

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

**DECLARATION OF DANIEL MINOLI IN SUPPORT OF PATENT
OWNER'S SUR-REPLY 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

TABLE OF CONTENTS

I. Introduction 1

II. Dr. Bhattacharjee’s Theories related to “Unsolicited” PAckets are wrong.....1

III. King Would Not Be Modified To Work In Reverse 7

IV. A Posita Would Not Modify Fangman Or King To Include Port Ranges.....9

V. Conclusion.....11

I, Daniel Minoli, declare as follows:

I. INTRODUCTION

1. My name is Daniel Minoli. I am over eighteen years of age, of sound mind, and qualified to make the statements set forth in this Declaration. With the exception of the legal principles counsel has supplied to me, all the facts and statements contained herein are within my personal knowledge and are in all respects true and correct.

2. I have been asked by Monarch Networking Solutions, LLC (“Monarch” or “Patent Owner”) to submit this declaration in response to the Reply filed by Juniper Networks, Inc. (“Juniper” or “Petitioner”) and the supporting declaration submitted by Dr. Samrat Bhattacharjee (“Bhattacharjee Declaration”) regarding U.S. Patent No. 8,693,369 (“the ’369 Patent”).

II. DR. BHATTACHARJEE’S THEORIES RELATED TO “UNSOLICITED” PACKETS ARE WRONG

3. In his declaration, Dr. Bhattacharjee says that Fangman must be able to handle “unsolicited inbound transmissions.”¹ EX1039 ¶¶13-15. This is wrong. A

¹ I note that the term “unsolicited” is not used in Fangman, and it is not clear what Dr. Bhattacharjee means by it. Every VoIP-related transmission between phones in Fangman requires a session to be established before any data exchange occurs. If by “unsolicited” Dr. Bhattacharjee simply means receiving a phone call, Fangman’s

POSITA would understand that no remote end device (e.g., a device on an “external” network) can communicate to an internal device (e.g., host or terminal device) unless a session has been pre-established with it via a signaling mechanism (such as MEGACO).

4. Dr. Bhattacharjee specifically argues that “if Fangman were to use a process ‘similar to traditional NAT or PAT’ that requires a ‘prior outgoing transmission,’ as Patent Owner assumes, (POR 13, 22), then the IP telephones in Fangman’s network would not be able to receive unsolicited inbound calls.” EX1039 ¶15. Dr. Bhattacharjee uses this proposition to argue that NAPPT in Fangman necessarily routes packets to a destination device using port ranges, rather than port numbers. EX1039 ¶16

5. The only example Dr. Bhattacharjee provides from Fangman of an “unsolicited” transmission is in reference to Figures 10A and 10B. EX1039 ¶17. He describes this disclosure as follows: “in the example provided in Figures 10A and

disclosure supports phone calls, but only needs to use port numbers as seen in FIGs 6A through 10B, not ranges, as I explain in this declaration. As I explain, although in Figures 4A and 4B, port ranges are assigned or registered (e.g., 462, 482, 492), in actual communication, as illustrated in Figures 6A-10B, will only employ a specific port, not a port range or a port mask.

10B, a service gateway **170B** receives an inbound data packet and performs NAPPT on that inbound data packet without first sending a prior outbound packet.” *Id.* He goes on to say that “In this example, the service gateway’s database would not contain information from a ‘prior outgoing transmission’ because there is no prior outgoing transmission. The only way the service gateway could route the data packet in this situation is by using NAPPT to route the inbound data packet based on stored port range.” *Id.*

6. I disagree with this analysis. Dr. Bhattacharjee appears to misunderstand Fangman’s system. In fact, in all instances, a phone operating in Fangman’s system will have already communicated with at least the media gateway controller that manages the public IP address and port number assigned to each registered phone.

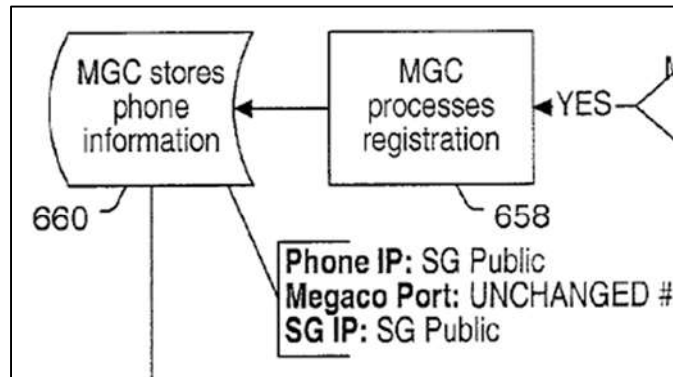
7. In simple terms, a computer on a client network cannot simply receive a packet from the internet, unsolicited. Fangman (EX1024) recognizes this and explains that “the IP telephone may be registered by the system, e.g., by the Media Gateway Controller (“MGC”), prior to the Call Setup process. EX1024 3:53-55. I note that though Fangman says the phone “may” register, every embodiment does in fact teach registering the phones with the MGC.

8. As an initial matter Fangman describes an alternate to traditional address translation called NAPPT, or Network Address Persistent Port Translation.

EX1039 4:9-17. NAPPT as described by Fangman is a process similar to traditional NAT but using a “persistent port number.” EX1024 8:45-57. Fangman states that NAPPT replaces private source IP addresses with “NATed” external IP addresses, but it does not modify port information. *Id.* In Fangman’s embodiments, NAPPT is performed on any packet leaving a private network, via a service gateway (“SG”), to a public network. *See, e.g., id.* 24:26-34

9. In Figures 10A-B that Dr. Bhattacharjee points to, Fangman describes a call by an internal phone to an external phone. EX1039 28:51-56. Though it claims to describe a phone call, the process actually begins with A DHCP-TFTP process (step 404), followed by a client registration process (step 406), and finally a call setup process (step 480), before the call process begins. EX1039 28:61-65. These processes are illustrated in Figures 5A through 7C. Of these, I will focus on the registration process 406 of Figure 6A-C. After an IP Phone has been powered on and the DHCP/TFTP process is complete, *see* Figure 5A-B, the registration process can begin, *Id.* 21:10-16. Following several steps, client device (the phone) selects a port number for signaling and transmits that port number to the MGC, using the NAPPT protocol in the client device’s service gateway (“SG”). *Id.* 21:17-35, 21:48-53. After several more steps, the packet, now with the SG’s public IP address and the client device’s port number, arrives at the MGC. 22:24-32. The MGC processes the registration and stores the registration information. *Id.* The stored information

includes “the IP telephone IP address, denoted as SG Public, referring to the Service Gateway's public IP address for the telephone 120, the MEGACO port, indicated here as UNCHANGED, and the SG IP, indicated as SG Public,” and is illustrated in Figure 6A:



Id. 22:29-32, Fig. 6A. The registration process continues until the registration process is complete. Importantly, the MGC now holds the Public IP address and port number for any phone registered in Fangman’s system.

10. The next step in Figure 10A is the call setup process, which is the beginning of a call from one phone to another, presumably meeting Dr. Bhattacharjee’s definition of “unsolicited”:

In step 702, the client call may begin. In the preferred embodiment, the call may be initiated by a client activating the IP telephone 120, e.g., by picking up the receiver, and dialing a destination telephone number.

EX1039 23:32-35. The process again discusses Fangman's NAPPT packet handling, but importantly, ends with Call Setup data arriving at the IP telephone. *Id.* 25:21-36; *see also id.* Figs. 7A-C.

11. Figures 10A-B then describes a subsequent RTP call “between an internal IP telephone 120A and an external IP telephone 120C, related to a call initiated by the first internal IP telephone 120A.” EX1039 28:53-56. At a first step “the system may determine if the MGC 150 provided a destination IP address and port,” i.e., the destination IP address and unchanged port number for the second phone. *Id.* 29:1-2. This is the information that the second phone 120C would have provided the MGC during its registration process, and the same port information is stored in the second phone's SG. *See* discussion of the registration process above. If the MGC did provide this information, “then in step 1008, the client may transmit an RTP packet to the destination telephone, i.e., IP telephone 120C.” 29:6-7.

12. As the above illustrates, Fangman explains that in the initial outbound packet sent by a first phone to a second, the destination address and destination port were both indicated by a media gateway controller during the call setup process. Since the IP phones in Fangman are already registered with the media gateway controller, a POSITA would understand that in this scenario, the call placed from Phone 1 to Phone 2 uses port numbers that have already been assigned to the respective devices. A truly “unsolicited” transmission from Phone 1 to Phone 2 is

impossible—both phones are registered with a port number at the media gateway controller before any call can take place. A POSITA would not understand Fangman to teach performing NAPPT with port ranges, but would instead understand Fangman to keep a table of port numbers associated with private IP address of telephones on the local network. Note that these figures and the related text in Fangman include additional detail to what I have discussed here, but it does not change my analysis.

III. KING WOULD NOT BE MODIFIED TO WORK IN REVERSE

13. As I explained in my previous declaration (EX2014) King (EX1025) discusses a system and methods for providing session source device information within a community (i.e., a group) of devices. EX1025 4:34-35, 4:52-57. Specifically, King focuses on mechanisms to impose policies as dictated by an Authentication, Authorization and Accounting (“AAA”) administrator or server on packet flows and on 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. *Id.* at 1:45-59, 5:8-19

14. This process is described in King as applying subscriber policies by identifying the subscriber device of a packet travelling from a private network to a public network, such as the internet. *Id.* 1:28-59. Though the process is described in detail, at a high level, it allows policies for a subscribed device to be applied to the

devices communications with the internet. Dr. Bhattacharjee argues that a POSITA would apply this policy identification system in reverse. Ex1039 ¶26. I disagree. As I discussed above with respect to Fangman, a client user device on a private network, such as those in King, would never receive “unsolicited” packets from the internet. Instead, and packet sent towards a user device on the private network would be part of a pre-established session. In this scenario, any policies that needed to be applied to that packet flow would have been identified when the session was initiated by the user device. Hence, even if applying King’s methods “in reverse” is as easy as Dr. Bhattacharjee claims, a POSITA would never attempt to implement that system.

15. Dr. Bhattacharjee also misunderstands the aggregation device 110 described by King. King’s aggregation device does not route packets (e.g., performing the IP routing function) in the sense that it does not perform any sort of NAT or PAT on the packets. King is clear that “since all address or port translation is performed at the CPE device, no such translation or deep packet inspection overheads need to be incurred at the aggregation device itself.” EX1025 6:58-61. The aggregation device simply obtains and “applies the policy to the service session permitting data sessions between the user device and remote entities.” *Id.* 2:47-48. The packet handling policy is effectuated and implemented by the CPE. A POSITA would understand there is no need for Kings aggregation device to provide NAT or PAT services when it was done by the CPE. I also note that Dr. Bhattacharjee states

that King teaches “replacing PAT.” EX1039 ¶27. This is not correct at the technical level and is at best an exaggeration. King describes modifying PAT, where “rather than performing conventional PAT, where outside source ports are assigned indiscriminately across inside PCs, translation is carried out to separate port ranges per host device.” EX1025 5:32-35. In this instance, the modified PAT is still performed by the CPE, not the aggregation device.

IV. A POSITA WOULD NOT MODIFY FANGMAN OR KING TO INCLUDE PORT RANGES

16. In his discussion for both Fangman and King, Dr. Bhattacharjee asserts that even if Fangman and King do not describe using port ranges as claimed by the '369 patent, a POSITA would modify Fangman's NAPPT and Kings already modified NAT and PAT to use port ranges, instead of the port numbers described by King and Fangman.² EX1039 ¶¶23, 28. But these assertions have no bases, outside of the hindsight provided by the '369 Patent. Regardless, I disagree with Dr. Bhattacharjee's conclusion. His analysis glosses over the real technical challenges involved with such a change, especially where the change is unnecessary. A POSITA would recognize that changing from NAT, PAT, NAPT, or NAPPT (as described respectively in King and Fangman) to a system relying on port ranges would

² In any event, '369 utilizes and distributes port masks to define port ranges, not port ranges per se.

fundamentally change how packet translation is handled. This change could introduce complexity and potential unforeseen incompatibility. For example, the '369 Patent recognizes that its teaching may require modification to DHCP. EX1001 10:4-56. To mitigate this risk, a POSITA would limit any changes to NAT-type techniques to those that are absolutely necessary. But, specific techniques described in Fangman and King would limit a POSITA from seeking additional complexity. Fangman describes the dual IP flow and the interaction with the intermediary Media Gateway Controller needed in VoIP. And King describes the policy controls and the interaction needed with the intermediary AAA servers and Service Manager. These interactions can be complex without making additional changes to NAT and the related techniques. A POSITA would also have to take into account how any changes with the NAT, PAT, NAPT, or NAPPT would need to be propagated to the various other network elements that form part of the overall networks of Fangman and King, and those changes would require to validate that them. In environments where relatively few connections need to be maintained, or where there are only insignificant drawbacks to using existing techniques, a POSITA would not consider the change to port ranges suggested by Dr. Bhattacharjee. In fact, both King and Fangman identified a use for port ranges in certain aspects, but neither chose to modify their NAT-like techniques to include port ranges. In both cases, the use of

individual ports in the address translation process was sufficient. The only reason to suggest these changes is hindsight in light of the '369 Patent.

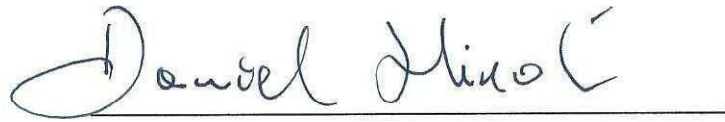
V. CONCLUSION

17. For at least the reasons set forth herein, it is my opinion that Petitioner has failed to show that any of the claims of the '369 Patent are unpatentable over the cited prior art.

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

Executed on December 3, 2024, in Red Bank, New Jersey.

Respectfully Submitted,

A handwritten signature in cursive script, reading "Daniel Minoli", written in dark ink. The signature is positioned above a horizontal line.

Daniel Minoli