside address and/or port ranges.” 7:27-31; EX-1003 ¶118).

wherein on reception of a configuration message comprising configuration data comprising a primary address, a port mask defining range of port numbers that is dedicated thereto, and a routing identifier, (*See Biswas* “When a CPE requests an inside address, the aggregator (or some device in concert with the aggregator) would reply with an inside DHCP address [*routing identifier*] and the outside address [*primary address*] and/or port ranges [*port mask*].” 7:27-31 “Once the inside and outside addresses [*routing identifier and primary address*] and/or port ranges [*port mask*] are assigned, data identifying both addresses must be routed to the same device.” 5:52-54; EX-1003 ¶119).

said method comprises the following steps: storing said configuration data; (See *Biswas* “Based on the disclosure in *Biswas* that configuration data is sent to the host [*piece of terminal equipment*] such as a PC, a POSA would have understood that the PC stores that data prior to using the data to send a data packet into the telecommunications network. EX-1003 ¶120).

and before sending a data packet into the telecommunications network, selecting a port number in the range of port numbers defined by the port mask, (See *Biswas* “Additionally, the edge router ensures that traffic from each responsible device [*piece of terminal equipment*] uses the outside address and a port within the port range [*a port number in the range of port numbers*] as an identifier for itself to communicate with outside devices. The edge router can also ensure such traffic uses outside addresses either by performing NAT functions or passing outside address information on to devices on the edge router’s network segment.” 2:66-3:5; EX-1003 ¶121).

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. (See *Biswas* “Additionally, the edge router ensures that traffic from each responsible device uses the outside address [*source address*] and a port within the port range [*source port number*] as an identifier for itself to communicate with outside devices. The edge router can also ensure such traffic uses outside addresses

either by performing NAT functions or passing outside address information on to devices on the edge router's network segment." 2:66-3:5; EX-1003 ¶122).

Claim 12

Biswas anticipates or renders obvious **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.** (*See Biswas* "The edge router receives the configuration message, including the primary address, and forwards it downstream. "The edge router can also ensure such traffic uses outside addresses either by performing NAT functions or passing outside address [*primary address*] information on to devices on the edge router's network segment [*pieces of terminal equipment*]." 3:3-5. "When a CPE requests an inside address, the aggregator (or some device in concert with the aggregator) would reply with an inside DHCP address and the outside address and/or port ranges." 7:27-31. "Once the CPE was aware of the outside address, it could either perform the NAT functions itself, or obviate the need for the majority of NAT processing by informing the PCs of a global address and its own port range." 7:58-62. "Once the inside and outside addresses and/or port ranges are assigned, data identifying both addresses must be routed to the same device." 5:52-54; EX-1003 ¶123).

Claim 13

Biswas anticipates or renders obvious **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.** (See *Biswas* “The gateway could then maintain a mapping between the aggregator’s assigned outside-address/port-range and the aggregator's inside-address.” 4:57-60. “When the gateway 110 received an outside packet, it could then route the packet to a selected aggregator based on both the outside address and the port number.” 5:6-8; EX-1003 ¶124.

Based on at least this disclosure in *Biswas* that port ranges are used to identify the inside address of a destination device that shares an outside address with other devices, a POSA would have understood that a packet would be rejected if the port number identified in the packet did not belong to the range of port numbers defined by the port range of any device. EX-1003 ¶124).

Claim 17

Biswas anticipates or renders obvious **a non-transitory computer-readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 11.** (See *Biswas*

“Generally, the techniques of the present invention may be implemented on software and/or hardware. For example, they can be implemented in an operating system kernel, in a separate user process, in a library package bound into network applications, on a specially constructed machine, or on a network interface card. In a specific embodiment of this invention, the technique of the present invention is implemented in software such as an operating system or in an application running on an operating system. A software or software/hardware hybrid implementation of the techniques of this invention may be implemented on a general-purpose programmable machine selectively activated or reconfigured by a computer program stored in memory.” 8:1-15; EX-1003 ¶125).

Claim 14

Biswas anticipates or renders obvious Claim 14 for at least the reasons set forth above with respect to Claim 11.

C. Proposed Rejection 2: Claims 1-3, 5-8, 10, 11, and 13-17 are anticipated by or obvious over *Fangman*

Claims 1-3, 5-8, 10, 11, and 13-17 are anticipated by or obvious over U.S. Patent No. 8,363,647 (“*Fangman*”) under §§ 102/103. EX-1003 ¶127.

Claim 1

Fangman anticipates or renders obvious **a method of routing an IP data packet in a telecommunications network to a destination equipment, (See**

Fangman “FIG. 2 illustrates one embodiment of a VoIP system for providing IP telephony services to a business or other organization [*telecommunications network*]. The system in FIG. 2 includes one or more IP telephones 120A and 120B [*destination equipment*]. As used herein, the terms “IP telephone” and “Media Gateway” are intended to include any telephony or communication device that operates to use a network protocol, such as Internet Protocol (IP). Thus, an IP telephone 120 is a Media Gateway, as is a Trunking Gateway. Said another way, an IP telephone or Media Gateway is a device that receives an analog input and encodes the signal into an IP data stream.” 6:8-18; EX-1003 ¶ 128).

said packet comprising a primary destination address and a destination port number, (*See Fangman* “In one embodiment, performing IP communications using the IP telephone may include the Service Gateway receiving a data packet [*IP data packet*] from the IP telephone, including a private source IP address, a source port number in the assigned range of port numbers [*destination port number*], and destination information associated with an IP device.” 3:66-4:4. “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 [*primary destination address*], a destination port number [*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.” 17:60-65; EX-1003 ¶ 129).

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; (See *Fangman* “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 [*primary destination address*], a destination port number [*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 [*primary destination address*] and the destination port number [*destination port number*] may be used to uniquely identify the IP telephone 120 [*destination equipment*]. 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 [*at least one identifier*]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.” 17:60-18:9; EX-1003 ¶ 130).

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 (See *Fangman* “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 [*primary destination address*], a destination port number [*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 [*primary destination address*] and the destination port number [*destination port number*] may be used to uniquely identify the IP telephone 120 [*destination equipment*]. 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 [*at least one identifier*] 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.” 17:60-18:9; EX-1003 ¶131).

routing the packet to the destination equipment based on said identifier.

(See *Fangman* “The packets are routed to the IP telephone via the private IP address. 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 [*identifier*] 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.” 18:1-9; EX-1003 ¶132).

Claim 2

Fangman anticipates or renders obvious **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.** (See *Fangman* “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 [*primary destination address*], a destination port number [*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 [*primary destination address*] and the destination port number [*destination port number*] may be used to uniquely identify the IP telephone 120 [*destination equipment*]. 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 [*at least one identifier*] 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.” 17:60-18:9; EX-1003 ¶133).

Claim 3

Fangman anticipates or renders obvious **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 address.** (*See Fangman*

“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 [*primary destination address*], a destination port number [*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 [primary destination address] and the destination port number [destination port number] may be used to uniquely identify the IP telephone 120 [destination equipment]. 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 [*at least one identifier*]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.” 17:60-18:9; EX-1003 ¶134).

Claim 15

Fangman anticipates or renders obvious **a non-transitory computer readable medium encoded with code program instructions executable by a microprocessor to perform the method according to claim 1.** (*See Fangman* “The system preferably includes a memory medium on which software according to an embodiment of the present invention may be stored. The term “memory medium” is intended to include an installation medium, e.g., a CD-ROM, floppy disks, or tape device; a computer system memory or random access memory (RAM) such as DRAM, SRAM, EDO RAM, RRAM, etc.; or a non-volatile memory such as a magnetic media, e.g., a hard drive, or optical storage. The

memory medium may include other types of memory as well, or combinations thereof. In addition, the memory medium may be located in a first computer in which the software program is stored or executed, or may be located in a second different computer which connects to the first computer over a network, such as the Internet. In the latter instance, the second computer provides the program instructions to the first computer for execution. Also, the computer system may take various forms, including a personal computer system, mainframe computer system, workstation, network appliance, Internet appliance, personal digital assistant (PDA), television set-top box, or other device. In general, the term “computer system” can be broadly defined to encompass any device having at least one processor which executes instructions from a memory medium, or any device which includes programmable logic that is configurable to perform a method or algorithm.” 30:62-31:19; EX-1003 ¶ 135).

Claim 5

Fangman anticipates or renders obvious Claim 5 for at least the reasons set forth above with respect to Claim 1.

Claim 6

Fangman anticipates or renders obvious Claim 6 for at least the reasons set forth above with respect to Claim 1.

Claim 7

Fangman anticipates or renders obvious **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:** (See *Fangman* “FIGS. 4A and 4B are flowchart diagrams that illustrate initialization, configuration, and use of an IP telephone 120 (or other Media Gateway) according to one embodiment of the present invention.” 15:18-21; EX-1003 ¶138).

assigning to said piece of terminal equipment a primary address shared with a plurality of pieces of terminal equipment; (See *Fangman* “The issue of unattainable addresses may be addressed by using a NAPT technology, as is well known in the art. Using a small number of mutable addresses for each SG 170 is a reasonable and justifiable approach which is consonant with the goals and methods of ARIN (American Registry for Internet Numbers). The use of VPN technologies and the use of the SG 170 as the default gateway for all the IP telephones 120 may simplify the routing architecture of the VoIP solution.” 13:40-48. “The SG 170 may use a single, public IP address [*primary address*] as the source and destination address for IPSec VPN tunnels. This address may be shared between the active and standby SGs 170. The SG 170 may use a single, public IP address [*primary address*] to provide NAT support for all the internal hosts [*pieces of terminal equipment*] needing VoIP protocol support. It may be able to use additional NAT

addresses to support a large number of internal hosts, e.g., IP telephones 120. This address may also be shared between the active and standby SGs 170. For the internal interfaces, the SG 170 must support virtual IP addresses for each VLAN interface.” 8:7-17. “Specifically, via DHCP the SG 170 may perform one or more of the following: assign the IP address and network mask” to the IP telephone. 8:48-49; EX-1003 ¶139).

assigning to said piece of terminal equipment a port mask defining a range of numbers dedicated to it and a routing identifier; and (See *Fangman* “Instead of dynamically assigning ports to IP telephones, the SG 170 may allocate a range of port numbers [*port mask*] for each IP telephone 120 [*piece of terminal equipment*] 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 [*routing identifier*] with the NATed external source IP address 8:30-37. “The SG 170 may then determine if the identifier is valid, and if the identifier is valid, assign a range of port numbers [*port mask*] to the IP telephone 120 based on the identifier. The IP telephone 120 may then use at least a subset of the range of port numbers to send or receive IP communications.” 16:13-19. “In one embodiment, the internal hosts, or IP telephones, may use a private IP address [*routing*

identifier] assigned by the SG DHCP service in the normal fashion for all IP headers.” 11:48-59. “Specifically, via DHCP the SG 170 may perform one or more of the following: assign the IP address and network mask,” 8:48-49; EX-1003 ¶ 140).

sending to said piece of terminal equipment a configuration message comprising said primary address, said port mask, and said routing identifier.

(See *Fangman* “As indicated in 452, in one embodiment, the system may provide DHCP lease information, port range allocation [*port mask*], and Media Gateway Controller (MGC) information, e.g., an MGC address, to the IP telephone 120 [*piece of terminal equipment*] based on the identifier, e.g., the Vendor Class ID. In one embodiment, the identifier of the IP telephone 120 may be included in a DHCP discover message issued by the IP telephone 120 to the SG 170, in which case the SG 170 may respond with a DHCP offer to the IP telephone (if the identifier is determined to be valid), where the DHCP offer may include DHCP lease information based on the validated identifier. The IP telephone 120 may then issue a DHCP request in response to the issued DHCP offer.” 16:24-37. “In one embodiment, the internal hosts, or IP telephones, may use a private IP address [*routing identifier*] assigned by the SG DHCP service in the normal fashion for all IP headers.” 11:48-59. “Specifically, via DHCP the SG 170 may perform one or more of the following: assign the IP address and network mask ...” 8:48-49. “As

described above with reference to FIG. 4A 404, the method may further include downloading initialization information to the IP telephone 120 via TFTP.”17:4-6 ; EX-1003 ¶ 141. A POSA understood a DHCP Offer [*configuration message*] as disclosed in *Fangman* includes at least a “primary address” as acknowledged by the ’369 Patent 10:4-13 (“the configuration message MESS-CONF is a DHCP_OFFER() type offer that contains the IP configuration data relating to the configuration of the terminal equipment that requested it. Such data includes at least: an IPv4 secondary address @PRIV; an IPv4 primary address @PUB;”). Additionally, a POSA understood a “DHCP server may return its own address in the ’siaddr’ field, if the server is prepared to supply the next bootstrap service (e.g., delivery of an operating system executable image). A DHCP server always returns its own address [*primary address*] in the ‘server identifier’ option. EX-1007 10; EX-1003 ¶142).

Claim 8

Fangman anticipates or renders obvious **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.** (See *Fangman* “As indicated

in 452, in one embodiment, the system may provide DHCP lease information, port range allocation, and Media Gateway Controller (MGC) information, e.g., an MGC address, to the IP telephone 120 based on the identifier, e.g., the Vendor Class ID. In one embodiment, the identifier of the IP telephone 120 may be included in a DHCP discover message issued by the IP telephone 120 to the SG 170, in which case the SG 170 may respond with a DHCP offer [*configuration message*] to the IP telephone (if the identifier is determined to be valid), where the DHCP offer may include DHCP lease information based on the validated identifier. The IP telephone 120 may then issue a DHCP request in response to the issued DHCP offer.” 16:24-37 “As described above with reference to FIG. 4A 404, the method may further include downloading initialization information to the IP telephone 120 via TFTP.” 17:4-6; EX-1003 ¶143)

Claim 16

Fangman anticipates or renders obvious **a non-transitory computer readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 7.** (*See Fangman* “The system preferably includes a memory medium on which software according to an embodiment of the present invention may be stored. The term “memory medium” is intended to include an installation medium, e.g., a CD-ROM, floppy disks, or tape device; a computer system memory or random access memory

(RAM) such as DRAM, SRAM, EDO RAM, RRAM, etc.; or a non-volatile memory such as a magnetic media, e.g., a hard drive, or optical storage. The memory medium may include other types of memory as well, or combinations thereof. In addition, the memory medium may be located in a first computer in which the software program is stored or executed, or may be located in a second different computer which connects to the first computer over a network, such as the Internet. In the latter instance, the second computer provides the program instructions to the first computer for execution. Also, the computer system may take various forms, including a personal computer system, mainframe computer system, workstation, network appliance, Internet appliance, personal digital assistant (PDA), television set-top box, or other device. In general, the term “computer system” can be broadly defined to encompass any device having at least one processor which executes instructions from a memory medium, or any device which includes programmable logic that is configurable to perform a method or algorithm.” 30:62-31:19; EX-1003 ¶144).

Claim 10

Fangman anticipates or renders obvious Claim 10 for at least the reasons set forth above with respect to Claim 7.

Claim 11

Fangman anticipates or renders obvious **a method of configuring a piece of terminal equipment connected to a telecommunications network**, (*See Fangman* “FIGS. 4A and 4B are flowchart diagrams that illustrate initialization, configuration, and use of an IP telephone 120 (or other Media Gateway) according to one embodiment of the present invention.” 15:18-21; EX-1003 ¶146).

wherein on reception of a configuration message comprising configuration data comprising a primary address, a port mask defining range of port numbers that is dedicated thereto, and a routing identifier, (*See Fangman* “As indicated in 452, in one embodiment, the system may provide DHCP lease information, port range allocation [*port mask*], and Media Gateway Controller (MGC) information, e.g., an MGC address, to the IP telephone 120 [*piece of terminal equipment*] based on the identifier, e.g., the Vendor Class ID. In one embodiment, the identifier of the IP telephone 120 may be included in a DHCP discover message issued by the IP telephone 120 to the SG 170, in which case the SG 170 may respond with a DHCP offer [*configuration message*] to the IP telephone (if the identifier is determined to be valid), where the DHCP offer may include DHCP lease information based on the validated identifier. The IP telephone 120 may then issue a DHCP request in response to the issued DHCP offer.” 16:24-37. “As described above with reference to FIG. 4A 404, the method

may further include downloading initialization information to the IP telephone 120 via TFTP.” 17:4-6 ; EX-1003 ¶ 147.

A POSA understood a DHCP Offer [*configuration message*] as disclosed in *Fangman* includes at least a “primary address” as acknowledged by the ’369 Patent 10:4-13 (“the configuration message MESS-CONF is a DHCP_OFFER() type offer that contains the IP configuration data relating to the configuration of the terminal equipment that requested it. Such data includes at least: an IPv4 secondary address @PRIV; an IPv4 primary address @PUB;”). Additionally, a POSA understood a “DHCP server may return its own address in the ‘siaddr’ field, if the server is prepared to supply the next bootstrap service (e.g., delivery of an operating system executable image). A DHCP server always returns its own address [primary address] in the ‘server identifier’ option. EX-1007 10; EX-1003 ¶147)

said method comprises the following steps: storing said configuration data; (See *Fangman* “The range of port numbers may include one or more port numbers which are not reserved for use by other IP protocols. The client DHCP lease negotiations may include the IP telephone issuing a DHCP discover message to the Service Gateway, which may then issue a DHCP offer to the IP telephone if the identifier is determined to be valid. The DHCP offer may include DHCP lease information based on the validated identifier, such as the range of port numbers

and information indicating operational software for the IP telephone. The Service Gateway may store the DHCP lease information. The IP telephone may store the DHCP lease information [*storing said configuration data*], and enable DHCP settings included in the DHCP lease information.” 3:21-33; EX-1003 ¶148).

and before sending a data packet into the telecommunications network, selecting a port number in the range of port numbers defined by the port mask, (*See Fangman* “After the registration, IP communications may be performed using the IP telephone, using one or more ports in the range of assigned ports.” 3:60-63. “Thus in step 410 the user may place and receive calls using the IP telephone 120, where the system, e.g., the SG 170 may mediate IP communications between the IP telephone and an IP device, and where the IP telephone uses at least a subset of the range of port numbers to send or receive the IP communications [*selecting a port number in the range of port numbers defined by the port mask*].” 15:67-16:5; EX-1003 ¶149).

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. (*See Fangman* “In one embodiment, performing IP communications using the IP telephone may include the Service Gateway receiving a data packet from the IP telephone, including a private source IP address, a source port number in the assigned range of port numbers, and destination information associated with

an IP device. The Service Gateway may then perform a Network Address Persistent Port Translation (NAPPT) on the data packet, and send the data packet to the IP device. Performing NAPPT on the data packet may include changing the private source IP address to a public source IP address [*primary address*] while leaving the source port number unchanged, and where the public source IP address [*source address*] and the source port number [*selected port number*] may be used to uniquely identify the IP telephone.” 3:66-4:11. “The Service Gateway 170 (as a NAT service) may change the IP source address, e.g., from private to public, but leave the port information unmodified.” 17:13-15; EX-1003 ¶150).

Claim 13

Fangman anticipates or renders obvious **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.** Based on the disclosure in *Fangman* that port ranges are used to identify the private address of an IP telephone device that shares a public address with other devices, a POSA understood that a packet would be rejected if the port number identified in the packet did not belong to the range of port numbers defined by the port range of any

device. EX-1003 ¶xx. Furthermore, it would have been obvious to a POSA to modify *Fangman*, to discard or reject packets received having port numbers outside the defined port range. A POSA would have been motivated to make the modification in order to enforce the mapping and unique identification of the IP telephone device, that enables the use of a common public IP address. A POSA would have had a reasonable expectation of success given the routine practice of rejecting miss-addressed packets. EX-1003 ¶151

Claim 17

Fangman anticipates or renders obvious **a non-transitory computer-readable medium encoded with program code instructions executable by a microprocessor to perform the method according to claim 11.** (See *Fangman* “The system preferably includes a memory medium on which software according to an embodiment of the present invention may be stored. The term “memory medium” is intended to include an installation medium, e.g., a CD-ROM, floppy disks, or tape device; a computer system memory or random access memory (RAM) such as DRAM, SRAM, EDO RAM, RRAM, etc.; or a non-volatile memory such as a magnetic media, e.g., a hard drive, or optical storage. The memory medium may include other types of memory as well, or combinations thereof. In addition, the memory medium may be located in a first computer in which the software program is stored or executed, or may be located in a second

different computer which connects to the first computer over a network, such as the Internet. In the latter instance, the second computer provides the program instructions to the first computer for execution. Also, the computer system may take various forms, including a personal computer system, mainframe computer system, workstation, network appliance, Internet appliance, personal digital assistant (PDA), television set-top box, or other device. In general, the term “computer system” can be broadly defined to encompass any device having at least one processor which executes instructions from a memory medium, or any device which includes programmable logic that is configurable to perform a method or algorithm.” *Fangman* 30:62-31:19; EX-1003 ¶152).

Claim 14

Fangman anticipates or renders obvious Claim 14 for at least the reasons set forth above with respect to Claim 11.

D. Secondary Considerations

This Request demonstrates that Claims 1-3 and 5-17 of the '369 Patent are unpatentable as anticipated by or obvious in view of the prior art references. Applicant did not identify any evidence of secondary considerations during prosecution, and the clear teachings in the prior art cannot be overcome by any supposed “secondary considerations.”

V. DISCLOSURE OF CONCURRENT LITIGATION AND ADMINISTRATIVE PROCEEDINGS

Based on publicly available information, the '369 Patent has been the subject of the following litigations, each of which remain pending at the time of this filing:

Monarch Networking Solutions, LLC v. Juniper Networks, Inc., Case No. 1:23-cv-670 (EDVA).

Requester is not a party to or otherwise involved in any of the above proceedings.

Based on publicly available information, the '369 Patent has not been the subject of any prior or current reexaminations or post-grant proceedings. Requester is unaware of any other proceedings involving the '369 Patent.

VI. CONCLUSION

The Commissioner is hereby authorized to charge Deposit Account 50-6990 the *Ex Parte* Reexamination fee of \$13,080 under 37 C.F.R. § 1.20(c)(2) and § 1.20(c)(3). Requester believes no other fee is due with this submission, however the Commissioner is hereby authorized to charge any fee deficiency or credit any over-payment to Deposit Account 05-6990.

Please direct all correspondence in this matter to the undersigned.

Dated: October 23, 2023

Respectfully submitted,

By: /D. Joseph English/
D. Joseph English
USPTO Reg. No. 42,514
Duane Morris LLP
901 New York Ave. NW,
Suite 700 East
Washington, D.C. 20001-4795
djenglish@duanemorris.com

Patrick Craig Muldoon*
USPTO Reg. No. 47,343
Duane Morris LLP
901 New York Ave. NW,
Suite 700 East
Washington, D.C. 20001-4795
pcmuldoon@duanemorris.com

ATTORNEYS FOR REQUESTER

**Not admitted in D.C. Practice in
D.C. limited to matters and
proceedings before the U.S. Patent
and Trademark Office and federal
courts.*

CERTIFICATION OF SERVICE ON PATENT OWNER
AT ITS ADDRESS OF RECORD (37 CFR 1.33(C))

Pursuant to 37 C.F.R. § 1.510(b)(5), the undersigned certifies that on the 23th day of October 2023, a complete and entire copy of this Request for Reexamination of U.S. Patent No. 8,693,369 and all supporting exhibits were served via Federal Express, postage prepaid, to Patent Owner by serving the correspondence address of record for the '369 Patent in accordance with 37 C.F.R. § 1.33(a) and (c):

NOBLITT & NEWSON, PLLC (Acacia)
Daniel J. Noblitt
8777 NORTH GAINES CENTER DRIVE, STE. 175
Scottsdale, AZ 85258
UNITED STATES

By: /D. Joseph English/
D. Joseph English
USPTO Reg. No. 42,514
Duane Morris LLP
901 New York Ave. NW,
Suite 700 East
Washington, D.C. 20001-4795
djenglish@duanemorris.com