

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner

v.

MONARCH NETWORKING SOLUTIONS LLC
Patent Owner

Case IPR2020-01678
U.S. Patent No. 8,451,844

**PATENT OWNER'S PRELIMINARY RESPONSE UNDER 37
C.F.R. § 42.107 TO PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 8,451,844**

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

Patent Owner's Exhibit List

Exhibit	Description
2001	“Let’s Solve IPv4 Address Exhaustion without Stateful CGN,” available at https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2015/pdf/BRKSPG-2606.pdf
2002	“Transition Mechanisms for IPv6 Hosts and Routers,” Network Working Group Request for Comments: 1933 (April 1996), available at https://tools.ietf.org/html/rfc1933
2003	Monarch Networking LLC’s Opening Claim Construction Brief, <i>Monarch Networking Solutions LLC v. Cisco Systems, Inc.</i> , No. 2:20-cv-00015-JRG, ECF No. 88 (E.D. Tex. Oct. 5, 2020)
2004	Defendant Cisco Systems, Inc.’s Responsive Claim Construction Brief, <i>Monarch Networking Solutions LLC v. Cisco Systems, Inc.</i> , No. 2:20-cv-00015-JRG, ECF No. 96 (E.D. Tex. Oct. 21, 2020)
2005	Monarch Networking LLC’s Reply Claim Construction Brief, <i>Monarch Networking Solutions LLC v. Cisco Systems, Inc.</i> , No. 2:20-cv-00015-JRG, ECF No. 103 (E.D. Tex. Oct. 30, 2020)
2006	Claim Construction Order, <i>Monarch Networking Solutions LLC v. Cisco Systems, Inc.</i> , No. 2:20-cv-00015-JRG, ECF No. 128 (E.D. Tex. January 7, 2021)
2007	Excerpt from IBM DICTIONARY OF COMPUTING, ed. George McDaniel, 1994 (definition of “domain”)
2008	U.S. Patent No. 7,245,622
2009	“Dynamic Host Configuration Protocol,” Network Working Group Request for Comments: 2131 (March 1997), available at https://tools.ietf.org/html/rfc2131
2010	“CISCO APPLICATION CONTROL ENGINE MODULE ROUTING AND BRIDGING CONFIGURATION GUIDE, Chapter 5 - Configuring the DHCP Relay,” available at https://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/ace/v3-00_A2/configuration/rtg_brdg/guide/rtbrgdgd/dhcp.html
2011	“Cisco IP Addressing Guide,” available at https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-business-architecture/sba_ipAddr_dg.pdf
2012	First Amended Docket Control Order, <i>Monarch Networking Solutions LLC v. Cisco Systems, Inc.</i> , No. 2:20-cv-00015-JRG, ECF No. 123 (E.D. Tex. Dec. 7, 2020)

Exhibit	Description
2013	Cisco OSI Model Chart, available at https://learningnetwork.cisco.com/s/article/osi-model-reference-chart
2014	“Internet Protocol, Version 6 (IPv6) Specification,” Network Working Group Request for Comments: 2460 (December 1998), available at https://tools.ietf.org/html/rfc2460
2015	“User Datagram Protocol,” Internet Standard Request for Comments: 768 (August 1980), available at https://tools.ietf.org/html/rfc768
2016	“Transmission Control Protocol,” Internet Standard Request for Comments: 793 (September 1981), available at https://tools.ietf.org/html/rfc793
2017	“IPv6 Extension Headers Review and Considerations,” available at https://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html
2018	Claim Construction Hearing Transcript, <i>Monarch Networking Solutions LLC v. Cisco Systems, Inc.</i> , No. 2:20-cv-00015-JRG, ECF No. 143 (E.D. Tex. Nov. 20, 2020)

Table of Contents

I. Introduction.....	1
II. Background.....	2
A. State of the Art	6
B. The '844 Patent Invention.....	8
C. Petitioner's References	13
1. Ananda	14
2. Wetterwald	16
3. RFC4380 (Teredo)	17
III. Person of Skill in the Art	18
IV. Claim Construction	19
A. "domain"	20
B. "means for constructing an IPv6 destination address by concatenating an operator prefix, said IPv4 destination address, and the destination port number"	22
C. "operator prefix"	23
V. Argument	24
A. All Grounds Fail to Present a Reasonable Likelihood of Success on the Merits	25
1. Petitioner has failed to identify the claimed operator prefix (All Independent Claims).....	26
2. Ananda does not disclose the claimed IPv4 and IPv6 domains (All Independent Claims).....	27
(a) Ananda does not disclose separate IPv6 and IPv4 domains.....	29
(b) Communication Backbone 210 and Subnets 215 and 220 are not separate domains under Petitioner's proposed construction.....	36
3. No asserted art discloses constructing a destination IPv6 address in an IPv6 domain from a received IPv4 data packet by concatenating a destination port number with an operator prefix and IPv4 destination address (All Independent Claims)	38
(a) Ananda	38
(b) Ananda with Wetterwald	41

(c) Ananda with Wetterwald and Teredo	42
4. The asserted grounds do not teach the claimed generating, routing, or extracting limitations (All Independent Claims).....	43
5. Petitioner has not asserted its grounds for invalidity with particularity (Ground 1)	43
6. A POSITA would not have combined Ananda and Wetterwald (All Grounds)	44
7. A POSITA would not have combined Ananda and Wetterwald with Teredo (All Grounds).....	50
B. The Board Should Exercise Its Discretion to Deny the Petition under § 314(a)	55
VI. Conclusion	60

Table of Authorities

Cases

<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020)	57
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 15 (P.T.A.B. May 13, 2020)	57
<i>Cuozzo Speed Techs., LLC v. Lee</i> , 136 S. Ct. 2131 (2016)	56
<i>Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha</i> , IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017)	57
<i>In re Kotzab</i> , 217 F.3d 1365 (Fed Cir. 2000)	13
<i>Koninklijke Philips N.V. v. Google LLC</i> , 948 F.3d 1330 (Fed. Cir. 2020)	44
<i>NHK Spring Co. Ltd. v. Intri-Plex Techs. Inc.</i> , IPR2018-00752, Paper 8 (P.T.A.B. Sept. 12, 2018)	56
<i>OrthoPediatrics Corp. v. K2M, Inc.</i> , IPR2018-01548, Paper 9 (P.T.A.B. March 1, 2019)	24, 26
<i>Solas OLED Ltd. v. Samsung Display Co.</i> , No. 2:19-CV-00152, 2020 U.S. Dist. LEXIS 125973 (E.D. Tex. July 17, 2020)	58, 59, 60

Statutes

35 U.S.C. § 312	29, 43, 44
35 U.S.C. § 314	passim
35 U.S.C. § 316	60

Rules

37 C.F.R. §42.104	23, 24, 27
37 C.F.R. §42.11	27

I. Introduction

Patent Owner Monarch Networking Solutions LLC (“Monarch” or “Patent Owner”) respectfully requests that the Board decline instituting *inter partes* review of U.S. Patent No. 8,451,844 (“the ’844 Patent”) because petitioner Cisco Systems, Inc. (“Cisco” or “Petitioner”) has not shown a reasonable likelihood of prevailing on the invalidity grounds presented on claims 1-10 of the ’844 Patent (“the Challenged Claims”).

Petitioner relies on Ananda to teach the claimed IPv4 domain and IPv6 domain from each independent claim of the ’844 Patent. Ananda, however, teaches strategies which allow a single organization to upgrade the IPv6 backbone within a single domain, not for routing communications between separate domains—one of which is an IPv4 domain—across an independent IPv6 domain. Furthermore, none of the asserted prior art references teaches constructing an IPv6 *destination* address by concatenating an *operator prefix*, an IPv4 *destination* address, and *destination* port information. Additionally, the bases for Petitioner’s proposed combination of Ananda, Wetterwald, and Teredo run contrary to the teachings of the references and the problems they attempt to solve. As a result, Petitioner’s proposed combinations amount to a list of cherry-picked features using the ’844 Patent as a guide, with insufficient explanation as to why a POSITA would have made the proposed combination.

Moreover, this proceeding lags well behind the parallel District Court litigation involving the same parties and issues. Fact and expert discovery will be complete in the litigation well before the Board is likely to even issue an institution

decision. Thus, it would be a waste of resources by the parties, the district court, and the Board to proceed on the instant Petition. Given the advanced state of the co-pending parallel litigation, the Board should exercise its discretion to deny institution under § 314(a).

II. Background

The '844 Patent provides solutions for routing data packets across domains using different versions of Internet Protocol ("IP") telecommunication networks. EX1001 at Abstract, 1:15-21. IP networks provide communication links between terminals connected to a network, allowing data to be exchanged between the terminals. *Id.* at 1:25-39. IP networks direct the data to the proper terminal using devices known as routers that route packets of data to their destinations on the basis of a destination address contained in each packet. *Id.* at 1:32-39, 6:59-7:10. The conventional version of this IP address system (referred to as "IPv4") provided a limited number of publicly available IPv4 addresses. *Id.* at 1:61-62. Due to the limited number of available addresses, operators of home or business domains would frequently operate a "private domain," in which terminals within the private domain received private addresses with access to the public networks (such as the Internet) limited to exchanges occurring through a home gateway or application layer gateway. *Id.* at 1:43-56. The private terminals needing access to the public network share a limited number of public addresses assigned to the home or business network through techniques such as network address translation ("NAT"). *Id.* at 1:51-60.

To further reduce the number of IPv4 public addresses needed, "a solution known as Double NAT or Operator NAT has been proposed and implemented. It

entails activating a NAT function within the telecommunications network of the operator so that the home gateways use a private address (instead of a public address) in their outgoing NAT tables.” *Id.* at 2:11-22. Both home gateway NAT and Operator NAT introduce significant drawbacks, including (1) requiring the interconnection equipment to track and maintain the state of connections in order to properly route packets; (2) introducing additional modifications of data packets for each level of NAT introduced (consuming additional time and processing resources); and (3) degradations in the levels and types of services available due to the limited availability of port forwarding and the resulting need to keep IP sessions active. *See id.* at 2:23-55; 3:40-52; 13:29-46.

A new Internet Protocol (referred to as “IPv6”) provides a significantly larger number of public IP addresses. *Id.* at 1:61-2:1. However, IPv6 is not designed to be backward compatible with IPv4; thus, integrating IPv6 networks with existing IPv4 networks requires configuration beyond that dictated by the protocol standards. *See, e.g.,* EX2002 at 1 (detailing “Transition Mechanisms for IPv6 Hosts and Routers” that are “designed to allow IPv6 nodes to maintain complete compatibility with IPv4”). Many organizations and operators have not been able to transition from IPv4 to IPv6 due to “financial, strategic, and technical reasons.” EX1001 at 2:7-10. “It is therefore necessary to provide for a changeover to IPv6 in the medium term. Such a changeover will necessarily lead to a period of transition during which IPv6 domains will have to interconnect with IPv4 domains.” *Id.* at 2:46-55.

A home gateway¹ provides interconnection between a private domain and a public network operated by service providers. *See id.* at 1:40-56. “The home gateway generally assigns private IP addresses to the terminals of its home network.” *Id.* at 1:43-44. The addresses may be IPv4 addresses, which typically are formatted with a length of 32 bits, and frequently represented as four integers (each representing an octet of bits) separated by periods. *Id.* at 6:21-22. Private IP addresses may be allocated from a reserved private address space including the following blocks:

10.0.0.0	-	10.255.255.255	(10/8 prefix)
172.16.0.0	-	172.31.255.255	(172.16/12 prefix)
192.168.0.0	-	192.168.255.255	(192.168/16 prefix)

EX1007 at 4. Addresses may be considered private in instances where the address is shared and thus the address is not globally routable. *Id.* at 2-4.

The same private addresses in such address spaces can be concurrently used or shared by multiple private networks. *Id.* (“The address space can thus be used by many enterprises. Addresses within this private address space will only be unique within the enterprise . . .”). Thus, subnetworks within the same private network (such as an internal network maintained by a business) typically share a single private address space, while independent private networks will have their own

¹ The term “home gateway” is used generically throughout this document to refer to various gateways and routers that are used to interface a private network with a public network, including customer premise equipment (CPE) gateways and border relays (BR).

private address space for each network maintained by one or more servers for that network. *Id.*

Because private addresses are not unique across the broader public network (such as the Internet), terminals assigned these private addresses generally have limited ability to communicate with other terminals outside of the private network. *See id.* at 2-4 (“In order to use private address space, an enterprise needs to determine which hosts do not need to have network layer connectivity outside the enterprise in the foreseeable future and thus could be classified as private.”). A gateway can offer some public network accessibility to terminals with a private address by maintaining a table that maps a public address and port to a private address and port (often referred to as “NAT” or “NAPT”). EX1001 at 1:51-60, 2:11-45, 3:40-52, 6:13-20, 13:43-56. However, interoperability through traditional NAT is limited by the number of available public addresses and/or ports, and it requires the gateway to monitor and maintain tables with state information about the current connections between terminals in the private domain and other terminals outside the private domain. *Id.* Thus, traditional methods of providing interoperability incurred significant overhead due to the requirement of tracking connection states in a network address and port translation (NAPT) table. These problems were further exacerbated by solutions such as Operator NAT, which required additional state tracking and modification of transmitted data packets within the telecommunication network of the operator. *Id.* at 2:11-45. Thus, for Operator NAT, state tracking is required at both a home gateway and at a border relay device. Thus, a telecommunications operator must include NAT state tables at both the home

gateway and at a border relay device within the telecommunication network, which significantly increases the cost and complexity of the telecommunication network. Due to these complexities, telecommunication operators and service providers were reluctant to implement core networks that implement IPv6 addressing schemes. EX1001 at 2:7-45.

A. State of the Art

Because there is no single standardized strategy for transitioning from IPv4 to IPv6, there is also no single standardized solution for providing interconnection from one device or network type to another. For example, one organization may need to update its infrastructure backbone to IPv6 without breaking connectivity for existing IPv4 terminals, while another organization may need to provide a terminal with the ability to traverse an intermediate IPv4 network to exchange packets with an IPv6 terminal in a third network, while yet another organization may need to provide connectivity to mobile hosts across access points connected to an IPv6 network. *Compare* EX1005 ¶¶71-74, with EX1009 at 10-11, with EX1008 at 2:40-3:20. Because of these and other factors, it is well-known that different interconnection solutions are frequently incompatible and individual pieces of an interconnection solution cannot just be mixed and matched. Instead, the solution must be specifically tailored to the problems of a given transition strategy.

Accordingly, numerous solutions have been proposed to allow interconnection between IPv4 and IPv6 networks. EX2001 at 19; *see also* EX1001 at 2:11-22. The various IP interconnection techniques generally fall into two categories: “stateful” and “stateless.” EX2001 at 11, 19. In a stateful solution, border

and/or edge devices must maintain the “state” of each connection or session within their networks. *Id.* at 12. When state must be maintained within a provider network or network core, this places a significant overhead burden on routing devices as they attempt to maintain the state for numerous connections. *Id.*

Stateless solutions avoid many of these drawbacks. *Id.* at 15. Because there is no need to maintain the “state” of the connections within the provider network or core network, stateless solutions provide better scaling, better performance, flexible network design and better cost effectiveness. *Id.*

Prior to the '844 Patent, the methods of providing interconnection between terminals in a separate IPv4 domain with a public IPv6 domain were often costly and complex, requiring the use of NAPT state tables to convert between IPv4 and IPv6 addresses for every packet transmission occurring between these different domains. EX1001 at 1:51-60, 2:11-45, 3:40-52, 6:13-20, 13:43-56. The invention developed by France Telecomm disclosed in the '844 Patent sought to minimize the reliance on these state tables by introducing techniques that supported stateless encapsulation and/or translation of an IPv4 data packet into an IPv6 data packet. *See id.* at 3:40-46, 3:59-65, 13:43-56.

B. The '844 Patent Invention

The '844 Patent issued on May 28, 2013 and it claims priority to a French application filed by France Telecom on June 30, 2008.² Some of the references considered by the USPTO patent examiner during examination, as indicated on the face of the '844 patent, include:

(1) U.S. Patent No. 7,245,622 which describes the use of a “Teredo” address and server system. *See, e.g.*, EX2008 Figs. 2-4, 7, 10:10-39. The '622 Patent identifies Christian Huitema (author of RFC4380 (EX1009 at 1)), as its inventor and also cites multiple documents with the same title as RFC4380.³ Cisco relies on RFC4380 for all invalidity grounds instead of the '622 patent, but the teachings substantially overlap.

(2) U.S. Patent Pub. No. 2005/0286553 to Wetterwald et al., which was the published version of Application No. 10/875,811. EX1010. The '811 Application was commonly-assigned, co-pending to, and incorporated by reference by U.S. Patent No. 7,639,686 to Wetterwald. EX1008 at 2:1-5. Cisco relies on Wetterwald

² Cisco has not challenged the June 30, 2008 priority date that is identified on the face of the '844 Patent. Pet. at 14. A PCT application was timely filed on June 16, 2009, claiming priority to the original French application.

³ The '622 Patent cites three publication with the title “Teredo: Tunneling IPV6 Over UDP Through NATS.” *Compare with* RFC4380 (EX1009), entitled “Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs).”

for all invalidity grounds instead of the '553 Publication, but the teachings substantially overlap.

The USPTO determined that Monarch's '844 Patent was patentably distinct from those cited references.

The '844 Patented invention discloses techniques for routing data packets to and from IPv4 terminals in separate domains via an intermediate IPv6 domain without the need to resort to NAT-based state tracking. EX1001 at 3:35-52.⁴

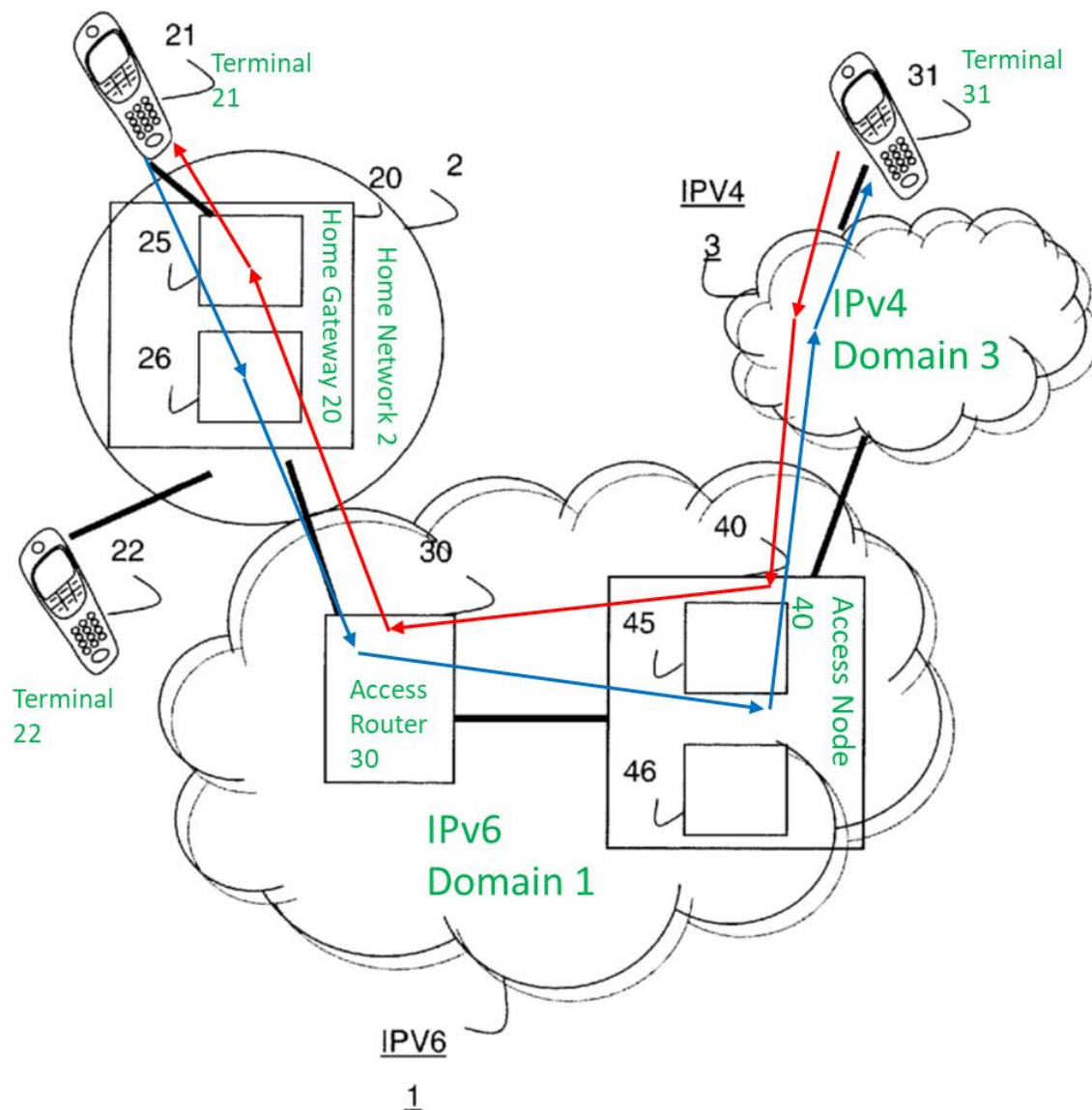


FIG. 1

The above diagram, an annotated version of Figure 1 of the '844 Patent, is an example of interconnected networks that benefit from the '844 invention. Domain 3 is an IPv4 domain connected to Domain 1, which is an IPv6 domain. EX1001 at 7:4-10. Domain 1 is further connected to Home Network 2, which is an IPv4 Domain providing network access to Terminals 21 and 22. *Id.* Because IPv4 addresses cannot be routed in an IPv6 domain, packets from a terminal in Domain 3 normally cannot be sent to a destination in Home Network 2, because to do so would require traversing IPv6 Domain 1.

The '844 invention provides the ability for terminals in an IPv4 domain (such as Terminal 31) to communicate with terminals in other IPv4 domains, even when reaching the destination terminal requires traversing an IPv6 domain. For example, the invention enables Terminal 31 in IPv4 Domain 3 to exchange data packets with Terminal 21 in Home Network 2, using the paths indicated by the red and blue arrows in the above figure. EX1001 at 9:62-11:41. Because Terminal 31 resides in an IPv4 Domain, it would normally be unable to communicate with Terminal 21 across IPv6 Domain 1, because IPv4 packets are not routable within an IPv6 domain. To communicate with Terminal 21, Terminal 31 creates an IPv4 packet with a header

⁴ The '844 patent does indicate that “an internal network address translation (NAT) device is often included in this kind of home gateway if it serves a plurality of user terminals 21, 22 in its home network.” EX1001 at 11:42-48. The home gateway may thus include an internal NAT to translate between public and private addresses.

containing the destination IPv4 address and port of Terminal 21. *Id.* at 10:4-9. That packet is routed to Access Node 40, which is a dual stack IPv4/IPv6 router capable of routing traffic between Domain 1 and Domain 3. *Id.* at 9:47-56.

The invention teaches that an IPv6 routable packet can be created from an IPv4 packet using a novel stateless approach which includes constructing an IPv6 destination address using a predetermined operator prefix, destination IPv4 address information derived from the incoming IPv4 data packet, and destination port information from the IPv4 data packet. EX1001 at 2:59-3:18. This approach is stateless in that portions of the constructed IPv6 destination address can be retrieved from information in the incoming IPv4 data packet (IPv4 destination address and port information) and from network information that has been provided by other routers within the IPv6 domain (the operator or IPv6 prefix). The router in the IPv6 domain receiving the IPv4 data packet is able to construct the IPv6 destination address “on-the-fly” from the received IPv4 data packet without requiring entries in state tables. Access Node 40 will select the IPv6 prefix corresponding to the interconnection device which has previously advertised that it is responsible for routing packets to the destination address (in this case, a prefix associated with Access Router 30). *Id.* at 8:39-44, 10:14-22. The access node 40 will then construct an IPv6 packet from information derived from the received IPv4 packet and the generated IPv6 packet will be routed through the IPv6 domain to Access Router 30, which can then forward the packet to Home Gateway 20. *Id.* at 11:9-15 The home gateway can determine whether it is a standard IPv6 packet or an IPv6 packet which has been generated from an IPv4 packet. *Id.* at 11:20-24. If it is a packet that was

generated from an IPv4 packet, the home gateway can generate an IPv4 packet from the IPv6 packet and route the IPv4 packet to a terminal within the home gateway network, such as Terminal 21. *Id.* at 11:25-41. This ability to uniquely route the data packet from an IPv4 source terminal through an intermediate IPv6 domain to the intended IPv4 destination terminal occurs despite the existence of other home gateways that may also use an address shared by home gateway 20. *See id.* at Figure 2 (shared@IPv4 address); 8:1-13 (“sharing the public address shared@IPv4 between home gateways ...”).

C. Petitioner’s References

Petitioner asserts three grounds of invalidity, arguing: (1) Claims 1-6, 8, and 10 “are obvious”⁵ over U.S. Patent Pub. No. 2004/0107287 to Ananda et al. (“Ananda”) in view of U.S. Patent No. 7,639,686 to Wetterwald (“Wetterwald,” EX1008) and further in view of Internet Engineering Task Force Request for Comments 4380 (“RFC4380” or “Teredo,” EX1009); (2) Claim 7 “is obvious” over

⁵ The test for obviousness is not whether a claimed invention “is obvious” or “are obvious” since such an analysis fails to take into account the issue of obviousness at the time of the invention in June 2008. The “critical” question is not whether the claimed invention is obvious now, but rather whether it would have been obvious when “casting the mind back to the time of invention,” and relying only on the “prior art references and the then-accepted wisdom in the field.” *In re Kotzab*, 217 F.3d 1365, 1369 (Fed Cir. 2000).

Ananda in view of Wetterwald and further in view of Teredo and Internet Engineering Task Force Request for Comments 4271 (“RFC4271,” EX1046); (3) Claim 9 “is obvious” over Ananda in view of Wetterwald and further in view of Teredo and Internet Engineering Task Force Request for Comments 1918 (“RFC1918,” EX1007). Pet. at 25-27, 32, 84, 87.

None of the prior art cited by Petitioner discloses a system as described and claimed in the ’844 patent, in which an IPv6 destination address is constructed using an operator prefix, and IPv4 destination address and port information derived from a received IPv4 data packet, thereby eliminating the need for state tables for the IPv4-to-IPv6 conversion operation. Further, a skilled artisan would not have been motivated to combine together these references in the manner proposed by Petitioner. And even if the teachings from the cited references had been combined, it would not have resulted in the inventions recited in the ’844 claims, absent the use of hindsight to reconstruct the claimed invention.

1. Ananda

Ananda teaches a technique that allows an organization or enterprise (such as a corporation or university) to upgrade parts of its internal network backbone from IPv4 routers to IPv6 routers without requiring that all hosts within the organization’s network be immediately upgraded to support IPv6. EX1005 ¶¶71-73. Ananda accomplishes this goal through the use of communication protocol interfaces (“CPIs”) located at specific points within the organization’s internal communication network. EX1005 Abstract, Fig. 2, ¶¶ 19, 63, 74. When necessary, these CPIs encapsulate an IPv4 packet within an IPv6 packet so that the IPv4 packet can be

transported across the organization's IPv6 backbone to another one of the organization's subnets that has not been fully upgraded to IPv6. *Id.* ¶ 63. Because Ananda's proposed solution is limited to a single organization, the destination subnet can be identified solely from the subnet id. *See id.* ¶¶ 103-108. Once the packet reaches the destination subnet, it can be routed to its destination using just the host id. *See id.*

Ananda does not disclose using port information when generating an IPv6 destination address. While Ananda addresses problems related to the transition from IPv4 to IPv6, it only provides a solution for routing communications ***for a single organization's network***, not for routing communications between separate domains—one of which is an IPv4 domain—across an independent IPv6 domain. *See* EX1005 ¶64 (“This enables a gradual adoption and transition ***of an organization*** from IPv4 to IPv6” (emphasis added)). Routing within a single organization, as taught by Ananda (as opposed to routing across independent domains, as taught by the '844 Patent) is a limited solution to IPv4 and IPv6 inoperability that is specific to that organization. This limited solution does not solve the more complicated problem of routing to and from an IPv4 domain across a separate IPv6 domain, as addressed by the '844 Patent. An internal network such as Ananda that is controlled and administered by a single entity is able to control the use of IP addresses in a manner that avoids any address conflict that might arise when an IPv4 address is shared.

2. Wetterwald

Wetterwald teaches techniques for routing data packets “that enables an IPv4 host to establish and maintain IP connectivity from among multiple access points within an access network.” EX1008 at 2:56-3:3. Wetterwald primarily relates to providing network access to wireless devices and discloses routing techniques for use within a single organization’s domain so that the domain can accommodate a mobile host that “traverses across multiple access points within a limited area (e.g., a building, campus, a city district, town, etc.).” *Id.* at 2:51-53, 4:28-45. The network includes an IPv6 access network 14 that includes access points 30 that provide wireless access cells 12 for the mobile devices. *Id.* at Figs. 1-2, 4:30-37. The access points are arranged in a cluster, with a single root referred to as a clusterhead. *Id.* at 4:46-49. The clusterhead 32 provides a single access point for the transfer of packets between an IPv6 access network and the public IPv4 network. *Id.* at 4:49-52.

Wetterwald does not disclose using port information when generating an IPv6 destination address, and in fact, suggests including port information within the payload of an IPv6 data packet, not in the IPv6 destination address. *Id.* at 8:25-28. Like Ananda, Wetterwald provides some level of interoperability between IPv4 and IPv6 elements within a domain. However, Wetterwald is concerned with providing mobile access connectivity, not with piecemeal transitioning of network infrastructure to IPv6 like Ananda. Wetterwald also does not teach how to achieve communication between one or more separate IPv4 domains interconnected by an IPv6 domain—it is concerned with providing mobile connectivity within a single organization’s domain. In Wetterwald, all addresses used with the access cells and

access networks obtain a unique address for use within that network from a DHCP server in a clusterhead device, thus eliminating any potential address conflicts. *Id.* at 4:60-64.

3. RFC4380 (Teredo)

RFC4380 (“Teredo”) is entitled “Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs).” EX1009 at 1. Teredo discusses “a service that enables nodes located behind one or more IPv4 Network Address Translations (NATs) to obtain IPv6 connectivity.” *Id.* at 1. In the Teredo system, an IPv4 client obtains a Teredo IPv6 **source** address that it can use in communications with an IPv6 network as a preliminary step prior to exchanging messages. *Id.* at 5. “Teredo clients can exchange IPv6 packets with plain IPv6 nodes (e.g., native nodes or 6to4 nodes) through Teredo relays.” *Id.* at 11. The IPv4 Teredo client generates an IPv6 packet having an IPv6 **source** address including a defined prefix, the IPv4 address of a Teredo server, a set of flags, and an obfuscated client port and IPv4 address:

```
+-----+-----+-----+-----+
| Prefix      | Server IPv4 | Flags  | Port  | Client IPv4 |
+-----+-----+-----+-----+
```

Id. at 11-12.

The Teredo client then generates an IPv4 packet in an IPv4 network that includes as its payload the IPv6 source address of the source IPv4 client and an IPv6 destination address of the destination IPv6 client. *Id.* at 13. This IPv4 message is transmitted to a Teredo server, which “decapsulates the IPv6 message and forwards it to the intended IPv6 destination.” *Id.* at 11. Teredo only discloses constructing an

IPv6 **source** address with IPv4 **source** address and **source** port information. The IPv6 destination address does not include that information. And in Teredo, that IPv6 source address is not generated from information derived from a received IPv4 data packet and it is not generated in an IPv6 domain, it is constructed at an IPv4 client in an IPv4 network. The Teredo server that receives the IPv4 data packet with the IPv6 source address in the IPv4 packet payload does not construct an IPv6 destination address or IPv6 source address through any concatenation operation—instead it simply forwards the IPv6 data packet decapsulated from the IPv4 data packet.

Aside from being designed for a single type of terminal (those located behind a NAT), Teredo also emphasizes that it is “designed to provide an ‘IPv6 access of **last resort**’ to nodes that need IPv6 connectivity but **cannot use any of the other** IPv6 transition schemes.” *Id.* at 8 (emphasis added). Teredo provides extensive explanation as to why its use should be a solution of absolute last resort, including the introduction of significant overhead and performance issues as well as serious security vulnerabilities. *Id.* at 9-11, 36, 41-45, 49.

III. Person of Skill in the Art

For purposes of this Preliminary Response, Patent Owner does not contest Petitioner’s recitation of the level of skill in the art, because even under Petitioner’s proposed level of skill Petitioner has failed to demonstrate a reasonable likelihood of success. Patent Owner reserves the right to propose its own definition of a person of ordinary skill in the art (“POSITA”) in the future if necessary.

IV. Claim Construction

Petitioner proposes constructions for the following terms: (A) “domain”; (B) “means for constructing an IPv6 destination address...”; (C) “means for generating an IPv6 data packet...”; (D) “means for routing the generated IPv6 data packet...”; (E) “means for extracting the IPv4 destination address...”; (F) “means for generating an IPv4 data packet...”; (G) “means for routing the IPv4 data packet...”; (H) “means for advertising to the IPv4 domain...”; (I) “means for advertising in the IPv6 domain...”; and (J) “means for obtaining an IPv4 address, a range of port numbers, and a range of authorized IPv6 addresses.” Pet. at 15-25.

In addition to these terms, in the parallel litigation Petitioner requested the construction of other terms from the ’844 patent that may be relevant to its IPR position, including the term “operator prefix,” which Petitioner argued was not a well-known term in the art. *See* EX2004 at 15-16; EX2006 at 22-25.

For the purposes of this Preliminary Response, it is not necessary for Monarch to propose constructions for terms other than “domain”; “means for constructing an IPv6 destination address by concatenating an operator prefix, said IPv4 destination address, and the destination port number”; and “operator prefix.” Even under Petitioner’s proposed constructions for the remaining terms, Petitioner has failed to demonstrate a reasonable likelihood of success on any of the challenged claims.⁶

⁶ Monarch reserves the right to propose constructions for the additional terms, if necessary, in its response. To the extent construction is required for these terms,

A. “domain”

Petitioner’s argument that “domain” simply equates to a network is wrong. Pet. at 15-17. This is apparent from both the intrinsic evidence and the extrinsic evidence, including Petitioner’s own materials, which establish that “domain” includes the concept of common control. The proper construction for “domain” is “a network or subnetwork and its address space that are under common control.”

The ’844 Patent’s specification states that “[a] telecommunications network administered by an operator is also referred to as a domain.” EX1001 at 1:30-31. Thus, the ’844 Patent supports defining domain to include the concept of control. One cannot speak of a domain without considering the particular entity that operates or controls it. Consistent with the specification passage cited above, a network administered by a different operator would be a different domain. In this regard, the specification highlights the difference between a private domain (a network that is controlled or administered by a homeowner or business entity), and a domain operated by a service provider. *Id.* at 1:32-50; 4:41-43 (“The neighboring IPv4 domain may be a public network managed by an operator or a private network, either a home network or a business network.”). This concept is important, because a network operator controlling a domain can take precautions, such as restricting where in the network address translation occurs, and ensuring private addresses are not re-used within that domain. In networks that are operated and controlled by

Monarch refers the Board to the Court’s Claim Construction in the parallel District Court proceeding. *See* EX2006.

different entities, such precautions are not possible: entities (such as a service provider) may implement their own layer of address translation, and the same private IPv4 addresses can be reused in different domains. *Id.* at 2:11-22 (discussing Operator NAT); EX1007 at 4 (“Addresses within this private address space will only be unique within the enterprise...”).

Newton’s Telecom Dictionary, cited with approval by Petitioner, is in accord and provides the formal definition of “[t]he **part** of a computer network in which the data processing resources **are under common control**.” EX1006 at 3 (emphases added). Petitioner also identifies the description of “domain” in RFC1983 (Internet Users’ Glossary), but once again, that definition highlights how Petitioner’s construction improperly fails to recognize the concept of common control. It also highlights that “domain” and “network” are not synonymous. RFC1983’s definition of “Administrative Domain” refers to “[a] collection of hosts and routers, and the interconnecting network(s), managed by a single administrative authority.” EX1015 at 4; *see id.* at 48 (defining “routing domain” as “[a] set of routers exchanging routing information within an administrative domain.”). The *IBM Dictionary of Computing* is in accord and defines “domain” as “[t]hat part of a computer network in which the data processing resources are under common control.” EX2007 at 4.

Petitioner also cites to other materials, but none of those passages support the conclusion that the term “domain” refers simply to a network. Petitioner’s extrinsic evidence illustrates that “subnet” or “subnetwork” are not synonymous with “network,” much less with “domain.”

Because none of its references addresses the requirement of common control inherent to the concept of a domain, Petitioner has failed to show a reasonable likelihood of success on the challenged claims.

B. “means for constructing an IPv6 destination address by concatenating an operator prefix, said IPv4 destination address, and the destination port number”

Petitioner and Monarch agree that this limitation is governed by 35 U.S.C. § 112(6), and that the function is “constructing an IPv6 destination address by concatenating an operator prefix, said IPv4 destination address, and the destination port number.”

Monarch proposes the structure identified by the District Court: “access node 40 with a device 25 that includes a processor programmed to perform the step of constructing an IPv6 destination address by concatenating an operator prefix, said IPv4 destination address, and the destination port number as illustrated in Figures 2 and 4.” EX2006 at 49-56, 59. Petitioner noted it “generally agree[d]” with the District Court’s approach at oral argument before the Court. EX2018 at 109:1-12, 118:22-120:21.

Cisco’s proposed construction focuses on inclusion of a network address translation table despite the ’844 specification highlighting the stateless nature of the disclosed operation. See Pet. at 18-19; EX1001 at 13:43-56. To the extent that Cisco is suggesting that this “means for constructing” limitation implicates a stateful operation, that requirement is inconsistent with the preferred embodiment, which is stateless (as the District Court found). See EX2006 at 57 (“Defendant’s reliance on a NAT table as the structure implementing this term is contrary to the preferred

embodiment.”). In addition, the “means for constructing an IPv6 destination address” limitation correlates to a router on the IPv6 domain (such as access node 40), which does not require a NAT table to construct the IPv6 address.

C. “operator prefix”

The term “operator prefix” was a term that Petitioner requested to have construed by the Court in the parallel lawsuit, claiming construction was necessary because it was not a well-known term in the art. *See* EX2004 at 15-16; EX2006 at 22-25. At the urging of Petitioner, the Court ruled that the term “operator prefix” had been explicitly defined in the patent specification and prosecution history of the ’844 patent and the related ’845 patent. EX2006 at 22-25. The Court adopted Petitioner’s position and construed “operator prefix” as “a prefix assigned to an Internet Service Provider by its Regional Internet Registry.” EX2006 at 25. PTAB rules require that a petitioner set forth how each challenged claim is to be construed, as well as how “the **construed** claim is unpatentable.” 37 C.F.R. §42.104(b)(3-4) (emphasis added). Due to advocating for and having received a construction of “operator prefix” in a parallel judicial proceeding, Petitioner would have known that the same term would be at issue in this proceeding and cannot now claim that no construction is necessary. *See OrthoPediatrics Corp. v. K2M, Inc.*, IPR2018-01548, Paper 9 at 9-12 (P.T.A.B. March 1, 2019). Because Petitioner failed to propose such a construction, the Petition fails to comply with 37 C.F.R. §42.104(b)(3-4), and should be denied. *Id.*

V. Argument

The Petition should be denied for multiple independent reasons. First, as to all challenged independent claims,⁷ Petitioner fails to raise a reasonable likelihood that Ananda combined with Wetterwald and Teredo discloses the claimed IPv6 domain and the IPv4 domain under the constructions advanced by the parties, nor does the combination disclose constructing an IPv6 destination address by concatenating an operator prefix, an IPv4 destination address, and a destination port number. Petitioner has not even attempted to show that an IPv6 address is constructed with an operator prefix, according to its own proposed construction for that term in district court, nor has Petitioner identified the use of destination port information in an IPv6 destination address in any reference. Additionally, the bases for Petitioner's proposed combination of Ananda, Wetterwald, and Teredo run contrary to the teachings of the references and the problems they attempt to solve. As a result, Petitioner's proposed combinations amount to a list of cherry-picked features using the '844 Patent as a guide, with insufficient explanation as to why a POSITA would have made the proposed combination.

Finally, the Petition should be denied under the Board's discretion, given the advanced state of the co-pending litigation involving the same issues.

⁷ For the purposes of this Preliminary Response, Monarch has restricted its arguments to the independent claims of the '844 Patent.

A. All Grounds Fail to Present a Reasonable Likelihood of Success on the Merits

Petitioner has not shown a reasonable likelihood of success for any of the asserted grounds. Regarding all grounds: (1) Petitioner has failed to propose a construction for the claimed operator prefix or identify the prefix (under the construction it previously sought) in any asserted prior art, (2) Ananda fails to teach the IPv4 and IPv6 domains for which Petitioner relies on it because Ananda's IPv4 subnetworks and IPv6 backbone are under common control and share a common address space, (3) no asserted art discloses constructing an IPv6 destination address by concatenating an operator prefix, and information related to an IPv4 destination address and destination port, (4) the asserted art fails to teach the generating, routing, and extracting limitations as a consequence of failing to teach the constructing limitations, (5) Petitioner has failed to assert its grounds with particularity as required, at times relying on the knowledge of a POSITA not included as part of its proposed combination, (6) Petitioner has failed to demonstrate why a POSITA would have combined Ananda (addressing piecemeal transitioning of infrastructure) with Wetterwald (addressing mobile access connectivity), and (7) Petitioner has failed to demonstrate why a POSITA would have combined Ananda and Wetterwald with Teredo, which was known to introduce significant drawbacks in security and performance.

1. Petitioner has failed to identify the claimed operator prefix (All Independent Claims)

Each of the independent claims of the '844 Patent requires an IPv6 destination address constructed by concatenating, *inter alia*, an operator prefix.⁸ As discussed in the Claim Construction section, Petitioner argued in the parallel District Court proceeding that “operator prefix” was a term that required construction, and the Court adopted Petitioner’s argument. Having argued for and obtained that construction in a judicial proceeding, Petitioner cannot now advocate here that no construction is necessary. *See OrthoPediatrics*, IPR2018-01548, Paper 9 at 9-12. Nor can it succeed on its Petition if it failed to provide a construction for a challenged claim or demonstrate how the **construed** claim is unpatentable. 37 C.F.R. §42.104(b)(3-4).⁹

⁸ The preambles of '844 Claims 1, 3, 5, and 10 form limitations of those claims. This is apparent because terms such as “IPv4 destination address,” “destination port number” and “IPv6 destination address” are recited in the body of the claim by using the article “the” which references the prior preamble recitation of those terms (*e.g.*, in Claim 3: “extracting **the** IPv4 destination address and **the** destination port number from **the** IPv6 destination address”).

⁹ Further, Petitioner’s failure to disclose inconsistent positions taken in this proceeding and in the parallel district court litigation is a violation of its duty of candor, which warrants denial of its Petition. *See* 37 C.F.R. §42.11-42.12;

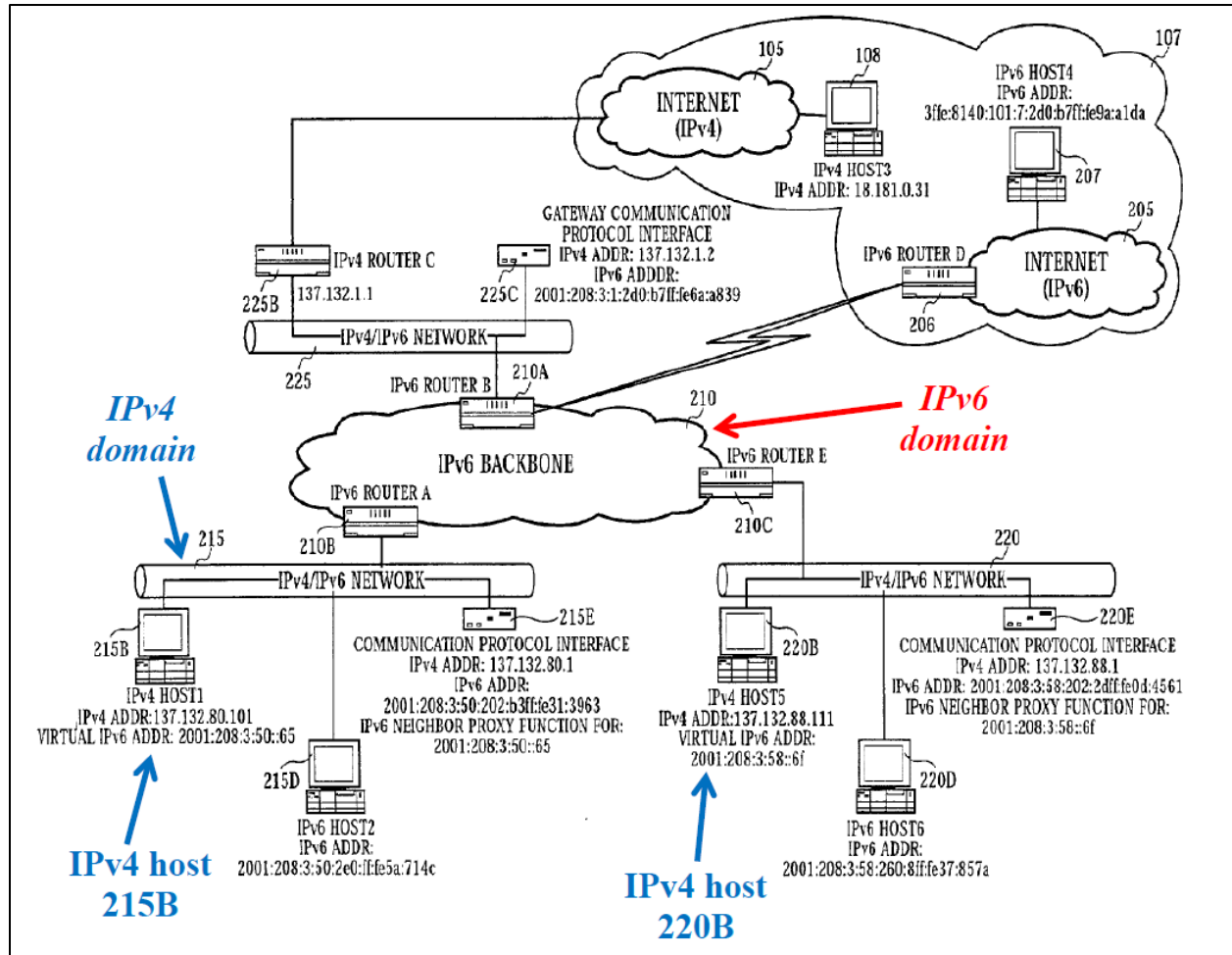
Furthermore, nowhere in its Petition does Petitioner identify “a prefix assigned to an Internet Service Provider by its Regional Internet Registry,” as it previously sought to construe the term “operator prefix.” *See, e.g.*, Petition at 48. For at least these reasons, the Petition should be denied.

2. Ananda does not disclose the claimed IPv4 and IPv6 domains (All Independent Claims)

Each of the independent claims of the '844 Patent require either “receiving a data packet from an *IPv4 domain* in an *IPv6 domain*” ('844 claims 1-2, 5 (emphasis added)) or “sending a data packet from an *IPv6 domain* to a destination address of an *IPv4 domain*” ('844 claims 3-4, 10 (emphasis added)). This sending/receiving of packets between the domain types is possible because the '844 Patent enables the transparent (to the hosts) interconnection of an IPv4 domain and an IPv6 domain.

Petitioner alleges that Ananda's IPv6 Communication Backbone 210 is the IPv6 domain and Ananda subnets 215 and 220 are IPv4 domains, as shown in the following annotated figure from the Petition:

§42.51(b)(1)(iii) (regarding disclosure of inconsistent positions); 77 Fed. Reg. 48756 at 48761 (same).



Pet. at 36-39 (Claim 1), 60-62 (Claim 3).¹⁰

Under any of the constructions proposed for “domain,” Petitioner fails to demonstrate that Ananda discloses separate IPv4 and IPv6 domains, as required by

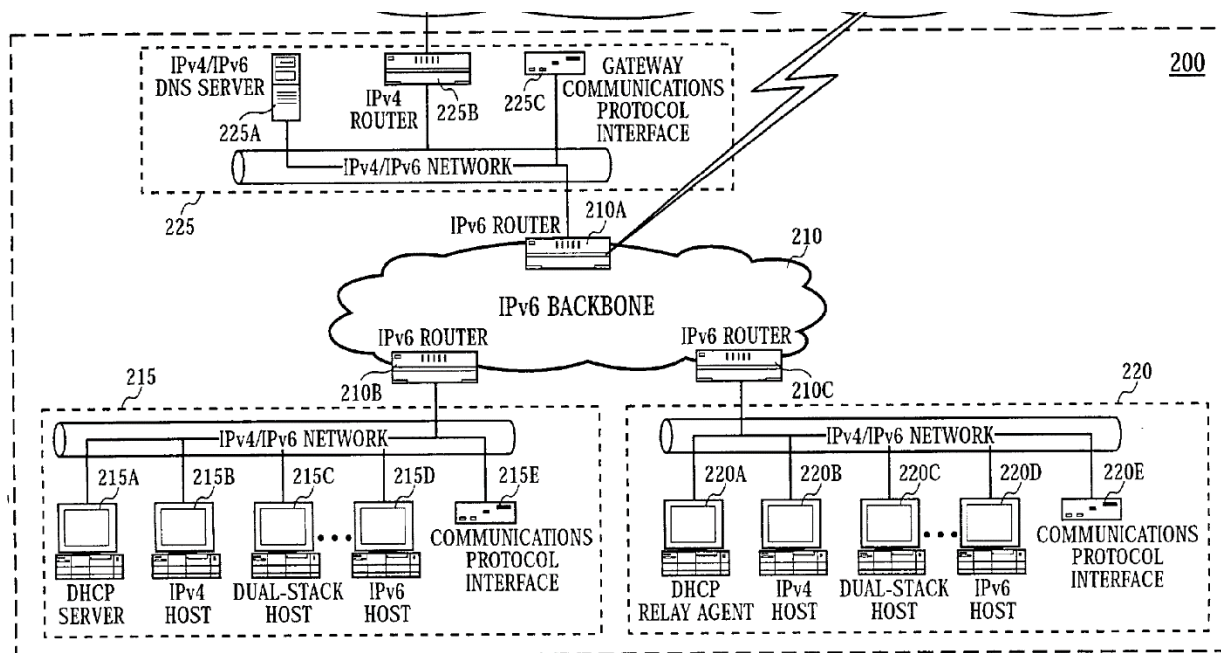
¹⁰ Petitioner never expressly identifies what in the asserted references teaches the IPv4 Domain and IPv6 Domain recited by Claims 2, 4, 5, and 10. Pet. at 58-60 (Claim 2), 70-71 (Claim 4), 71-72 (Claim 5), 83 (Claim 10). For at least this reason, Petitioner has failed to satisfy 35 U.S.C. § 312(a)(3) and 37 CFR § 42.104(b)(4) for Claims 2, 4, 5, and 10.

the claim language. Regarding Patent Owner’s proposed construction, Petitioner has failed to demonstrate that IPv6 Communication Backbone 210 and subnets 215 and 220 are separate domains. IPv6 Communication Backbone 210 and subnets 215 and 220 all *share common control and a common address space*; therefore, all three are components of the ***same domain***. Regarding Petitioner’s proposed construction, IPv6 Communication Backbone 210 and subnets 215 and 220 are components of a *single network*; thus again, those subnets are components of the ***same domain***.

(a) Ananda does not disclose separate IPv6 and IPv4 domains

As detailed above, “domain” should be construed as “a network or subnetwork and its address space that are under common control.” *See supra* §IV.A. IPv6 Communication Backbone 210 and subnets 215 and 220—and their corresponding address space—are under common control, and thus form a single domain. For this reason, Communication Backbone 210 cannot be a separate IPv6 domain from subnets 215 and 220.

Petitioner suggests “Ananda discloses transitioning IPv4 network 100 to an IPv6 network” corresponding to communication network 200. Pet. at 33. Ananda teaches that a “communication network 100 is typically employed in an organization, for example in a corporation or university.” EX1005 ¶71. This individual network encompasses all the network elements of the organization inside the large, dashed box shown in Ananda Fig. 2:



Id. Fig. 2 (excerpt).

Communication Backbone 210 and subnets 215 and 220 all belong to the same network 200, which is commonly controlled by the same organization. *See* Pet. at 60 (“Ananda teaches a communication network 200 with CPIs 215E, 220E for transporting [] IPv4 data packets encapsulated in IPv6 data packets...across an IPv6 communication backbone 210”). This is further supported by the fact that Ananda teaches how to reconfigure prior art networks, such as “communication network 100 [which] is typically employed in an organization, for example in a corporation or university,” into a configuration similar to that of network 200 illustrated in Figure 2 of Ananda. *See* Pet. at 33 (“Ananda discloses transitioning IPv4 network 100 to an IPv6 network by replacing the IPv4 routers 110A-110C in Figure 1 with IPv6 routers 210A-210C and upgrading the IPv4 backbone 110 to an IPv6 backbone 210.”).

Not only are Communication Backbone 210 and the subnets 215 and 220 commonly controlled within a single organization’s network (network 200)—their

address space is also commonly controlled. As an initial matter, Petitioner alleges that subnets 215 and 220 either are private networks that use private address space or would have been modified accordingly. *See id.* at 34 (“The IPv4 hosts 215B, 220B may continue to have private IPv4 addresses.”), 82 (“Ananda discloses that the subnet 215 corresponds to pre-transition subnet 115, which is a private network...Thus, it would have been obvious to a POSITA for subnet 215 to be a “*private network*.” (emphasis in original)). Even accepting without conceding Petitioner’s argument that subnets 215 and 220 use private IPv4 addresses, those subnets still fail to disclose separate domains with independently controlled address spaces.

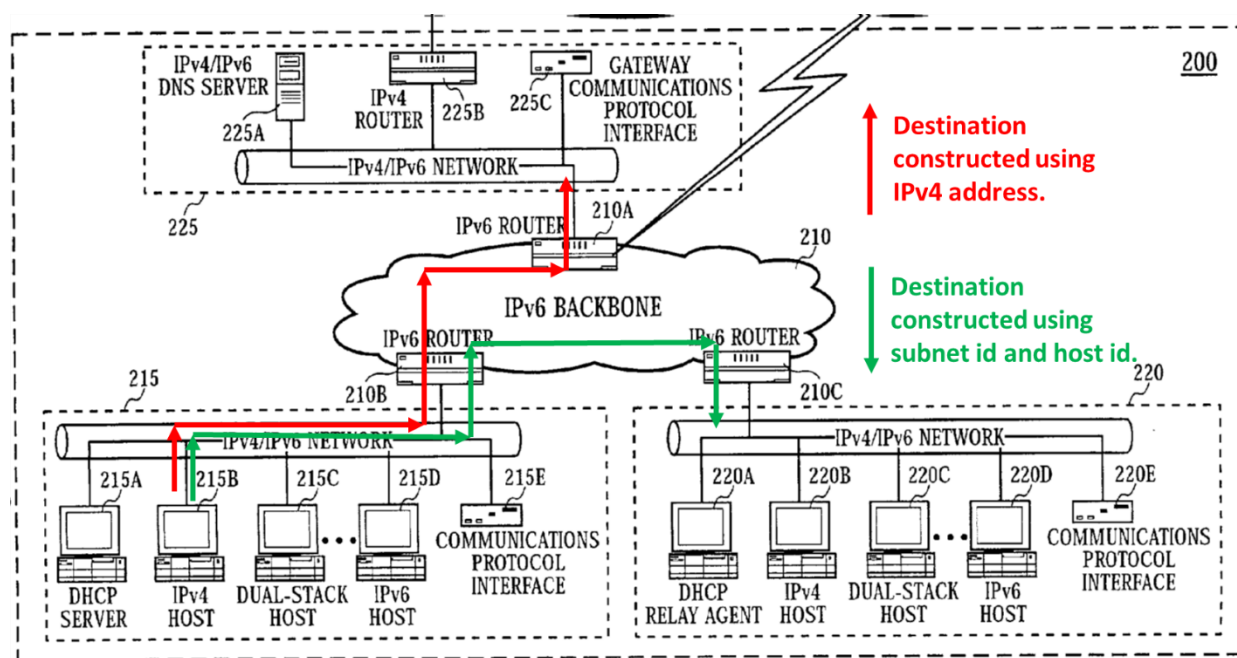
A private network has its own private address space consisting of addresses from reusable predefined blocks. EX1007 at 4. Nothing in Ananda would have suggested to a POSITA that subnets 215 or 220 have separate private address spaces allocated independently from each other. To the contrary, Ananda teaches that subnets 215 and 220 ***share*** an address space, and thus are part of the ***same domain***. Specifically, subnet 215 includes a DHCP Server 215A; subnet 220, on the other hand, includes a DHCP Relay Agent 220A. EX1005 Fig. 2. The DHCP Relay Agent simply relays information between clients on its subnet (220) and the DHCP server (which is located on a different subnet, 215). *See* EX2009 at 3 (“Using BOOTP ***relay agents eliminates the necessity of having a DHCP server on each physical network segment***.” (emphasis added)); *see also* EX2010 at 5-2 (“A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers ***when they are not on***

the same physical subnet.” (emphasis added)). The same DHCP server, 215A, controls address allocation for both subnet 215 and subnet 220; accordingly, their address space is shared. Thus, Ananda’s disclosure makes it apparent that the IPv4 subnets share the same address space, and thus, it necessarily follows that these subnets exist within the same domain.

In fact, implementing the subnets as private networks with separate address spaces introduces the possibility of conflicting private IP addresses assigned to hosts in the various subnets within the organization, which would require additional use of NAT/NAPT and renumbering of the hosts. Cisco’s own documentation discusses how undesirable conflicting address spaces are within an organization. *See* Ex. 2011 at 13-14 (Cisco documentation describing a scenario where an organization’s Branch and Headquarters both assigned the same private address range, noting “the [address] spaces conflict, meaning they use the same subnets as seen in Figure 6. This is a real problem.”).

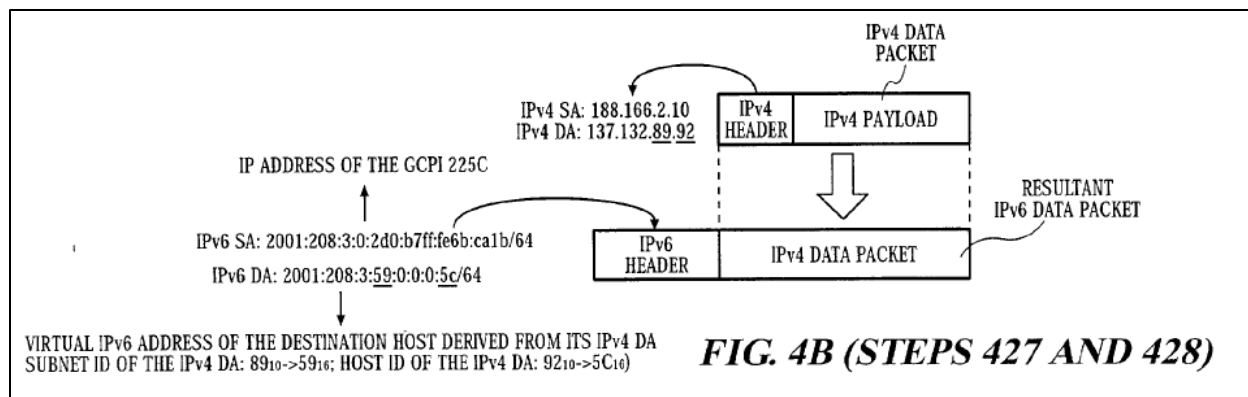
In fact, modifying subnets 215 and 220 to be private networks—with independent private address spaces—would limit communication between private hosts within the subnet and other hosts outside of the organization’s network. *See* Ex. 1007 at 4 (“Private hosts can communicate with all other hosts inside the enterprise, both public and private. However, they cannot have IP connectivity to any host outside of the enterprise.”). Additionally, the modifications proposed by Petitioner would also limit communications within the enterprise because each subnet would be independently responsible for controlling its own address space.

Ananda describes two different ways of constructing an IPv6 destination address for an IPv4 packet that must traverse its IPv6 backbone 210. The first embeds within the IPv6 destination address a public IPv4 address and is used when the packet is being sent to an IPv4 terminal on the IPv4 Internet (*e.g.*, Ananda Host3, 108, in Figure 8). *See* Ex. 1005 ¶¶103-105. The second embeds a subnet id and host id within the IPv6 destination address and is used when the packet is being sent to an IPv4 terminal (*e.g.*, Ananda Host5, 220B, in Figure 8) in a different subnet within the enterprise network (*e.g.*, Ananda network 200 in Figure 2). *See id.* ¶¶103, 106-107. These two scenarios are illustrated below:



Id. Fig. 2 (annotated excerpt). Based on Petitioner's allegations that the subnets 215 and 220 are private IPv4 networks, only the second method is implicated, which involves transmissions between IPv4 terminals on different subnets within the enterprise network.

Ananda cannot teach that subnet 220 (or subnet 215) is its own private domain as Petitioner contends; if it was, using only a subnet id and host id would not guarantee a unique destination address and IP routing would be broken. As shown in Figure 4B, Ananda identifies the subnet id and host id as the third and fourth octets in the IPv4 destination address (89 and 92 in the diagram below):



Id. Fig. 4B.

Ananda expressly teaches that the combination of subnet id and host id (rather than the IPv4 address) is sufficient to route the packet to a host in one of the subnets within communication network 200, such as the subnets 215 and 220 that Petitioner alleges are private IPv4 networks. *See id.* ¶¶101, 106-107. However, if each subnet of Ananda was a separate private domain as Petitioner argues, then the combination of subnet id and host id would not be sufficient to identify a host in a particular subnet. Addresses from a private address space are only unique within that private network. Ex. 1007 at 4 (“Addresses within this private address space will only be unique within the enterprise[.]”).

If subnet 215 and subnet 220 were separate private networks, then each subnet would manage its own independent private address space. Accordingly, each subnet could assign the same IPv4 address (containing the same subnet id and host id) to a host within its respective subnet, making routing and communication between those two subnets impossible. Even hosts without the same IP address could have this problem. For example, if subnet 215 assigned a host the private IPv4 address 172.16.1.7, and subnet 220 assigned a host the private IPv4 address 192.168.1.7, then both hosts would have an identical subnet id (“1”) and host id (“7”). Routing based on subnet id and host id, as disclosed by Ananda when routing between subnets 215 and 220, would result in conflicts if the subnets were changed to private IPv4 domains, which each control their own address space.

Petitioner also alleges that subnets 215 and 220 are independently controlled by their own CPI and IPv6 router. *See* Pet. at 41 (“Ananda further explains how each multi-protocol subnet includes a CPI and an IPv6 router that controls network traffic flowing to and from the individual subnet.”). However, both of those components are responsible for routing packets—not controlling a domain. Petitioner’s logic would suggest that any router touched by packets going to or coming from a subnet exercises control over that subnet. A POSITA would not generally understand a router to impose control on a domain. As detailed above, the addresses used within the subnets are controlled by a single server. DHCP Server 215A directly controls the address space of 215 subnet components, and DHCP Relay Agent 220A, as an agent of DHCP Server 215A, relays DHCP Server 215A’s control of the IP addresses for terminals of subnet 220. EX1005 ¶78 (describing dual-stack DHCP server 215A

within subnet 215); *id.* ¶79 (describing dual-stack DHCP relay 220A within subnet 220); *see supra* (evidence detailing the relationship between DHCP servers and relays).

Based on Ananda's teachings, one of skill in the art would have understood that the IPv4 address space used for subnets 215 and 220 is shared and commonly controlled. Since Ananda's subnets 215 and 220 and their corresponding address space are commonly controlled, they fail to disclose or teach two ***separate*** IPv4 domains, as required by the Challenged Claims.

(b) Communication Backbone 210 and Subnets 215 and 220 are not separate domains under Petitioner's proposed construction

Petitioner proposes that "domain" be construed as "network." *See* Pet. at 15-17. This construction is wrong for the reasons detailed above. *See supra* §IV.A. However, even alternatively accepting Petitioner's proposal, Ananda still does not teach that subnets and a backbone are networks. The very extrinsic evidence on which Petitioner relies indicates that "domain," "backbone," "subnetwork," and "network" are not synonymous.

Ananda consistently refers to the component 200 of Figure 2 as being the "communications network." *See* EX1005 ¶76 ("[t]he communication network 200"); *id.* ¶80 (same); *id.* ¶130 (same). Further, Ananda consistently refers to components 215 and 220 (which Petitioner has identified as the claimed first and second IPv4 domains) as "subnets" of the communication network 200. *See id.* ¶¶76-83. Ananda specifically defines "subnet" to be different than "network": "It should be noted that ***a subnet***, as defined by The Free On-line Dictionary of Computing . . . ***is a portion***

of a network . . .” (emphases added)). *Id.* ¶66. Thus, on its face, Ananda teaches that subnets and networks are not the same. Because a subnet is not a network, even under Petitioner’s proposal that “domain” means “network,” the subnets of Ananda cannot be separate domains.

Similarly, Ananda refers to the communication backbone as the “infrastructure portion” of the communication network comprising a number of inter-coupled routers. *Id.* ¶¶65, 67, 76-77. RFC1208, which Petitioner cites with approval, is “A Glossary of Networking Terms,” and further supports the understanding that the communication backbone is not a separate domain, but rather an infrastructure component of a network. EX1014 at 3 (“backbone: The primary connectivity mechanism of a hierarchical distributed system. All systems which have connectivity to an intermediate system on the backbone are assured of connectivity to each other.”). Thus, Communication Backbone 210 is not a standalone domain, but rather an infrastructure portion of a single domain.

In summary, Petitioner’s allegation that Communication Backbone 210 and subnets 215 and 220 are separate domains contradicts both the teachings of Ananda and Petitioner’s own extrinsic evidence. Ananda teaches that “subnets” and “backbones” are “portions” of a network, which is not the same as a network. The extrinsic evidence further supports this distinction. Thus, even under Petitioner’s proposed construction for “domain,” Ananda’s Communication Backbone 210 does not satisfy the claims’ requirements for an IPv6 domain, nor do subnets 215 and 220 satisfy the claims’ requirements for an IPv4 domain. Because each claim requires an

IPv4 Domain and an IPv6 Domain, Petitioner cannot show a reasonable likelihood of success on any of the proposed grounds.

3. No asserted art discloses constructing a destination IPv6 address in an IPv6 domain from a received IPv4 data packet by concatenating a destination port number with an operator prefix and IPv4 destination address (All Independent Claims)

All independent claims of the '844 Patent require an IPv6 destination address constructed in an IPv6 domain by concatenating an operator prefix with IPv4 destination address and **port** information.¹¹ EX1001 at 14:29-43 (claim 1); *id.* at 14:48 (claim 2 referring to the method of claim 1); *id.* at 50-54 (claim 3); *id.* at 14:65 (claim 4 referring to the method of claim 3); *id.* at 15:5-7 (claim 5); *id.* at 16:20-24 (claim 10). None of the asserted art teaches or renders obvious constructing an IPv6 address in an IPv6 domain by concatenating port information during construction of the IPv6 destination address.

(a) Ananda

Ananda does not teach or in any way suggest to a POSITA to construct an IPv6 destination address by concatenating destination port information. Petitioner appears to agree, because it does not cite any portion of Ananda as teaching concatenation of destination port information. Instead, Petitioner argues it would have been obvious to add a destination port number to an IPv6 address taught by Ananda:

¹¹ As explained in the '844 patent, a port number may represent a range of authorized port numbers. See EX1001 at Figures 2, 4; 5:4-9; 8:9-13; 8:39-61; 9:62-10:3.

Since Ananda's IPv6 address construction technique uses only a portion of the 64 bits available in the second half of an IPv6 address, it would have been obvious to a POSITA that the TCP/UDP source port number, destination port number, or both, could be advantageously incorporated into the constructed IPv6 address itself.

Pet. at 48-49.

Petitioner's reasoning that it would have been obvious to add port information to the IPv6 address purely because the space to do so was available evinces a misunderstanding of how a POSITA would have understood the roles of IP addresses and port information in network communications, and is based solely on hindsight using the '844 Patent as a guide.

To understand why constructing an IPv6 address using port information would not be obvious, it is important to understand the background of IP address and port specifications. A POSITA would know that a port is not defined as a part of the internet protocol (IP) specification at all, let alone used to construct an IP address. Ports and internet protocol addresses are different technologies understood as belonging to separate conceptual "layers" of a network. For example, POSITAs frequently refer to the OSI Reference Model when discussing different layers of networking. The OSI Reference Model is:

A seven-layer structure designed to describe computer network architectures and the way that data passes through them. This model was developed by the ISO in 1978 to clearly define the interfaces in multivendor networks, and to provide users of those networks with conceptual guidelines in the construction of such networks.

EX1015 at 43.

Internet Protocol standards (which define IP address structure and usage and are part of OSI Layer 3) do not include the concept of ports. For example, neither RFC791 (defining the IPv4 specification), RFC1884 (addressing IPv6 addressing architecture), nor RFC2460 (defining the IPv6 specification) includes the word “port.” *See generally* EX1012; EX1013; EX2014. Ports are a part of upper layer standards (such as UDP and TCP), and are generally understood to be a component of OSI Layer 4 (or higher). *See generally* EX2015; EX2016; EX2013 Because of this, it would not have been obvious to a POSITA to begin adding in attributes to an IPv6 address from a different technology implementing a different layer of the OSI model, regardless of whether there was space available to fit that attribute in. Not all transport layer mechanisms based on IP even utilize the concept of ports.

Furthermore, Petitioner’s analysis ignores the fact that an IPv6 address is limited to 128 bits. Even if a POSITA tried to construct an address, particularly in the context of a larger system or systemic framework, the address bits themselves are a scarce resource even in a larger IPv6 address space; one would not use the address bits unless needed, as they may be needed for other purposes, including other purposes as yet unknown for later applications (which are often reserved for future implementations). Petitioner’s suggestion that it would have been apparent to include port information ignores what one of skill in the art would have recognized; one does not try to use a limited a resource (address bits) without a clear, specific, important purpose in mind.

Therefore, a POSITA would not have found it obvious to alter Ananda in the suggested manner.

(b) Ananda with Wetterwald

Additionally, Wetterwald fails to teach concatenating port information in the IPv6 destination address. Petitioner cites a portion of Wetterwald which suggests (in a single sentence without elaboration) that port information can be added as IPv6 *option headers*. Pet. at 48-49; EX1008 at 8:24-28. An option header is an “extension” header added to a packet that is located separately from the IPv6 header where the destination address is located. EX2014 at 6-7. An option header is not part of the IPv6 address, which is contained within the IPv6 header. EX2014 at 4-6. While Wetterwald cites to RFC2460, RFC2460 does not suggest that port information should be added as option headers—as noted above, the word “port” does not appear in RFC2460. Even if the port was added as an option header in Wetterwald, nothing about that would suggest to a POSITA that it should also be concatenated into the IPv6 destination address. Wetterwald even discusses a method of constructing an IPv6 address in the same paragraph in which it suggests adding the port as an option header—if it were truly obvious to a POSITA to concatenate port information to the IPv6 address, Wetterwald would not have suggested incurring the additional complexity and overhead of adding it as an extension header. EX1008 at 8:6-28; EX2017 at 6 (noting “it is important to evaluate the impact of [Extension Headers]...on the IPv6 forwarding performance of the network device.”). That Wetterwald suggests that the ports be added as costly extension headers and not in the address header further demonstrates that a POSITA would not have viewed it as obvious to add a port number to the IPv6 address.

(c) Ananda with Wetterwald and Teredo

Teredo also fails to teach concatenating destination port information to the IPv6 destination address. Petitioner argues:

It was known in the art to include a port number in a constructed IPv6 address. The Teredo protocol (RFC4380) provided connectivity and integration between IPv4 and IPv6 networks using a “Teredo IPv6 address” that includes “the UDP port and IPv4 address at which a client can be reached.” Ex.1009, 5.

Pet. at 49.

Notably, the quoted portion specifies that the Teredo IPv6 address includes the port “at which a **client** can be **reached**.” EX1009 at 5 (emphasis added). The port at which the client can be reached is not a destination port—it is a ***source*** port. A Teredo IPv6 address includes 5 components:

Prefix	Server IPv4	Flags	Port	Client IPv4
--------	-------------	-------	------	-------------

Id. at 11-12. The only “port” component is “the obfuscated ‘mapped UDP port’ of the Teredo service **at the client**.” *Id.* (emphasis added). Therefore, Teredo also fails to teach the use of *destination* port information when constructing an IPv6 address. Additionally, the IPv6 source address is generated in an IPv4 network by an IPv4 client and included in the IPv4 packet payload. It is not generated in the IPv6 domain based on destination address and port information received from an IPv4 data packet.

Further, the Teredo server that receives the IPv4 packet from the IPv4 client does not construct any IPv6 address (much less an IPv6 destination address) through

a concatenation process. Instead, it simply decapsulates the IPv6 packet from the IPv4 data packet and forwards the decapsulated IPv6 data packet. *Id.* at 11.

4. The asserted grounds do not teach the claimed generating, routing, or extracting limitations (All Independent Claims)

'844 claims 1, 2, and 5 require “generating an IPv6 data packet *from the IPv6 constructed destination address*” and “routing the generated IPv6 data packet in the IPv6 domain *using the IPv6 constructed destination address.*” (emphasis added). '844 claims 3, 4, 6, and 10 require “extracting the IPv4 destination address and the destination port number *from the IPv6 destination address.*” Because the asserted grounds fail to teach the claimed constructed IPv6 destination address (as discussed in §V.A.3), they also fail to teach the limitations which rely on the constructed IPv6 destination address.

5. Petitioner has not asserted its grounds for invalidity with particularity (Ground 1)

35 U.S.C. § 312(a)(3) requires that the Petitioner identify the grounds for each claim challenged with particularity. Petitioner identifies its basis for Ground 1 as “35 U.S.C. § 103 over Ananda, Wetterwald, and RFC4380.” Pet. at 25.

However, Petitioner also relies on additional grounds, including a POSITA's knowledge. *See, e.g.,* Pet. at 45 (“A POSITA would have known that a TCP-formatted packet would include a TCP destination port number.”), 45 (“It was well known for IPv4 data packets to include destination addresses and port numbers.”), 48 (“It would have been well-known to a POSITA that TCP/UDP source and destination port numbers are each just 16 bits long.”).

Because it is not clear whether Petitioner's invalidity grounds are based solely on Ananda, Wetterwald, and RFC4380, or whether it is actually those grounds in further view of a POSITA's knowledge, Petitioner has failed the particularity requirement that "the petition identifies, in writing and with particularity, each claim challenged, [and] the grounds on which the challenge to each claim is based..." 35 U.S.C. §312(a)(3). Even if Patent Owner could infer what Petitioner's intention was, the Board cannot institute on grounds other than those specifically proposed by Petitioner. *See Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1336 (Fed. Cir. 2020). Thus, Petitioner has failed to show a reasonable likelihood of success for Ground 1 (and therefore all independent claims).

6. A POSITA would not have combined Ananda and Wetterwald (All Grounds)

Petitioner relies on Wetterwald for teaching limitations for each of the independent claims. *See, e.g.*, limitations [1.0.2] (Pet. at 45-46), [1.1] (Pet. at 48-49), [3.0.2] (Pet. at 63-64), [3.1] (Pet. at 68). However, Petitioner's proposed combination with Wetterwald is motivated solely by improper hindsight reconstruction and not based on teachings from the references themselves.

Before addressing the flaws in Petitioner's reasoning, it is helpful to understand how dissimilar Ananda and Wetterwald are at a high level, both from the viewpoint of the problems being solved as well as the proposed solutions. As discussed in §II.A, there is no single standardized strategy for transitioning from IPv4 to IPv6, and as a result there is no one-size-fits-all interconnection solution. Throughout its analysis, Petitioner has treated all art that somehow involves a level

of interaction between IPv4 and IPv6 as “combinable,” regardless of the transition strategy being employed or the particular interconnection problem the POSITA was trying to solve.

As discussed in §II.C.1, Ananda proposes a system that allows an organization (such as a corporation or university) to upgrade parts of its domain backbone from IPv4 routers to IPv6 routers without requiring that all hosts within the organization’s network be immediately upgraded to support IPv6. EX1005 ¶¶71-74. The goal of the Ananda invention is to provide an organization with the flexibility regarding when and how it transitions its backbone infrastructure, because transitioning an entire domain to IPv6 all at once might otherwise be cost prohibitive. *Id.* It accomplishes this through the use of CPIs positioned in various subnets within the Ananda domain that encapsulate IPv4 traffic within IPv6 packets, allowing packets from the IPv4 hosts within the subnets to successfully traverse the IPv6 backbone and reach another subnet. *Id.* Abstract, Fig. 2, ¶¶19, 63, 74.

On the other hand, Wetterwald is not trying to provide the same piecemeal transition option as Ananda. As discussed in §II.C.2, Wetterwald seeks to enable mobile hosts to roam between multiple access points within an access network and maintain IP connectivity. EX1008 at 2:55-3:10. Wetterwald accomplishes this through the use of multiple access points which feed DHCP requests and traffic to a single “clusterhead” which assigns addresses to the hosts and provides a single access gateway for transfer of packets between the internal network and the public IPv4 network. *Id.* at 4:46-64, 5:22-58. A POSITA looking to modify Ananda (addressing piecemeal transitioning of infrastructure) would not have looked to

Wetterwald (addressing mobile access connectivity) just because both references discuss utilizing both IPv4 and IPv6 protocols.

Petitioner argues that a POSITA would have combined Ananda with Wetterwald, because:

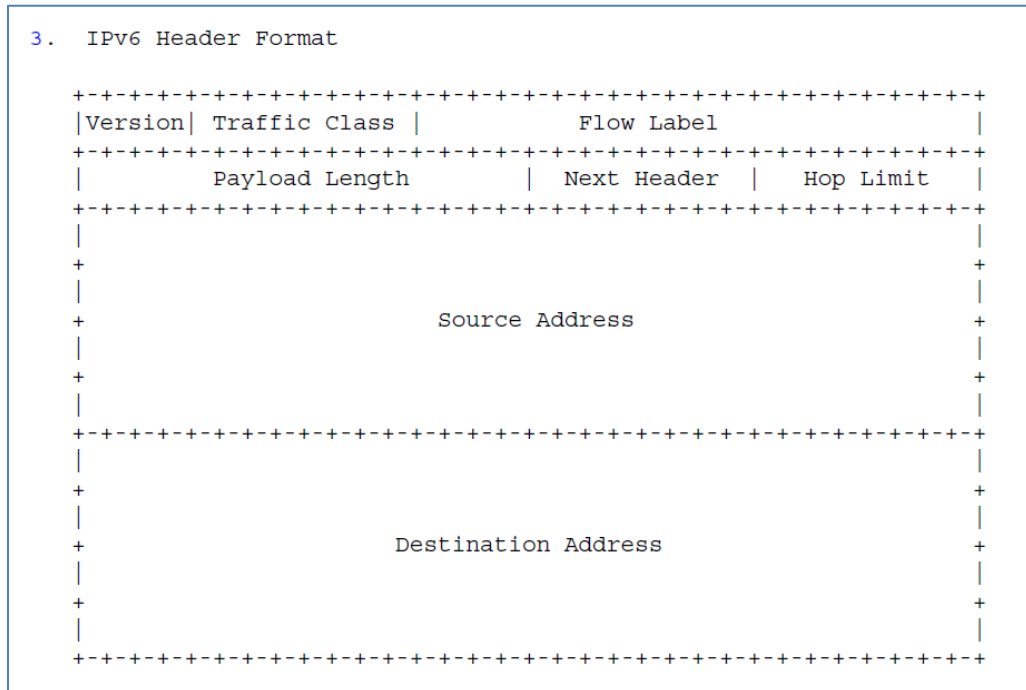
By including port information in the IPv6 address itself, a POSITA would have recognized that the port information could be made available in the IPv6 header without adding an option header (as referenced by Wetterwald) that would increase the overall IPv6 packet size.

Pet. at 49.

Notably, neither Ananda nor Wetterwald teaches reducing overall IPv6 packet size as a goal. Furthermore, Wetterwald suggests including port information in the option extension header (rather than the IPv6 address header) in the same paragraph where it describes constructing the IPv6 address. EX1008 at 8:6-28. If the benefit of including the same port information in the IPv6 address was truly obvious in light of Wetterwald, then Wetterwald would not have suggested adding the port information in a separate extension header, which Petitioner acknowledges “increase[es] the overall IPv6 packet size.” Pet at 49.

Wetterwald references RFC 2460 with regard to the option headers. EX1008 at 8:25-28. The optional “extensions” described in RFC 2460 are in addition to the standard IPv6 header, and thus they do not form part of the IPv6 destination address that is included in the standard IPv6 headers. EX2014 at 4 (showing IPv6 header format with destination address) and 6 (showing other extension headers that are

provided after the IPv6 header). On page 4, RFC 2460 shows the format of an IPv6 header which is where the source address and destination address are found:



With regard to the payload, RFC 2460 states that “any extension headers,” such as those disclosed in Section 4, form part of the payload:

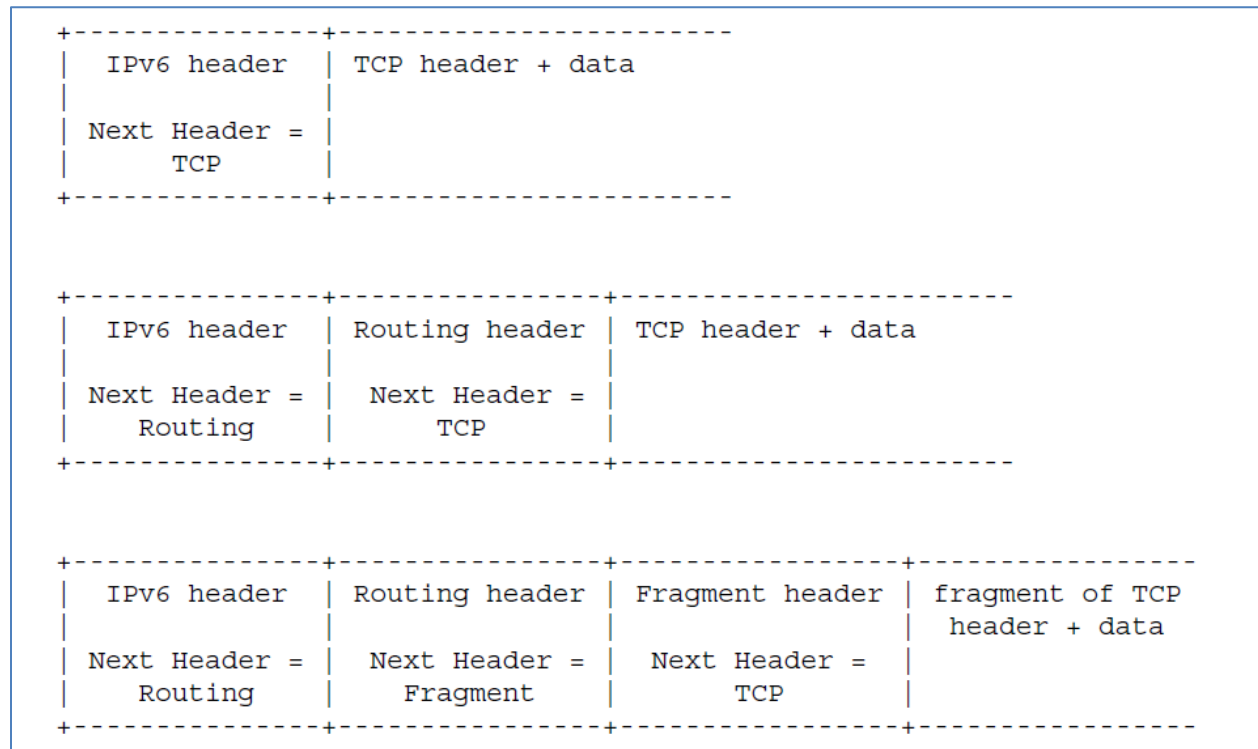
Payload Length 16-bit unsigned integer. Length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header, in octets. (Note that any extension headers [section 4] present are considered part of the payload, i.e., included in the length count.)

EX2014 at 4-5. In Section 4, RFC 2460 reconfirms that any optional information is encoded in separate headers that are distinct from the IPv6 header information where the source and destination IPv6 addresses are located:

4. IPv6 Extension Headers

In IPv6, optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. As illustrated in these examples, an IPv6 packet may carry zero, one, or more extension headers, each identified by the Next Header field of the preceding header:

EX2014 at 6. Examples of these separate extension headers are shown in Section 4:



EX2014 at 6.

The use of additional optional headers in a portion of an IPv6 packet that is separate from the IPv6 headers does not satisfy the claim requirement that this information be provided in the IPv6 destination address. Further, RFC 2460 indicates that any of the header extensions form part of the **payload**, not the IPv6 headers. RFC 2460 at 4-5. Including port information in an IPv6 option header

would thus result in that information being placed in the payload of the IPv6 data packet, not in the IPv6 headers where the IPv6 destination address must be located. See EX2014 at 4-6.

Thus, Petitioner's conclusion that it would have been obvious to include the port information in the IPv6 address is based purely on hindsight bias, and not based on anything in the references themselves.

Petitioner's other justifications for looking to Wetterwald are similarly unavailing. Petitioner suggests:

A POSITA would have been motivated to modify Ananda's IPv6 address construction technique to incorporate a destination port number in the IPv6 address, as taught by Wetterwald and RFC4380, for the same reasons that the Teredo protocol incorporates a port number in an IPv6 address.

Pet. at 49. However, in the same page Petitioner conceded that Wetterwald does not teach incorporating destination port information in the IPv6 address, it teaches the port information should be added to a separate header. How could a POSITA be motivated to use Wetterwald for something which it does not even teach?

Finally, in regards to Claim 5's "means for constructing an IPv6 destination address" limitation, Petitioner argues:

To assist with maintaining port number information and performing 'IPv6-to-IPv4 translations and vice versa' (Ex.1008, 6:38-47), it would have been obvious to a POSITA to modify Ananda's CPI 215E to store within its memory a NAT table, like that taught by Wetterwald, for translating addresses.

Pet. at 73; *see also* Pet. at 79-80.

As discussed above in §IV.B, and as the District Court found in the parallel litigation, the corresponding structure for the means plus function limitation does not include a NAT state table. One of the benefits of constructing the IPv6 address in the claimed manner is to enable interconnection between IPv6 and IPv4 “without having recourse to state tables that are laborious to maintain.” EX1001 at 3:46-52, 6:13-20. Petitioner’s argument that a POSITA would have looked to Wetterwald to add additional NAT state tables that the invention enables the POSITA to avoid using is nonsensical. Therefore, Petitioner has identified no reason for a POSITA to look to Wetterwald to combine with or improve on Ananda.

7. A POSITA would not have combined Ananda and Wetterwald with Teredo (All Grounds)

Petitioner argues under all grounds that a POSITA would have combined Ananda, Wetterwald, and Teredo (RFC4380), but fails to carry its burden of demonstrating why a POSITA would have made the proposed combination. Pet. at 25, 36. In fact, a POSITA would not have made the proposed combination, at least because a POSITA would not have looked to Teredo to improve Ananda or Wetterwald due to the significant drawbacks and limited usefulness in utilizing the teachings of Teredo.

First, Teredo describes itself as an “‘IPv6 access of last resort’ to nodes that need IPv6 connectivity but cannot use any of the other IPv6 transition schemes.” EX1009 at 8, 36 (“[I]t is important that it should not be used any longer than necessary.”). Thus, even the reference itself repeatedly teaches away from its own use—a fact Petitioner never addresses.

The reason that Teredo repeatedly admonishes against its own use is clear: using the teachings of Teredo to provide IPv6 access introduces *significant* shortcomings and vulnerabilities that would *not* motivate a POSITA to look to it to improve other art. Furthermore, the teachings of Teredo are only intended for use in tunneling through NATs. EX1009 at 9 (“Teredo is meant as a short-term solution to the specific problem of providing IPv6 service to nodes located behind a NAT.”). Despite this limitation, Teredo does not even work for some common NAT types (such as symmetric NAT). EX1009 at 6-7, 10, 49. Petitioner does not explain why a POSITA looking to improve Ananda and Wetterwald would look to a “last resort” technology limited to use with NATs that is not even usable with common types of NATs.

Second, one of the goals of both Ananda and Wetterwald was to provide a solution that was transparent to host machines while enabling interconnectivity between IPv4 and IPv6 client devices. EX1005 ¶64 (“The present invention, as described below, advantageously supports transparent operation of both IPv4 and IPv6 in multi-protocol subnets of a communication network of an organization....This enables a gradual adoption and transition of an organization from IPv4 to IPv6 without the need for modifications to be made to end or destination host(s), and independent of the various operating systems...”); EX1008 at 3:21-23 (“[A]n IPv4 host can continue using an assigned DHCP address as it moves throughout the access network in a manner that is transparent to nodes outside the access network.”). Teredo requires modifications to be made to a host that is intended to make use of its system—a POSITA looking to maintain the transparency

benefit of Ananda and Wetterwald would not have looked to Teredo because it requires making modifications to the operation of the hosts. *See, e.g.*, EX1009 at 10-11, 16-17 (describing operations that must be performed by the Teredo client). As discussed in §II.C.3, Teredo clients must be modified to interact with Teredo servers and relays, and the clients even have to construct their own IPv6 source address. The whole point of using a solution like that proposed by Ananda was to allow organizations to begin transitioning to IPv6 while still avoiding making these types of modifications to the end hosts. EX1005 ¶¶71-73 (noting an obstacle of implementing IPv6 was that it “necessitates modifications to all existing end components, and the costs associated with conducting modifications on this scale is prohibitive. Such costs provide little motivation on the part of an organization to change from IPv4 to IPv6.”).

Next, the performance degradations introduced by Teredo would make it unsuitable for integration with Wetterwald, due to Wetterwald’s emphasis on transporting latency-sensitive data. Implementing the teachings of Teredo introduces significant additional overhead to a system, requiring additional control and relay servers, and requiring administrators to try to balance the load on individual servers. EX1009 at 9, 47-49. Teredo also introduces undesirable performance degradations, such as jitter—a term used to describe high variability in packet latency. “Teredo introduces jitter into the IPv6 service it provides, due to the queuing of packets while bubble exchanges take place. This jitter can negatively impact applications, particularly latency sensitive ones, such as Voice over IP (VoIP).” *Id.* at 49. One of the stated goals of Wetterwald was to better support “latency-sensitive data streams

(e.g., Voice over IP).” EX1008 at 3:24-28, 5:64-67, 9:65-10:3. Therefore, a POSITA would not have looked to Teredo to improve Wetterwald because the deleterious effect it has on packet latency runs counter to Wetterwald’s goal of better supporting latency sensitive streams.

Furthermore, implementing the teachings of Teredo introduces significant additional risks, including increased risk of: (1) denial of service attacks (EX1009 at 10, 29, 44-45) and (2) spoofing attacks (*id.* at 39-41). A POSITA would not generally look to improve a networking technology with another technology that makes it significantly more vulnerable to attack. Despite those significant risks, the only motivation to combine with Teredo identified by Petitioner was that its teachings could be used to detect spoofed traffic.

Petitioner argues:

A POSITA would have been motivated to modify Ananda’s IPv6 address construction technique to incorporate a destination port number in the IPv6 address, as taught by Wetterwald and RFC4380, for the same reasons that the Teredo protocol incorporates a port number in an IPv6 address. Ex.1003, ¶ 107. For example, Teredo protocol uses the port number included in the IPv6 address to detect potentially fraudulent (“spoofed”) traffic[.]

Pet. at 49.

However, susceptibility to spoofing is an issue *exacerbated* by the Teredo architecture, not solved by it. Because Teredo introduces additional servers that clients must interact with (Teredo Servers and Teredo Relays), those same servers are also potential vectors for spoofing attacks. See EX1009 at 39-41 (“7.2.1. Attacker

Spoofing the Teredo Server”), 41 (“7.2.2. Attacker Spoofing a Teredo Relay”). For example, “[a]n attacker may try to use Teredo either to pass itself for another IPv6 host or to place itself as a man-in-the-middle between a Teredo host and a native IPv6 host. The attacker will mount such attacks by spoofing a Teredo relay, i.e., by convincing the Teredo host that packets bound to the native IPv6 host should be relayed to the IPv4 address of the attacker.” *Id.* at 41. A POSITA generally would not look to a given reference to solve a problem that the reference itself introduced or made more severe.

Petitioner claims that “Teredo protocol uses the port number included in the IPv6 address to detect potentially fraudulent (“spoofed”) traffic.” Pet. at 49-50 (citing EX1009 at 22-23). However, even the cited portion makes clear that Teredo’s port and address comparison is a haphazard proposal at best—Teredo requires that some packets be accepted even when “the mapped IPv4 address and mapped port in the source address do not match the source IPv4 address and source port of the packet”:

5) If the source IPv6 address is a Teredo address, and **the mapped IPv4 address and mapped port in the source address do not match the source IPv4 address and source port of the packet, the client checks whether there is an existing “local” entry for that IPv6 address. If there is such an entry**, and if the local IPv4 address and local port indicated in that entry match the source IPv4 address and source port of the packet, the client updates the “local” entry, whose status should be set to “trusted”. If the packet is a bubble, it should be discarded after this processing; otherwise, **the packet should be accepted**. In all cases,

the client must de-queue and forward any packet queued for that destination.

6) In the other cases, the packet may be accepted, but **the client should be conscious that the source address may be spoofed**; before processing the packet, the client should perform the “direct IPv6 connectivity test” described in Section 5.2.9.

EX1009 at 23.

Thus, it is clear even from the cited reference that a POSITA would not look to Teredo to detect spoofed traffic, because (1) Teredo introduces new spoofing vulnerabilities due to the use of Teredo Servers and relays, and (2) the proposed method of detecting spoofed traffic is only viable in a subset of use cases. When combined with the other advertised downsides of using Teredo (which even its creator considered to be a “last resort”), Petitioner has not shown that a POSITA would look to Teredo to improve Ananda and/or Wetterwald.

B. The Board Should Exercise Its Discretion to Deny the Petition under § 314(a)

Patent Owner asserted the '844 Patent against Petitioner in the parallel proceeding *Monarch Networking Sols. LLC v. Cisco Sys. Inc.*, No. 2:20-cv-00015-JRG (E.D. Tex.) (filed Jan. 21, 2020). Given the advanced stage of the litigation—which addresses the same issues raised in the instant Petition—the Board should deny institution, as institution would constitute an inefficient duplication of ongoing litigation. Under § 314(a), the Director has discretion to deny institution. *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2140 (2016).

The Board considers the presence and status of parallel district court litigation in determining whether to deny institution. *See NHK Spring Co. Ltd. v. Intri-Plex Techs. Inc.*, IPR2018-00752, Paper 8, at 20 (P.T.A.B. Sept. 12, 2018) (precedential); *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15, at 17 (P.T.A.B. May 13, 2020)(informative); *see also Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19, at 16-17 (P.T.A.B. Sept. 6, 2017) (“[W]e recognize that an objective of the AIA is to provide an effective and efficient alternative to district court litigation”). *Fintiv* “sets forth factors that balance considerations of system efficiency, fairness, and patent quality when a patent owner raises an argument for discretionary denial due to the advanced state of a parallel proceeding.” *Fintiv*, IPR2020-00019, Paper 15, at 7-8 (citing *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11, at 5-6 (P.T.A.B. Mar. 20, 2020) (precedential)). The factors are:

1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
2. proximity of the court’s trial date to the Board’s projected statutory deadline for a final written decision;
3. investment in the parallel proceeding by the court and the parties;
4. overlap between issues raised in the petition and in the parallel proceeding;
5. whether the petitioner and the defendant in the parallel proceeding are the same party; and
6. other circumstances that impact the Board’s exercise of discretion, including the merits.

Id. These factors favor a discretionary denial under § 314(a).

Factor 1: The parallel proceeding is ongoing in front of Judge Gilstrap in the Eastern District of Texas. “District courts [in EDTX] typically consider three factors

when determining whether to grant a stay pending inter partes review of a patent in suit: (1) whether the stay will unduly prejudice the nonmoving party, (2) whether the proceedings before the court have reached an advanced stage, including whether discovery is complete and a trial date has been set, and (3) whether the stay will likely result in simplifying the case before the court.” *Solas OLED Ltd. v. Samsung Display Co.*, No. 2:19-CV-00152-JRG, 2020 U.S. Dist. LEXIS 125973, at *3 (E.D. Tex. July 17, 2020) . Based on these factors, it is unlikely that Judge Gilstrap would grant a stay in the parallel proceeding.

First, a stay would unduly prejudice Monarch. Monarch’s Preliminary Response deadline is February 16, 2021. If an institution decision issues three months after that date (*see* 35 U.S.C. § 314(b)), it would be May 16, 2021 before the parties know whether institution will occur. By that point, both fact and expert discovery will be completed in the district court action, meaning Monarch will have already incurred the majority of expenses associated with the litigation—which Judge Gilstrap has previously found to be a sufficient showing of prejudice. *See Solas*, 2020 U.S. Dist. LEXIS 125973, at *4-6.

Under the amended Docket Control Order, fact discovery closed on January 12, 2021, and expert discovery closes on February 19, 2021. *See* EX2012 at 3. These dates occur well before the likely date for an institution decision, and expenses relating to fact and expert discovery already will have been incurred by the parties.

Second, the parallel proceeding will have reached an advanced stage before an institution decision is reached. As noted above, all discovery will be completed by February 19, 2021. Jury Selection is scheduled for early June 7, 2021. *See*

EX2012 at 1. Judge Gilstrap has previously held that even when a party is diligent about filing an IPR, if claim construction has been completed and all discovery is closed, then the factor still favors denial of a stay. *See Solas*, 2020 U.S. Dist. LEXIS 125973, at *6-7.

Third, even if this proceeding would simplify issues for trial, Judge Gilstrap has held that consideration alone does not outweigh the prejudice to the non-moving party and the advanced stage of the proceeding. *See id.* at *7-9. It is unlikely a stay would be granted if institution occurred, and thus this factor favors denial.

Factor 2: Trial is scheduled to start on June 7, 2021. EX2012 at 1. If the Board reaches its institution decision within three months of receiving the preliminary response, 35 U.S.C. § 314(b), and issues a final written decision within 1 year of institution, 35 U.S.C. § 316(a)(11), a final written decision would likely issue in May 2022—almost one year after the expected conclusion of the district court litigation in June 2021. The parties are days away from completing discovery; none of the hypothetical delay scenarios suggested by Cisco could reasonably be expected to result in a nine-month delay of the trial date. EX2012 at 3. This factor favors exercising discretion to deny the Petition.

Factor 3: For the same reasons discussed above, this factor also favors denial. The parties have received the Court's claim construction order, Cisco has submitted its 694-page invalidity expert report in the district court case, and by the time the institution decision issues the parties will have completed discovery, filed all dispositive motions, and incurred all costs thereof. Both the Court and the parties

have already made significant investments in the litigation. Thus, this factor favors denial.

Factor 4: As Petitioner concedes, Petitioner asserted the same invalidity grounds in the parallel proceeding. Pet. at 30. Petitioner conceded that the same grounds are part of Petitioner’s invalidity contentions, and Cisco has only offered to “cease asserting in the district court litigation the combination of references on which trial is instituted for the claims on which trial is instituted, while trial is instituted.” Petition at 30. Such a narrow stipulation favors exercising discretionary denial. As the Board noted in its precedential opinion in *Sotera Wireless, Inc. v. Masimo Corporation*, IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020), what is important is whether the “Petitioner broadly stipulates to not pursue ‘*any ground* raised or that could have been reasonably raised.’” *Id.* at 19 (emphasis in original). Petitioner’s overly narrow stipulation does little to “address[] concerns of duplicative efforts and potentially conflicting decisions” in the litigation. *Id.* Thus, in the absence of a meaningful stipulation, the significant overlap between the proceedings favors discretionary denial.

Factor 5: Petitioner is the Defendant in the parallel litigation. Under the Board’s precedential *Sotera* opinion, when the parties are the same this factor supports denying institution. *Sotera*, IPR2020-01019, Paper 12 at 19.

Factor 6: As discussed above, the merits of this Petition are particularly weak. Petitioner has failed to present references or combinations that disclose the claimed IPv4 domain and IPv6 domain under both parties’ proposed constructions. Additionally, Petitioner’s proposed IPv6 address construction combination fails to

identify an operator prefix (under its requested construction in a parallel proceeding) or destination port information in any reference. Further, Petitioner fails to present a reasonable motivation to combine the proposed references and the proposed combinations still fail to disclose or teach limitations present in every challenged claim. Therefore, this factor favors denial.

On balance, the *Fintiv* factors favor discretionary denial because costly litigation discovery will be complete approximately three days from the filing of this Preliminary Response.

VI. Conclusion

Patent Owner respectfully requests that the Board deny institution of *inter partes* review for the reasons stated herein.

Dated: February 16, 2021

Respectfully submitted,
By: /Michael F. Heim/
Michael F. Heim (Reg. No. 32,702)
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 PRELIMINARY RESPONSE UNDER 37 C.F.R. § 42.107 TO PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 8,451,844 was served via email to lead and backup counsel of record for Petitioners as follows:

Lead Counsel for Petitioner	
Theodore M. Foster (Reg. No. 57,456) HAYNES AND BOONE, LLP 2323 Victory Ave., Suite 700 Dallas, TX 75219	Phone: 972-739-8649 Fax: 214-200-0853 ipr.theo.foster@haynesboone.com
Back-Up Counsel for Petitioner	
David L. McCombs (Reg. No. 32,271) HAYNES AND BOONE, LLP 2323 Victory Ave., Suite 700 Dallas, TX 75219	Phone: 214-651-5533 Fax: 214-200-0853 david.mccombs.ipr@haynesboone.com
Jonathan R. Bowser (Reg. No. 54,574) HAYNES AND BOONE, LLP 2323 Victory Ave., Suite 700 Dallas, TX 75219	Phone: 202-654-4503 Fax: 214-200-0853 jon.bowser.ipr@haynesboone.com

Dated: February 16, 2021

Respectfully submitted,

By: /Michael F. Heim/

Michael F. Heim (Reg. No. 32,702)

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 13,980 words.

Dated: February 16, 2021

Respectfully submitted,

By: /Michael F. Heim/

Michael F. Heim (Reg. No. 32,702)

Attorney for Patent Owner

Monarch Networking Solutions LLC