

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

JUNIPER NETWORKS, INC.,
Petitioner,

v.

MONARCH NETWORKING SOLUTIONS, LLC,
Patent Owner.

Case IPR2024-00175
Patent 8,693,369

**PATENT OWNER'S RESPONSE
TO PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 8,693,369**

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

EXHIBIT LIST

Exhibit	Description
EX2001	Declaration of Daniel Minoli in Support of Patent Owner's Preliminary Response
EX2002	<i>Curriculum Vitae</i> of Danieal Minoli
EX2003	RFC 793 ("Transmission Control Protocol") (Sept. 1981), available at https://datatracker.ietf.org/doc/html/rfc793
EX2004	RFC 768 ("User Datagram Protocol") (Aug. 1980), available at https://datatracker.ietf.org/doc/html/rfc768
EX2005	RFC 1933 ("Transition Mechanisms for IPv6 Hosts and Routers") (Apr. 1996), available at https://datatracker.ietf.org/doc/html/rfc1933
EX2006	RFC 1631 ("The IP Network Address Translator (NAT)") (May 1994), available at https://datatracker.ietf.org/doc/html/rfc1637
EX2007	RFC 2663 ("IP Network Address Translator (NAT) Terminology and Considerations") (Aug. 1999), available at https://datatracker.ietf.org/doc/html/rfc2663
EX2008	Decision Ordering Reexamination, No. 90/015,315 (Jan. 18, 2024)
EX2009	PTO Reexamination Statistics, available at https://www.uspto.gov/sites/default/files/documents/reexamination-op-stats.pdf (last accessed Feb. 20, 2024)
EX2010	U.S. Pat. Pub. 2002/0141389 to Fangman <i>et al.</i>
EX2011	RFC 2460 ("Internet Protocol, Version 6 (IPv6) Specification") (Dec. 1998), available at https://datatracker.ietf.org/doc/html/rfc2460
EX2012	Declaration in Support of Motion for <i>Pro Hac</i> Vice Admission of William B. Collier, Jr.
EX2013	RFC 1010 ("Assigned Numbers") (May 1987), available at https://datatracker.ietf.org/doc/html/rfc1010

Exhibit	Description
EX2014	Declaration of Daniel Minoli in Support of Patent Owner's Response

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Background.....	2
	A. The State of the Art.....	2
	1. The Internet Protocol	2
	2. The '369 Patent	5
	B. Effective Filing Date of the '369 Patent.....	8
	C. Level of Ordinary Skill in the Art.....	8
	D. Petitioner's References	9
	1. Biswas [EX1022]	9
	2. Kumar [EX1023].....	10
	3. Fangman [EX1024].....	12
	4. King [EX1025].....	13
	5. RFC 791 [EX1026]	15
III.	Claim Construction	15
IV.	Arguments	15
	A. Ground 1: Biswas In View Of Kumar Does Not Disclose Or Render Obvious The Claims of the '369 Patent.	16
	1. Biswas In View Of Kumar Does Not Disclose Or Render Obvious The Use Of A Routing Device Identifier (8, 12)	16
	B. Grounds 2 and 4: Fangman Does Not Teach Or Suggest All Elements Of Independent Claims 1, 5, and 6 Of The '369 Independent Claims	20
	1. Fangman Does Not Disclose “Determining A Port Mask Assigned To The Destination Equipment...” And “Selecting At	

Least One Identifier...Based On The Port Mask” (1[A], 1[B], 5[A], 5[B], 6[A], 6[B])	20
2. Fangman In View Of Kumar Does Not Render Obvious The Use of Port Masks	25
C. Grounds 3 and 5: King Does Not Teach Or Suggest All Elements Of Independent Claims 1, 5, and 6 Of The '369 Independent Claims	27
1. King Does Not Disclose “Determining A Port Mask Assigned To The Destination Equipment...” And “Selecting At Least One Identifier...Based On The Port Mask” (1[A], 1[B], 5[A], 5[B], 6[A], 6[B]).....	28
2. King Does Not Disclose “Routing The Packet To The Destination Equipment Based On Said Identifier” (1[C], 5[C], 6[C])	31
3. King In View Of Kumar Does Not Render Obvious The Use Of Port Masks.....	33
V. Conclusion	35

TABLE OF AUTHORITIES

Cases

<i>Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015)	17
<i>In re Magnum Oil Tools Int’l, Ltd.</i> , 829 F.3d 1364 (Fed. Cir. 2016)	17
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	15

Statutes

35 U.S.C. § 316(e)	17
--------------------------	----

Regulations

37 C.F.R. § 42.100(b)	15
-----------------------------	----

I. Introduction

Petitioner Juniper Networks, Inc. (“Juniper”) filed a Petition (“Pet.”) challenging all claims of U.S. Patent No. 8,693,369 (“the ’369 Patent”) on five grounds. *See* Pet., ii-iii. Because Petitioner has failed to carry its burden to establish obviousness, Patent Owner Monarch Networking Solutions, LLC (“Monarch”) respectfully requests the Board affirm the validity of the ’369 Patent.

Juniper asserts five invalidity grounds, all based on obviousness. Ground 1, which is primarily based on the Biswas reference, fails because neither Biswas nor Kumar teaches the “identifier of a routing device....” element of claims 8 and 12 of the ’369 Patent. Contrary to Petitioner’s assertions, the teachings of Kumar that Petitioner relies on do not describe anything that identifies the routing device as required by the claims.

Grounds 2 and 4, which are primarily based on the Fangman reference, fail because Fangman does not teach that a packet is routed based on a port mask (or even a port range) as required by the independent claims of the ’369 Patent. At best, Fangman describes using a single port, not the claimed port range or mask. Grounds 2 and 4 also fail because a POSITA would not have combined Fangman with the teachings of Kumar.

Grounds 3 and 5 are based primarily on the King reference. These grounds fail because King, like Fangman, does not teach routing a packet based on a port

mask. King also does not teach that a packet is routed with a destination identifier (identified in part by a port mask) as required by the independent claims of the '369 Patent. Grounds 2 and 5 also fail because a POSITA would not have been motivated to combine Fangman with the teachings of Kumar.

II. Background

A. The State of the Art

1. The Internet Protocol

The Internet allows packets of data to be transmitted between remote devices or networks. These packets are sent and received using Internet Protocol (“IP”), and traditionally Internet Protocol version 4 (“IPv4”). EX2014 ¶ 28-29.¹

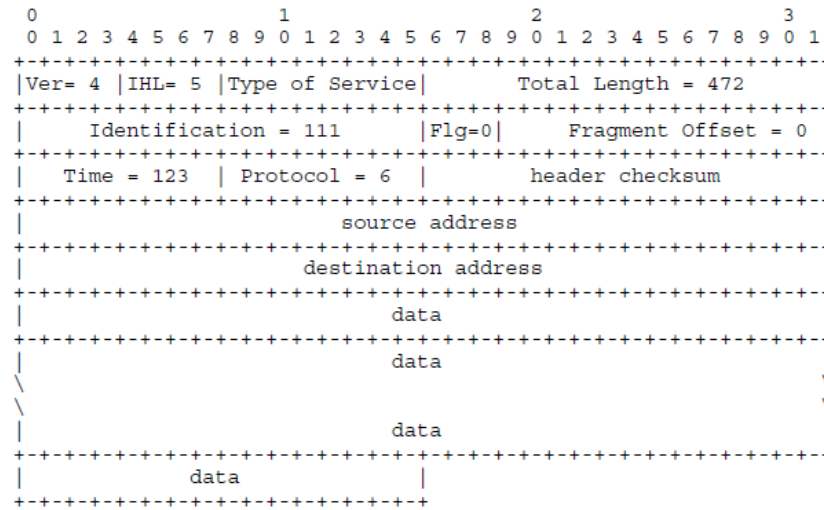
IPv4 defines numerous aspects of the Internet Protocol, including the structure of the IP packets. *See generally* EX1026; EX2014 ¶ 28-29. These packets include a “header” part that carries the information used to transmit data packets to their destinations. EX1026 at 8, 11;² EX2014 ¶ 28-29. The IP header uses “addresses” to identify the source and destination of the packet, typically in the form of 32-bit numbers. EX1026 at 1-2, 11, 14; EX2014 ¶ 28-29.

¹ Monarch withdraws the declaration of Daniel Minoli (EX2001) submitted with the Preliminary Response. *See* 2019 Consolidated Trial Practice Guide at 51.

² All pin citations to exhibits are to the original pagination.

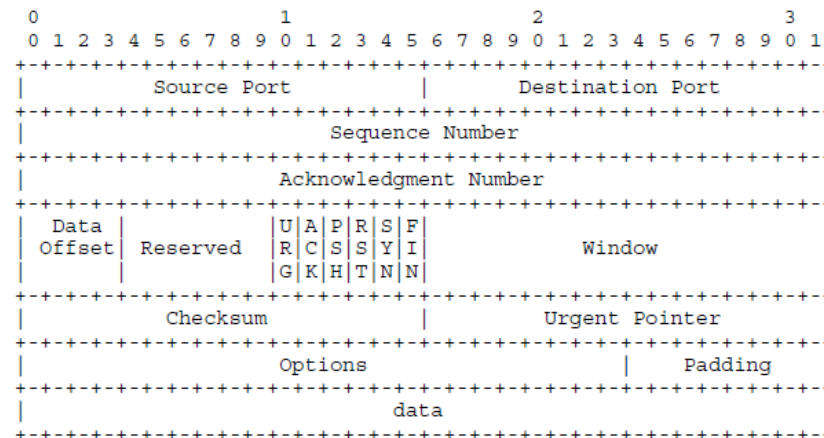
The IPv4 packet also includes a data or payload section carrying the data being transmitted between devices. EX2014 ¶ 28-29. Within the data section, the packet often includes a higher layer protocol such as Transmission Control Protocol (“TCP”) or User Datagram Protocol (“UDP”). *Id.* ¶¶ 30-32. These protocols include their own header information. *Id.* In the case of TCP and UDP, the header includes a source port and a destination port. *Id.* Like IPv4 addresses, the port numbers are typically represented as 16-bit numbers. *Id.* ¶¶ 31-32.

The resulting structure of an IPv4 packet containing a TCP packet is illustrated below (where the TCP packet would be within the data portion of the IPv4 packet):



Example Internet Datagram

Figure 6. (RFC 791)



TCP Header Format

Note that one tick mark represents one bit position.

Figure 3. (RFC 793)

Id. ¶ 31 (citing EX1026, Fig. 6, EX2003, Fig. 3).

In the IP protocol, unique addresses are used to identify individual devices on a network. *Id.* ¶ 33. So any device directly connected to a public IP network, such as the Internet, needs a unique IP address to communicate with the rest of the network. *Id.* IPv4 provides for approximately 4.3 billion unique addresses. *Id.* But by the time

of the '369 Patent, IP practitioners understood that the internet would run out of unique addresses. *Id.*; EX1001, 1:53-54 Those practitioners sought solutions to either avoid exhaustion or replace IPv4 addresses. EX2014 ¶ 33; EX1001, 1:53-54.

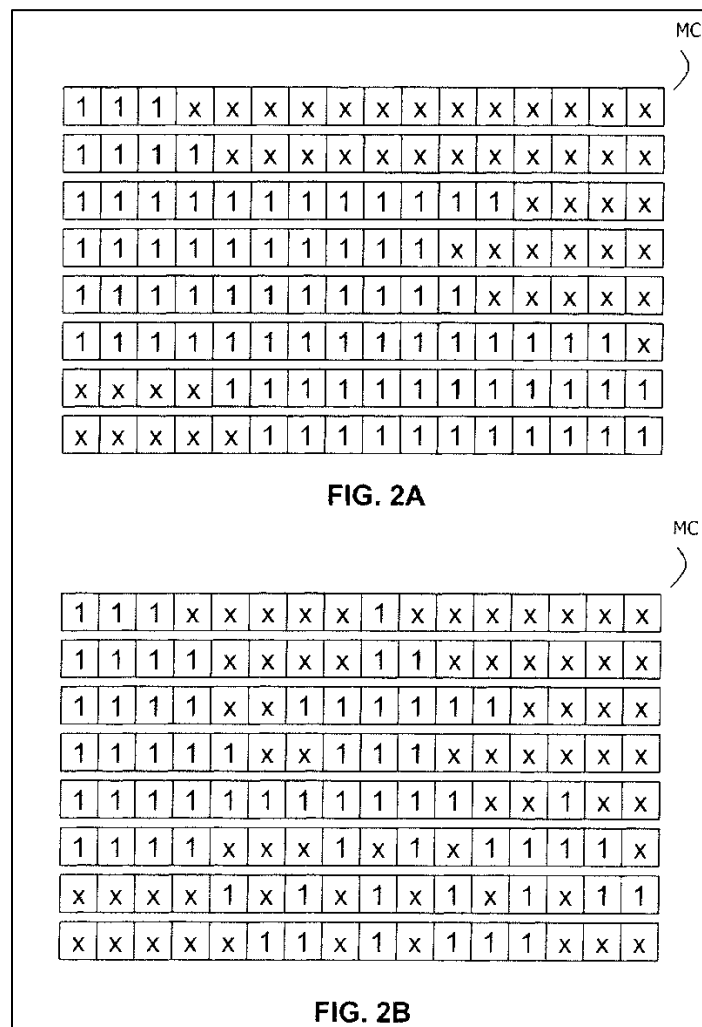
One solution is Internet Protocol version 6 (“IPv6”). EX2014 ¶ 34; EX1001, 1:55-59. IPv6 dramatically increases the available number of addresses by using larger numbers to represent the address, typically represented as a 128-bit value. EX2014 ¶ 34; EX1001, 1:55-59. However, at the time of the '369 Patent, IPv6 adoption was proceeding slowly. *Id.*; EX1001, 1:59-60. Until IPv6 is more widely and universally adopted, other solutions are needed to conserve public IPv4 addresses. *See, e.g.*, EX2014 ¶ 35 (referencing other solutions taken to address the imminent risk of IPv4 address exhaustion); EX1001, 1:67-2:1 (same).

One alternative solution is Operator NAT, which maintains “state tables” associating private IP addresses and port numbers with public IP addresses and port numbers. EX2014 ¶ 35; EX1001, 2:19-41. But Operator NAT has several disadvantages, such as significantly increasing the processing overhead required to route packets. *Id.* ¶ 35; EX1001, 2:19-41.

2. The '369 Patent

Mohamed Boucadair, the inventor of the '369 Patent, sought to alleviate these drawbacks while working at Orange, a French telecommunications company. EX1001, cover, 1:53-54, 2:45-55. One solution described by the '369 Patent is to

provide a shared public address and a portion of the available public port numbers to terminal devices connected to a private network. EX1001, 3:11-29. In this embodiment, the '369 Patent describes assigning and transmitting port masks from an edge router to a terminal device. EX1001, 7:29-32. These port masks represent a range or set of port numbers. EX1001, 7:49-67. Examples of port masks are illustrated in Figs. 2A and 2B:



By conveying and maintaining the port range assignments as masks, edge routers using the methods of the '369 Patent can significantly reduce overhead. EX2014

¶ 41. For example, this technique allows the terminal devices to use public IP addresses and a set (or range) of port numbers when transmitting a packet. EX1001, 4:65-66, 7:32-35; EX2014 ¶ 41. This way, the edge router does not need to perform NAT on the packet before sending it into the public network, simplifying packet routing. EX2014 ¶ 41; *see* EX1001, 2:15-23, 3:18-23, 8:57-67 (similar).

The '369 Patent has seven independent claims that fall into two categories. EX2014 ¶ 42. The first group of independent claims are 1, 5, and 6. *Id.*; EX1001, 14:15-15:2. These claims are directed to methods and devices that route a packet to a destination device based on determining a port mask assigned to the destination device. EX2014 ¶ 42; EX1001, 14:15-15:2. The second group includes independent claims 7, 10, 11, and 14. EX2014 ¶ 42; EX1001, 15:3-16:44. These claims are directed to methods and devices that assign a port range to a device in the form of a mask and transmitting the mask to the device. EX2014 ¶ 42 EX1001, 15:3-16:44. Claims 1 and 7 are presented below, using the same annotations as Petitioner:

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

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

1[b] selecting at least one identifier of the destination equipment of the packet from a plurality of equipment identifiers associated

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

1[c] routing the packet to the destination equipment based on said identifier.

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

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

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

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

EX1001, 14:15-28; 15:3-15 (annotations added). *See also* Pet., viii-xi (same).

B. Effective Filing Date of the '369 Patent

The '369 Patent claims priority to March 31, 2008, and issued on April 8, 2014. EX1001, cover. Petitioner does not dispute that the priority date of the '369 Patent is March 31, 2008. Pet., 8.

C. Level of Ordinary Skill in the Art

For purposes of this proceeding, Patent Owner does not contest Petitioner's recitation of the level of skill in the art, because even under the proposed level of skill (Pet., 14), Petitioner has failed to demonstrate that the claims of the '369 Patent

are invalid. Patent Owner reserves the right to propose its own definition of a person of ordinary skill in the art in the future if necessary.

D. Petitioner’s References

Petitioner asserts five grounds of invalidity based on combinations of five references: (1) Biswas; (2) Kumar; (3) Fangman; (4) King; and (5) RFC 791.

Ground	Claims	Statute	References
1	7-14 and 16-17	§ 103	Biswas and Kumar
2	1-3, 5-6, and 15	§ 103	Fangman and Kumar
3	1-3, 5-6, and 15	§ 103	King and Kumar
4	4	§ 102	Fangman, Kumar, and RFC 791
5	4	§ 103	King, Kumar, and RFC 791

Pet., 4.

1. Biswas [EX1022]

Biswas is U.S. Patent No. 8,019,889, titled “Method and apparatus for making end-host network address translation (NAT) global address and port ranges aware.” EX1022, cover. It describes methods for assigning public addresses and port ranges, and handling packets with those addresses embedded in the packet payload. *Id.*, 2:23-33; EX2014 ¶ 46.

Like the ’369 Patent, Biswas recognized the imminent exhaustion of public IPv4 addresses. EX2014 ¶ 57; EX1022, 1:22-2:19. Biswas also recognized the drawbacks of existing address conservation techniques, such as NAT. EX2014 ¶ 47;

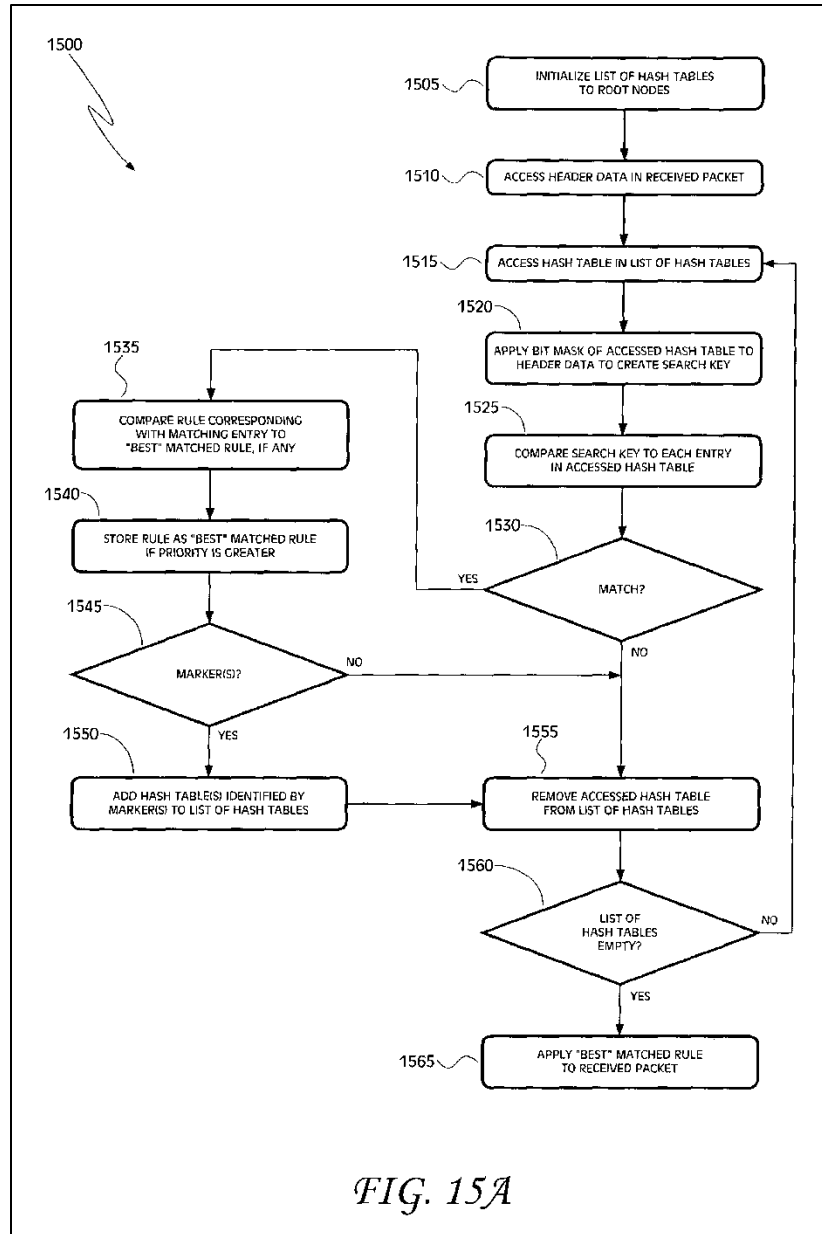
EX1022, 2:3-19. To avoid these drawbacks, Biswas describes an edge router that can assign a “Global Address” and, optionally, a “Global Port Range” to a host device of a private network. EX2014 ¶ 47; EX1022, 2:23-33. The global address and port from the global port range can be used by the host device as an embedded source address and port for a packet that is transmitted to another device on a public IP network. EX2014 ¶ 47; EX1022, 2:23-33.

Petitioner acknowledges that Biswas does not describe port masks or their use, unlike the relevant claims of the '369 Patent. Pet., 22; *also* EX2014 ¶ 49. As Petitioner notes, Biswas also does not describe “how [an] edge router [] determines whether a destination port is within one of its stored port ranges.” Pet., 24.

2. Kumar [EX1023]

Kumar is U.S. Patent No. 7,394,809, titled “Method and apparatus for packet classification using a forest of hash tables data structure.” EX1023, cover. Kumar relates to methods of classifying packets in a “packet classifier” for managing Quality of Service (“QoS”) or security considerations. *Id.*, 1:20-24, 2:57-65; EX2014 ¶ 50. More specifically, Kumar describes methods of creating a “forest of hash tables data structure” using bit masks corresponding to rules and using those rules to classify packets into various categories. EX1023, Abstract; EX2014 ¶ 50.

Kumar’s process for generating a database for sets of rules and identifying a “best” match for an arriving packet is illustrated by Fig. 15A:



EX2014 ¶ 51; EX1023, 7:4-14, Fig. 15A.

Unlike the '369 Patent, Kumar does not discuss IP address conservation. EX2014 ¶ 52-53. Instead, Kumar focuses on “classifying packets.” *Id.* ¶ 53; EX1023, 1:35-65. Kumar does not directly compare a port number in a received packet to a port mask but creates a “search key” by applying a bit mask of a hash

table to header data of a packet. EX2014 ¶ 52; EX1023, 19:2-27. That key is compared to each entry of each relevant hash table until a best match is found. EX2014 ¶ 52; EX1023, 19:2-27.

3. Fangman [EX1024]

Fangman is U.S. Patent No. 7,068,647, titled “System and method for routing IP packets.” EX1024, cover. It describes systems and methods for routing voice packets between IP Telephones over a telecommunications network, an environment also known as IP telephony or voice over IP (“VoIP”). *Id.*, Abstract, 1:14-15; EX2014 ¶ 54. In particular, Fangman illustrates a network address persistent port translation (“NAPPT”) technique for translating packets to or from a public IP address to a private IP address. EX1024, Abstract, 4:9-17; EX2014 ¶ 54-55.

To address the existing problems of NAT techniques, see EX2014 ¶¶ 55-56, Fangman describes alternative techniques for initiating IP Telephony connections, particularly the NAPPT technique. *Id.* ¶ 57; EX1024, 3:3-10, 4:28-33. In NAPPT, the private source address is translated to a public address, but the source port is unchanged. EX2014 ¶ 58; EX1024, 18:23-30. The public source address and the “persistent” port can identify the device corresponding to a packet sent back to the private network. EX2014 ¶ 58; EX1024, 18:23-39.

Notably, Fangman does not teach routing a packet based on determining a port range (or port mask) for a packet received at a router. EX2014 ¶ 59. Instead,

Fangman only uses the port number in the packet to identify a destination device, similar to traditional NAT or PAT. *Id.*; EX1024, 18:23-39.

4. King [EX1025]

King is U.S. Patent No. 8,032,639, titled “Apparatus and method for providing data session source device information.” EX1025, cover. It describes a system and methods for providing source device information within a group of devices. *Id.*, 4:34-35, 4:52-57; EX2014 ¶ 60. King’s systems implement packet handling policies as dictated by an Authentication, Authorization and Accounting (“AAA”) administrator or server on packet flows. EX2014 ¶ 60. Specifically, King describes a device that can aggregate source host sessions (a “service aggregation device”) to manage connections between a “community” and a wide area network such as the internet. EX2014 ¶ 60; EX1025, 1:45-59, 5:8-20.

King focuses on the connection and interaction between user devices, customer premises equipment (“CPE”), and the aggregation device. EX2014 ¶ 61. User devices typically access wider networks, such as the Internet, through CPEs. *Id.*; EX1025, 1:22-25. The CPE in turn communicates with an aggregation device, which serves as a gateway to the wider network. EX2014 ¶ 61; EX1025, 1:25-28. To manage the data traffic from the user devices, the aggregation device often needs to apply a “policy” to the traffic from each user device. EX2014 ¶ 61; EX1025, 1:28-

30. These policies can take numerous forms, such as ensuring a device is authorized or a billing method. EX2014 ¶ 61; EX1025, 1:30-33.

These policies can be obtained from a management device. EX2014 ¶ 62; EX1025, 2:22-24, 2:40-48. To obtain the right policy, the aggregation device must identify the correct user device. EX2014 ¶ 64; EX1025, 2:16-18. According to King, this can present challenges, especially when port translation is used at the CPE before a packet is sent to the aggregation device. EX2014 ¶¶ 63-64; EX1025, 3:42-44, 3:53-4:2.

So, in King's system, the CPE and aggregation device are both able to access a common database assigning public IP addresses and a range of usable ports to the user device. EX2014 ¶ 64; EX1025, 5:28-42. By referencing this table, the aggregation device can identify the source of a packet (in the form of "source identifier information") and obtain correct policy information from the management device. EX2014 ¶ 64; EX1025, 5:36-56.

Unlike the '369 Patent, King does not describe the transmission of a packet based on the derived identity of the destination device. EX2014 ¶ 65. Instead, only the identity of the source device is sent (without the corresponding packet) to the management device, which returns policy information based on the user information. *Id.* King also does not use destination addresses or ports in its method, nor does it describe port masks. *Id.*

5. RFC 791 [EX1026]

RFC 791 is titled “DARPA Internet Program Protocol Specification.” EX1026, cover, 1. It specifies that Standard Internet Protocol developed for the Department of Defense. *Id.*, iii (Preface). RFC 791 describes a model of the Internet transmission path and provides the general specification for the IP, such as the header format. EX1026, 11 (“3.1. Internet Header Format”).

III. Claim Construction

Claims are construed according to *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). *See* 37 C.F.R. § 42.100(b). Petitioner contends that no terms require construction. Pet., 14. For the purposes of this proceeding, Monarch agrees.

IV. Arguments

The Board should confirm the patentability of the '369 Patent for multiple independent reasons, as described below. Each of petitioner's grounds fail for failing to disclose each and every element of the independent claims of the '369 Patent. Regarding Ground 1, neither Biswas nor Kumar teaches or render obvious the use of the claimed routing device identifier. Contrary to Petitioner's assertions, the teachings of Kumar that Petitioner relies on do not describe anything that identifies the routing device as required by the claims.

Regarding Grounds 2 and 4, Fangman (alone or in combination with Kumar) does not teach or render obvious determining a port mask assigned to a user device or selecting an identifier based on the port mask. Specifically, Fangman does not

teach using port masks or port ranges to route packets to a destination device. Moreover, Fangman and Kumar are directed to different aspects of network transmissions, and a POSITA would not have been motivated to combine them.

Regarding Grounds 3 and 5, King does not render obvious determining a port mask assigned to a destination device or selecting an identifier of the destination device based on the port mask. King also does not render obvious routing a packet using an identifier of a destination device. Specifically, King's teachings focus on identifying a source device, rather than a destination device. Moreover, A POSITA would not be motivated to combine the teachings of King with Kumar, in part because there is no suggestion to combine Kumar's rules database with King's methods to obtain a transmission policy.

A. Ground 1: Biswas In View Of Kumar Does Not Disclose Or Render Obvious The Claims of the '369 Patent.

Petitioner has not carried its burden to establish that claim 7-14 and 17 are obvious over Biswas in view of Kumar. With respect to claims 8 and 12, Petitioner's references do not render obvious the claims "identifier of a routing device" as explained below.

1. Biswas In View Of Kumar Does Not Disclose Or Render Obvious The Use Of A Routing Device Identifier (8, 12)

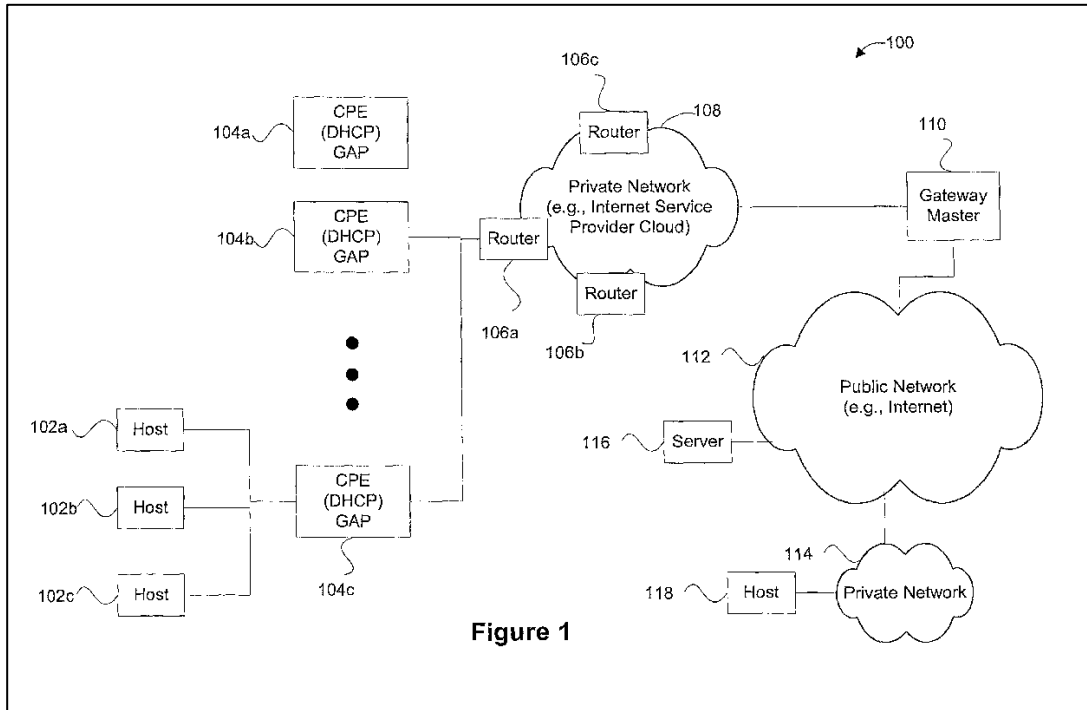
Claim 8 of the '369 Patent depends from claim 7 and claim 12 depends from claim 11. Both claims 8 and 12 require an "identifier of a routing device adapted to

route a data packet comprising said primary address as the destination address to said piece of terminal equipment....” EX1001 15:16-22, 16:7-12. In claim 8, this is also called a “routing device identifier.” *Id.* at 15:16-22.

Petitioner relies solely on Biswas for this limitation. Pet., 27-28. But Petitioner fails to carry its burden to show that Biswas renders obvious the routing device identifier. *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1375 (Fed. Cir. 2016) (“In an inter partes review, the burden of persuasion is on the petitioner to prove “unpatentability by a preponderance of the evidence,” 35 U.S.C. § 316(e), and that burden never shifts to the patentee.” (quoting *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015))).

Petitioner contends that Biswas’s gateway master 110 discloses the “routing device” and Biswas’s global address teaches the “routing device identifier.” Pet. at 28, 33-34. To support this conclusion, Petitioner incorrectly contends that a POSITA would understand that Biswas’s “global address” is an “identifier” of the gateway master 110. *Id.*

Biswas describes the function of three groups of devices (hosts 102a-c, edge routers 104a-b, and gateway master 110) in the illustrative network of figure 1:



EX1022 Fig. 1. Biswas explains edge routers 104 assign a “Global Address,” and, optionally, a “Global Port Range” to a host device 102 of the private network. EX2014 ¶ 72; EX1022, 2:23-33, 6:37-40. The assigned global address and global port range can be transmitted to a host device in a dynamic host configuration protocol (“DHCP”) reply or similar transmission. EX2014 ¶ 72; EX1022, 2:52-59. Upon reception, the global address and a port from the global port range are used by the host device in a packet sent to a device on a public IP network, as either an embedded or translated source address and port. EX2014 ¶ 72; EX1022, 2:23-33.

Importantly, gateway master 110 does not assign the global address. Instead, that address is assigned by, and belongs to, edge routers 104. EX2014 ¶ 72; EX1022 6:37-40 (“The edge routers 104 may be provisioned such that each edge router in the

private network 108 has a unique and non-overlapping global address (GA) and global port range (GPR).”). The host 102 then uses the address as a *source* address for a packet sent out of the private network. EX2014 ¶ 72; EX1022, 6:37-49, 11:25-12:19. In this embodiment, the global address identifies either the host 102 or edge router 104 (the source of the packet), not master gateway 110.

When sending a packet within Biswas’s private network, the host 102, edge router 104, and gateway master 110 must use private addresses to route the packets through the network. EX2014 ¶¶ 73-74; EX1022, 6:12-19. But the global address is a public address that cannot route packets in the private network. EX2014 ¶¶ 73-74; EX1022, 6:12-19. As a result, the global address cannot identify gateway master to any device within the private network, even if it could be used as a destination address outside the network.

Accordingly, in both internet and intranet transmissions from the host device, the global address cannot identify master gateway 110, as petitioner argues. Nothing else in Biswas suggests that the Global Address could identify gateway master 110 to host 102, edge 104, or any other device on the private network. Accordingly, Biswas’s Global Address cannot teach the claimed “identifier of a routing device” of claims 8 and 12.

B. Grounds 2 and 4: Fangman Does Not Teach Or Suggest All Elements Of Independent Claims 1, 5, and 6 Of The '369 Independent Claims

In both Grounds 2 and 4, Petitioner relies on Fangman (in view of Kumar) to allege obviousness of certain claims of the '369 Patent. Pet., 38-53, 66-69. Specifically, the Petition alleges “Fangman’s teachings disclose an edge router that implements a method for configuring a piece of terminal equipment connected to a telecommunications network, including by assigning a piece of terminal equipment a shared primary address, a range of port numbers dedicated to it, and a routing identifier.” Pet., 41. But, Fangman does not teach using port ranges or port masks to route packets to a destination device, as required by claims 1–5, 6, and 15 of the '369 Patent. Moreover, Fangman and Kumar are directed to different aspects of network transmission, and a POSITA would not have been motivated to combine them.

1. Fangman Does Not Disclose “Determining A Port Mask Assigned To The Destination Equipment…” And “Selecting At Least One Identifier…Based On The Port Mask” (1[A], 1[B], 5[A], 5[B], 6[A], 6[B])

Independent claims 1, 5, and 6 claim, in part, a process where an edge router receives a packet and determines whether or not the destination port number in the packet falls within a ranges of port numbers assigned a terminal device connected to the router. The determination is made using port masks that correspond to the assigned ranges. Specifically, element 1[a] recites “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.” EX1001, 14:20-22. Claim element 1[b] also requires “selecting at least one identifier of the destination equipment of the packet . . . based on the port mask”. *Id.*, 14:23-26. Claims 5 and 6 include similar limitations from the perspective of “a device for routing an IP data packet . . .” and “telecommunications network equipment . . .” *Id.*, 14:46-53, 14:60-67. Petitioner’s analysis for claims 5 and 6 primarily refers to the analysis for claim 1. *See* Pet., 52-53.

Petitioner relies on Fangman alone for this limitation and focuses on Fangman’s description of the routing functions of a service gateway. Pet., 43-45.

The majority of Fangman’s disclosure focuses on the initial setup of an IP telephony connection. EX2014 ¶¶ 78; EX1024, 16:64-17:3, 17:21-25. Fangman explains that a service gateway can assign a range of ports to an IP telephone (i.e., a terminal device). EX2014 ¶ 78; EX1024, 16:64-17:3, 17:21-25 (discussing port allocation in the context of a DHCP process). But Fangman only briefly discusses handling packets received at the service gateway. This discussion is quoted below:

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

destination IP address to a private destination IP address while leaving the destination port number unchanged. Note that in this embodiment, the private IP address may be an IP address of the IP telephone **120**. After NAPPTing the data packet, the SG **170** may send the data packet to the IP telephone **120**.

EX1024, 18:31-47; EX2014 ¶ 79. Above, Fangman first describes the contents of a packet received at service gateway 170 (i.e., that it may include “[1] a public destination IP address, [2] a destination port number; and [3] 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**.”). EX1024, 18:31-36; EX2014 ¶ 79. Fangman then explains how this packet may be handled: “In one embodiment, the public destination IP address and the destination port number may be used to uniquely identify the IP telephone **120**.” EX1024, 18:37-39; EX2014 ¶ 79. Focusing on the destination port number, Fangman teaches that the packet includes a port number within the range assigned to the destination IP telephone. EX2014 ¶ 79. The port number may be used to identify the destination IP telephone. *Id.*

This is part of Fangman’s Network Address Persistent Port Translation (“NAPPT”), and it relies on a “persistent” port number to transmit packets between networks. *Supra* § II.D.3; EX2014 ¶ 80-81. Using this technique, the service gateway checks whether the persistent *port number* in the destination packet matches the port number used by the IP telephone in a prior outgoing transmission. EX2014 ¶¶ 81-83; EX1024, 18:31-47. But by using a single persistent port, NAPPT

does not teach or suggest that the destination *port range* (or a port mask) is used to identify the destination IP telephone as required by these claims. EX2014 ¶ 79-81.

Despite this, Petitioner points to several statements in Fangman that allegedly teach these claim elements. Pet., 44-45. These are misstatements or misquotes of Fangman. *See* EX2014 ¶¶ 82-84. In each instance, Petitioner conflates Fangman’s treatment of outgoing packets or initial setup (dealing with *source* addresses and *source* ports) with an incoming packet (handling *destination* addresses and *destination* port). *See id.*

Petitioner first states that “Fangman explains that to perform NAPPT on received data packets, the service gateway ‘maintain[s] a table’ that ‘map[s]’ the port range assigned to an IP telephone to its internal (or “private”) IP address.” Pet. 44 (citing EX1024, 8:45-58, 10:66-67, 11:14-15). Petitioner concludes that a POSITA would understand that the “service gateway 170 consults its mapping table to determine ‘the assigned range of port number’ to which the ‘destination port number’ in the IP packet belongs....” Pet., 44. This is a misreading of Fangman. EX2014 ¶¶ 82-83.

The cited section explains that the service gateway 170 “may allocate a range of port numbers for each IP telephone 120 as it acquires its lease during a DHCP process....” EX1024, 8:45-48; EX2014 ¶ 83. In the next sentence, Fangman suggests that this is separate from the NAPPT process, which “maintain[s] a table of semi-

permanent mapping of the external IP address and ports to the internal hosts and ports.” EX1024, 8:49-51; EX2014 ¶ 83. Fangman then says the port information may be validated “to ensure the correct internal host is using its assigned port range.” EX1024, 8:55-56; EX2014 ¶ 83. The validation occurs on packets sent by IP telephone **120** and validates the *source* port number. EX2014 ¶ 83; *see* EX1024, 8:51-56 (similar). Nothing in Fangman suggests validation of the *destination* port number. EX2014 ¶ 83; *see also* EX1024, Fig. 6C (illustrating that NAPPT does not change the source port in step 638). This disclosure cannot teach or render obvious “determining a port mask assigned to the *destination equipment*, the port mask defining a range of port number to which the *destination port number* belongs.” EX2014 ¶ 83; EX1001, 14:20-22.

Petitioner and its expert also point to columns 10 and 11 of Fangman. Pet. 44. But those sections only describe capabilities in the service gateway used in the initialization and DHCP process. EX2014 ¶ 84; EX1024, 10:20-11:67. They say nothing about how Fangman’s service gateway routes incoming packets.

In sum, nothing in Fangman teaches using a destination port range (or mask) to determine a destination for a packet as required by claims 1, 5, and 6. EX2014 ¶ 85. To the extent that Fangman discusses port ranges, it is only in the context of assigning source ports for outgoing transmissions. Petitioner and its expert never acknowledge the difference in Fangman’s treatment of source and destination ports.

Nor do they explain why a POSITA would be motivated to modify Fangman's handling of destination ports to apply the teachings related to source ports. As explained above, when handling a return packet, Fangman teaches consulting the port number stored in its NAPPT table to identify a destination device. Nothing in Fangman suggests that a port range (or mask) is used in the NAPPT process to identify a destination device. *Id.* In fact, Fangman confirms that it uses only a port number in NAPPT. *Id.* ¶ 86; EX1024, 18:39-42 (“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....” (emphasis added)).

2. Fangman In View Of Kumar Does Not Render Obvious The Use of Port Masks

Petitioner has not carried its burden on Grounds 2 and 4 for the additional reason that Fangman does not disclose the use of port masks at all, and a POSITA would not combine the teachings of Fangman with those of Kumar. As noted above, claims 1, 5, and 6 include similar limitations that require the use of port masks. Petitioner's analyses for claims 5 and 6 primarily refer to the analysis for claim 1. Pet., 52-53.

Petitioner acknowledges that Fangman does not describe using a port mask to define a range of ports. Pet., 45. Instead, Petitioner contends that Fangman would be combined with the teaching of Kumar to render the element obvious. *Id.* But, Petitioner fails to show that a POSITA would combine the two references.

As explained above, Fangman does not use port ranges to identify the destination of a packet. *See supra* § IV.B.1; EX2014 ¶ 89. Petitioner and its expert have not provided any reason to replace a single port number with a port mask. EX2014 ¶ 89.

Regardless, Petitioner has not carried its burden to show a POSITA seeking to implement the routing method of Fangman would look to Kumar. Unlike Fangman, which as explained above, describes techniques for establishing IP telephone connections, Kumar addresses policies in a packet classifier, such as in a firewall. *Id.* ¶ 90. As noted above, firewall packet handling deals with traffic flow management, not IP telephony or connection setup and management. *Id.* Kumar does not address the complexities or processes involved with IP telephony. *Id.* Accordingly, a POSITA would not look to Kumar when seeking to improve the system of Fangman for the purpose of IP address conservation. *Id.*

Petitioner also has not explained how the system of Kumar would provide any benefit to the IP telephony system of Fangman. *Id.* ¶ 91. As noted above, Kumar describes a complex hierarchical data structure comprised of a “forest of hash tables.” EX1023, Abstract, 10:27-47; EX2014 ¶ 91. When an IP packet arrives at Kumar’s packet classifier, the header, rather than only the port number, is converted to a “search key” using an “AND” operation with the bit mask of a hash table. EX1023, 19:2-10; EX2014 ¶ 91. This search key is compared to every hash table.

EX1023, 19:11-18; EX2014 ¶ 91. This process continues with each hash table until a match is found. EX1023, 19:36-40; EX2014 ¶ 91. As a result, Kumar adds significant processing demands that would burden Fangman's NAPPT system. EX2014 ¶ 91. A POSITA would not implement the Kumar system in Fangman and increase the complexity of Fangman. Accordingly, Petitioner has not shown that a POSITA would combine Fangman and Kumar to render claims 1, 5, and 6, or their dependents, obvious.

C. Grounds 3 and 5: King Does Not Teach Or Suggest All Elements Of Independent Claims 1, 5, and 6 Of The '369 Independent Claims

In Grounds 3 and 5 rely, Petitioner asserts that King (in view of Kumar) renders obviousness certain claims of the '369 Patent. Pet. at 53-66, 69-70. Specifically, Petitioner alleges "King's teachings disclose intermediary devices that assign user devices a shared primary address, a range of port numbers dedicated to it, and a routing identifier." *Id.* at 55. However, King does not disclose several elements of independent claims 1, 5, and 6 of the '369 Patent.

King's teachings focus on identifying a source device, not a destination device. Thus, King does not render obvious determining a port mask assigned to a destination device or selecting an identifier of the destination device based on the port mask. King also does not describe routing a packet using an identifier of a destination device. Moreover, A POSITA would not be motivated to combine the

teachings of King with Kumar, because a POSITA would not look to Kumar to improve the teachings of Kumar.

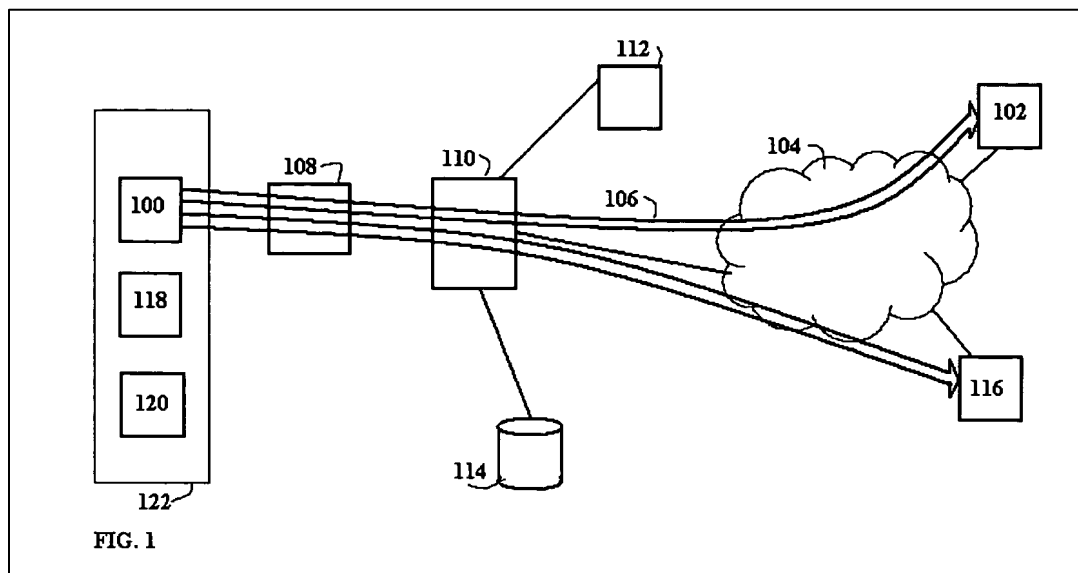
1. King Does Not Disclose “Determining A Port Mask Assigned To The Destination Equipment…” And “Selecting At Least One Identifier…Based On The Port Mask” (1[A], 1[B], 5[A], 5[B], 6[A], 6[B])

As explained above, independent claims 1, 5, and 6 claim, in part, a process where an edge router receives a packet and determines whether or not the destination port number in the packet falls within a ranges of port numbers assigned a terminal device connected to the router. *Supra* § IV.B.1. As with Fangman, Petitioner relies on King alone for these limitations. Pet. 57-62.

Petitioner’s analysis of King is fundamentally flawed for at least two reasons. *First*, Petitioner conflates **source** port processing with **destination** port processing. *Second*, Petitioner proposes a combination of King’s method to obtain a “policy” with its method of routing a packet. These are fundamentally different processes, and Petitioner fails to explain why a POSITA would make the proposed modifications. As a result, Petitioner has not carried it burden to show King renders obvious the same elements as Fangman for similar reasons. *See supra* § IV.B.1. As with Fangman, Petitioner’s analysis for claims 5 and 6 primarily refers to the analysis for claim 1. Pet., 65-66.

King describes methods for an “aggregation device” to obtain user policy information from a management device, such as an authorization, authentication, and accounting (“AAA”) server. *Supra* § II.D.4. A key improvement is using a table of source address and source port assignments accessible by both the customer premises equipment (“CPE”) and the aggregation device. EX2014 ¶ 95. By knowing the source port range assigned to each device by the CPE, the aggregation device can identify a user device and use that identification to obtain policy information from an AAA server. *Id.*

The system described by King is illustrated in Figure 1:



EX1025, Fig. 1; EX2014 ¶ 96. Figure 1 shows a packet flowing from a first user device **100** to a CPE device **108**, then an aggregation device **110**, and onward to remote devices **102** and/or **116**. EX1025, 1:34-59; EX2014 ¶ 96. When aggregation device **110** receives the packet, aggregation device **110** must know what policy to

apply to the packet, such as a QoS policy or parental control policy. EX1025, 1:28-33; EX2014 ¶ 96. Because aggregation device **110** includes a table with *source* port ranges assigned by CPE device **108**, it can use the *source* port to identify the *source* device and obtain a policy for that device from AAA server **114**. EX1025, 5:63-65, Figs. 6, 7; EX2014 ¶ 96. The packet can then be transmitted using that policy. EX1025, 5:51-57; EX2014 ¶ 96.

This process never uses the *destination* port (i.e., a “port [] assigned to the destination equipment”) required by the ’369 claims. EX2014 ¶ 97. Nothing Petitioner points to in King suggests that the above method could function in reverse, i.e., to identify a policy for a packet transmitted from destination device **102** to user device **100** by using the destination port. *Id.*

Even King’s language that Petitioner points to explicitly uses ports associated with *source* equipment rather than destination ports:

“[T]he CPE may assign TCP port numbers 1024 to 1039 to data sessions **associated with the first user or source device 100** and TCP port numbers 1040 to 1055 to data sessions **associated with the second user or source device 118.**”

“[I]ncoming packets can then be classified ... **based on source port range.**”

“In particular on receipt of a packet with (translated) *source* address IPCPE and (translated) TCP port in the range **1024 to 1039** the aggregation device derives corresponding *source device information.*”

EX1025, 5:28-32, 5:37-38, 5:42-46. *See also* Pet., 55, 58; EX1003 ¶¶ 185, 193-194 (citing EX1025, 5:28-32, 5:32-35, 5:36-42, 5:26-46); EX2014 ¶ 98. Petitioner and its expert never explain why teachings based on the source port would be applied to the destination port. *See* EX2014 ¶ 98.

Accordingly, Petitioner has not shown that King in view of Kumar renders obvious “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” or “selecting at least one identifier of the *destination* equipment of the packet . . . based on the port mask”. EX2014 ¶ 99.

2. King Does Not Disclose “Routing The Packet To The Destination Equipment Based On Said Identifier” (1[C], 5[C], 6[C])

Independent claims 1, 5, and 6 also claim routing a packet to its destination based on the identifier (identified using the destination port mask). Specifically, claim element 1[c] recites “routing the packet to the destination equipment based on said identifier.” EX1001, 14:27-28. Claims 5 and 6 include similar limitations from the perspective of “a device for routing an IP data packet . . .” and “telecommunications network equipment . . .” *Id.*, 14:41-15:2. Petitioner relies exclusively on King and dedicates only a single substantive paragraph to this element for claims 1, 5, and 6. Pet., 63, 65-66.

Like the prior element, Petitioner mis-states King's teachings to support its arguments. Contrary to Petitioner's assertion, King never states that the device identifier information (identified based on the port mask) could be used to route a packet to the destination equipment. EX2014 ¶ 102.

Petitioner argues that King's IP address of a user device would be used to route the packet. Pet., 63. This analysis focuses exclusively on King's description of a prior art system that does not implement the techniques of King. *Compare* EX1003 ¶ 204 (citing EX1025, 2:49-61, 3:2-6, Fig. 5) *with* (EX1025, 1:34-36, 1:60-61, 2:25-28); EX2014 ¶ 102.

King's entire description of this prior art process is found in columns 2 and 3:

In particular at step **500** the user device initiates a service session with its IP address as source identifier and a native data session identifier such as a TCP source port as data session identifier. At step **502** the CPE translates the source address to its own overloaded IP address. At step **504** the CPE additionally translates the TCP source port to its own TCP port in a Port Address Translation (PAT) step as described in more detail below. Then, as step **506**, the CPE forwards returning traffic with the translated overloaded IP address and TCP port to the user device, reinstating the user device IP address as destination address and the user device assigned TCP port number.

EX1025, 2:62-3:6. Petitioner points to the last step above describing that return traffic can be translated and sent to a local device. Pet., 63-64. This return traffic is not otherwise discussed in King. See EX2014 ¶ 102.

Nothing in this process suggests using port ranges or the claimed identifier. Indeed, King teaches away from using the above technique: it is the prior PAT

technique that proved problematic when trying to identifying source devices. EX1025, 3:42-52; *Id.* Petitioner does not explain why a POSITA would combine the prior art technique with the policy identification method of King, or how the source identifier used to obtain policy information from a AAA device would be used to route a packet to its destination equipment. EX2014 ¶ 102.

In sum, King does not teach or suggests “routing the packet to the *destination* equipment based on said identifier [of the *destination* equipment].”

3. King In View Of Kumar Does Not Render Obvious The Use Of Port Masks

Petitioner has not carried its burden on Grounds 3 and 5 for the additional reason that King does not disclose the use of port masks at all, and a POSITA would not combine the teachings of King with those of Kumar. As noted above, claims 1, 5, and 6 each include similar limitations that require the use of port masks. Petitioner’s analyses for claims 5 and 6 primarily refer to the analysis for claim 1. Pet., 65-66.

Petitioner acknowledges that King does not describe using a port mask to define a range of ports. Pet., 59. Instead, Petitioner contends that a POSITA would combine King with the teachings of Kumar to render this element obvious. *Id.* But, Petitioner’s analysis does not support the conclusion that a POSITA would combine the two references. Petitioner cherry-picks Kumar’s discussion of masks without

acknowledging the complexity of implementing Kumar's search methods in King's policy management system. EX2014 ¶ 106-107.

For example, Petitioner has not shown that a POSITA seeking to implement the methods of King would look to Kumar. *Id.* Unlike King, which concerns obtaining a policy from an AAA server, Kumar addresses applying rules in a packet classifier, such as in a firewall. *Id.* ¶ 107. As noted above, firewall packet handling deals with traffic flow management, not IP policy acquisition or routing. Thus, Kumar does not address obtaining policy information from an outside source. *Id.* ¶ 106. Accordingly, a POSITA would not look to Kumar when seeking to improve the system of King for the purpose of obtaining policy information. *Id.* ¶ 106-107.

Petitioner also failed to consider the complexity Kumar's teachings would impose of King. As noted above, Kumar uses a search system where packet headers are converted into search keys. *See, e.g.*, EX1023, 18:65-19:10. Combining these systems would add considerable processing demands that a POSITA would realize increases the complexity of King's method of obtaining a policy from a AAA server. EX2014 ¶ 107. Thus, a POSITA would not implement the Kumar's system in King.

Petitioner's analysis also fails to explain how King and Kumar would be combined or how a POSITA would have a reasonable expectation of success. For example, the petition never explains how the complex forest of hash tables of Kumar would be implemented in King's translation table or policy management system.

Accordingly, Petitioner has not shown that a POSITA would combine Fangman and Kumar to render claims 1, 5, and 6 obvious.

V. Conclusion

Monarch respectfully requests that the Board affirm the validity of the claims if the '369 Patent for the reasons stated herein.

Dated: July 30, 2024

Respectfully submitted,

By: /R. Allan Bullwinkel/
R. Allan Bullwinkel (Reg. No. 77,630)
Attorney for Patent Owner
Monarch Networking Solutions, LLC

CERTIFICATE OF SERVICE

The undersigned certifies that pursuant to 37 C.F.R. § 42.6(e), a copy of the foregoing Patent Owner's Response was served via email to lead and backup counsel of record for Petitioners as follows:

Lead Counsel	Back-Up Counsel
James M. Glass (Reg. No. 46,729) Quinn Emanuel Urquhart & Sullivan, LLP 51 Madison Ave., 22nd Floor New York, New York 10010 Phone: 212-847-7000 Fax: 212-849-7100 jimglass@quinnemanuel.com	Todd M. Briggs (Reg. No. 44,040) Kevin Johnson (Reg. No. 38,927) Quinn Emanuel Urquhart & Sullivan, LLP 555 Twin Dolphin Drive, 5th Floor Redwood Shores, CA 94065 Phone: (650) 801-5000 Fax: (650) 801-5100 toddbriggs@quinnemanuel.com kevinjohnson@quinnemanuel.com Nima Hefazi (Reg. No. 63,658) Quinn Emanuel Urquhart & Sullivan, LLP 865 S Figueroa St 10th Floor, Los Angeles, CA 90017 Phone: (213) 443-3000 Fax: (213) 443-3100 nimahefazi@quinnemanuel.com

Dated: July 30, 2024

Respectfully submitted,
By: /R. Allan Bullwinkel/
R. Allan Bullwinkel (Reg. No. 77,630)
Attorney for Patent Owner
Monarch Networking Solutions, LLC

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d), the undersigned hereby certifies that this brief complies with the type-volume limitation of 37 C.F.R. § 42.24 because this brief contains 7,406 words as calculated by Microsoft Word, excluding the items exempted under 37 C.F.R. § 42.24.

Dated: July 30, 2024

Respectfully submitted,
By: /R. Allan Bullwinkel/
R. Allan Bullwinkel (Reg. No. 77,630)
Attorney for Patent Owner
Monarch Networking Solutions, LLC