

Filed: March 5, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. and FORTINET, INC.,
Petitioner,

v.

INFOEXPRESS INC.,
Patent Owner.

IPR2024-00539
U.S. Patent No. 8,051,460

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 8,051,460**

TABLE OF CONTENTS

	Page
Table of Authorities.....	i
Exhibit list.....	ii
I. INTRODUCTION	1
II. MANDATORY NOTICES	1
A. Real Party-in-Interest	1
B. Related Matters.....	1
C. Lead and Back-Up Counsel and Service.....	2
III. PAYMENT OF FEES	3
IV. REQUIREMENTS FOR <i>INTER PARTES</i> REVIEW	3
A. Grounds for Standing	3
B. Identification of Challenged Claims	3
V. THE 460 PATENT	4
A. Effective Filing Date	4
B. Person of Ordinary Skill in the Art.....	4
C. Overview of the 460 Patent	4
VI. CLAIM CONSTRUCTION	7
VII. PRINCIPAL PRIOR ART.....	7
A. Summary of Krantz	7
B. Summary of Herrmann.....	10
VIII. CLAIMS 1-6, 10-14, 16-22, 27, and 29-30 ARE UNPATENTABLE	13
A. Ground 1: Claims 1-2, 10-14, 16-17, 27, and 29-30 are Obvious Based on Krantz.....	13
1. Claim 1	13
i. [1.0] A method of granting access to a protected network, the method comprising:	13
ii. [1.1] receiving a request for access to a less-restricted subset of the protected network from an access device,..	19
iii. [1.2] the request received through a communication port of an access point,.....	23

iv.	[1.3] the communication port configured for communicating between the access device and a restricted subset of the protected network, ...	26
v.	[1.4] the restricted subset including a gatekeeper; applying a security policy to the access device in response to the request; using the gatekeeper to determine if requirements of the security policy are satisfied by the access device, and	36
vi.	[1.5] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when the requirements of the security policy are satisfied.	40
2.	Claim 2	47
i.	[2.0] The method of claim 1, further comprising authenticating a user of the access device.	47
3.	Claim 10	48
i.	[10.0] The method of claim 1, wherein the access point is a network switch.	48
4.	Claim 11	49
i.	[11.0] The method of claim 1, wherein the access point is a wireless access point.	49
5.	Claim 12	49
i.	[12.0] The method of claim 1, wherein the access point is a remote access virtual private network.	49
6.	Claim 13	51
i.	[13.0] The method of claim 1, wherein the gatekeeper is accessible to elements of the less-restricted subset of the protected network.	51
7.	Claim 14	52
i.	[14.0] The method of claim 1, wherein the restricted subset of the protected network is characterized by an access control list.	52
8.	Claim 16	53

i.	[16.0] A non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor to perform a method for controlling access to a computer network, the method comprising:	53
ii.	[16.1] receiving a request for access to a less-restricted subset of the protected network from an access device, ...	55
iii.	[16.2] the request being received through a communication port of an access point, ...	55
iv.	[16.3] the communication port configured for communicating between the access device and a restricted subset of the protected network, ...	55
v.	[16.4] the restricted subset including a gatekeeper; applying a security policy to the access device in response to the request; and	55
vi.	[16.5] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when requirements of the security policy are satisfied.	55
9.	Claim 17	55
i.	[17.0] The non-transitory computer readable storage medium of claim 16, wherein the program is further executable by a processor to authenticate a user of the access device.	55
10.	Claim 27	56
i.	[27.0] The non-transitory computer readable storage medium of claim 16, wherein the program is further executable to update the access device when requirements of the security policy are not satisfied.	56
11.	Claim 29	57
i.	[29.0] The non-transitory computer readable storage medium of claim 16, wherein the restricted subset of the protected network is characterized by an access control list.	57
12.	Claim 30	57

i.	[30.0] The non-transitory computer readable storage medium of claim 29, wherein access to the restricted subset of the protected network is responsive to a VLAN configured to communicate with the protected network subject to the access control list.	57
B.	Ground 2: Claims 1-6, 10-14, 16-22, 27, and 29-30 are Obvious Based on Krantz and Herrmann.....	58
1.	Claims 1-2, 10-14, 16-17, 27, and 29-30	58
2.	Claim 3	66
i.	[3.0] The method of claim 1, further comprising obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.....	66
3.	Claim 4	68
i.	[4.0] The method of claim 3, wherein the system data includes antivirus software status.	68
4.	Claim 5	70
i.	[5.0] The method of claim 1, further comprising communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and	70
ii.	[5.1] wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.....	74
5.	Claim 6	74
i.	[6.0] The method of claim 5, wherein the system data includes information regarding devices connected to the access device.....	74
6.	Claim 18	77
i.	[18.0] The non-transitory computer readable storage medium of claim 16, ...	77
ii.	[18.1] wherein the program is further executable by a processor to obtain system data from the access device, and.....	77

iii.	[18.2] wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.....	77
7.	Claim 19.....	77
i.	[19.0] The non-transitory computer readable storage medium of claim 18, wherein the system data includes antivirus software version data.	77
8.	Claim 20.....	77
i.	[20.0] The non-transitory computer readable storage medium of claim 16,.....	77
ii.	[20.1] wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and	78
iii.	[20.2] wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.....	78
9.	Claim 21	78
i.	[21.0] The non-transitory computer storage readable medium of claim 20, wherein the system data includes information regarding devices connected to the access device.	78
10.	Claim 22.....	78
i.	[22.0] The non-transitory computer readable storage medium of claim 16, wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset.....	78
IX.	THE BOARD SHOULD NOT EXERCISE ITS DISCRETION AND DENY INSTITUTION.....	81
A.	The Board Should Not Deny Institution Under 35 U.S.C. § 325(d) ...	81
B.	The Board Should Not Deny Institution Under 35 U.S.C. § 314(a)....	81
1.	No Evidence Regarding a Stay	81
2.	Parallel Proceeding Trial Date	82

3.	Parallel Proceeding Investment.....	82
4.	Overlapping Issues with the Parallel Proceeding.....	83
5.	Overlapping Parties.....	83
6.	Strength of Petition and Other Considerations	83
X.	CONCLUSION.....	84
	Certificate of Compliance	85
	Certificate of Service	86

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>Amazon Web Services et al. v. Zentian Ltd.</i> , IPR2023-01194, Paper 10 (Jan. 10, 2024).....	92
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 15 at 12 (May 13, 2020).....	83
<i>InfoExpress Inc. v. Cisco Systems, Inc.</i> , 4-23-cv-02698 (NDCA).....	1
<i>InfoExpress Inc. v. Fortinet, Inc.</i> , 4-23-cv-04389 (NDCA).....	1
<i>Samsung Bioepis Co. Ltd v. Regeneron Pharmaceuticals, Inc.</i> , IPR2023-00739, Paper 9 (Oct. 20, 2023)	84
<i>Vivid Techs., Inc. v. Am. Sci. & Eng.'s. Inc.</i> , 200 F.3d 795, 803(Fed. Cir. 1999)	6

Statutes

35 U.S.C. § 102(e)	6, 9
35 U.S.C. §103	1, 3, 15
35 U.S.C. § 314(a)	83
35 U.S.C. § 325(d)	83

Other Authorities

37 C.F.R. § 42.6(e).....	88
37 C.F.R. § 42.24	87
37 C.F.R. § 42.100(b)	6

EXHIBIT LIST

No.	Exhibit Description
1001	U.S. Patent No. 8,051,460
1002	U.S. Patent No. 8,051,460 File History
1003	Declaration of Henry Houh, Ph.D
1004	CV of Henry Houh, Ph.D
1005	U.S. Patent Pub. No. 2004/0111520 to Krantz et al
1006	U.S. Patent Pub. No. 2004/0107360 to Herrmann et al
1007	IEEE Std 802.1Q-1998 – IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
1008	U.S. Patent No. 6,430,621 to Srikanth et al.
1009	U.S. Patent No. 6,032,194 to Gai et al.
1010	Cisco IOS 12.0 Switching Services (1999)
1011	Microsoft Computer Dictionary 5 th Edition (2002)
1012	Webster’s New World Computer Dictionary (2001)
1013	Dictionary of Computer and Internet Terms 8 th Edition (2003)
1014	U.S. Patent No. 5,987,611 to Freund
1015	U.S. Patent No. 7,260,726 to Doe et al
1016	RFC 2716 – PPP EAP TLS Authentication Protocol
1017	Wireless security with 802.1x and PEAP (2003)

I. INTRODUCTION

Petitioner (Cisco Systems, Inc. and Fortinet, Inc.) submits this Petition for *Inter Partes* Review of claims 1-6, 10-14, 16-22, 27 and 29-30 (the “Challenged Claims”) of U.S. Patent No. 8,051,460 (the “460 Patent” (Ex.1001)), assigned to Patent Owner, InfoExpress Inc. Petitioner submits that the Challenged Claims of the 460 Patent are unpatentable under 35 U.S.C. §103 in view of the references discussed herein.

II. MANDATORY NOTICES

A. Real Party-in-Interest

The real parties-in-interest for this Petition are Cisco Systems, Inc. and Fortinet, Inc.

B. Related Matters

The 460 Patent is asserted by Patent Owver in the following matters:

- *InfoExpress Inc. v. Fortinet, Inc.*, 4-23-cv-04389 (NDCA)
- *InfoExpress Inc. v. Cisco Systems, Inc.*, 4-23-cv-02698 (NDCA)

C. Lead and Back-Up Counsel and Service

Lead Counsel	Back-Up Counsel
Scott M. Border (Reg. #77,744) Winston & Strawn LLP 1901 L Street, N.W. Washington, D.C. 20036 Tel: (202) 282-5054 Fax: (202) 282-5100 sborder@winston.com	Joseph C. Masullo (<i>pro hac vice</i> to be submitted) Winston & Strawn LLP 1901 L Street, N.W. Washington, D.C. 20036 Tel: (202) 282-5897 Fax: (202) 282-5100 jmasullo@winston.com
Back-Up Counsel	Back-Up Counsel
Patrick D. McPherson (Reg. No. 46,255) DUANE MORRIS LLP, 901 New York Avenue N.W., Suite 700 East Washington, DC 20001 Tel: (202) 776-7800 Fax: (202) 776-7801 PDMcPherson@duanemorris.com	Patrick Muldoon (Reg. No. 47,343) DUANE MORRIS LLP, 901 New York Avenue N.W., Suite 700 East Washington, DC 20001 Tel: (202) 776-7840 Fax: (202) 776-7801 PCMuldoon@duanemorris.com
Back-Up Counsel	
David C. Dotson (Reg. No. 59,427) DUANE MORRIS LLP 1075 Peachtree Street NW, Suite 1700 Atlanta, GA 30309-3929 Tel: (404) 253-6982 Fax: (404) 581-5951 DCDotson@duanemorris.com	

Petitioner consents to electronic service by email at WS-Cisco-InfoExpress@winston.com and the e-mail addresses listed above.

III. PAYMENT OF FEES

Petitioner authorizes the Office to charge the filing fee and any other necessary fee to Deposit Account No. 501814.

IV. REQUIREMENTS FOR *INTER PARTES* REVIEW

A. Grounds for Standing

Petitioner (*i.e.*, Cisco and Fortinet) certifies that the 460 Patent is available for *inter partes* review. Petitioner is not barred or estopped from requesting an *inter partes* review challenging the claims on the identified grounds herein.

Petitioner has not filed a civil action challenging the validity of a claim of the 460 Patent. This petition is being filed no more than 1 year after the date on which Petitioner was served with a complaint alleging infringement of the 460 Patent.

B. Identification of Challenged Claims

Ground 1: Claims 1-2, 10-14, 16-17, 27, and 29-30 are unpatentable as obvious under 35 U.S.C. § 103 based on Krantz (Ex.1005).

Ground 2: Claims 1-6, 10-14, 16-22, 27, and 29-30 are unpatentable as obvious under 35 U.S.C. § 103 based on Krantz in view of Herrmann (Ex.1006).

V. THE 460 PATENT

A. Effective Filing Date

Petitioner assumes for the purposes of this Petition that **September 24, 2003**, is the effective filing date.

B. Person of Ordinary Skill in the Art

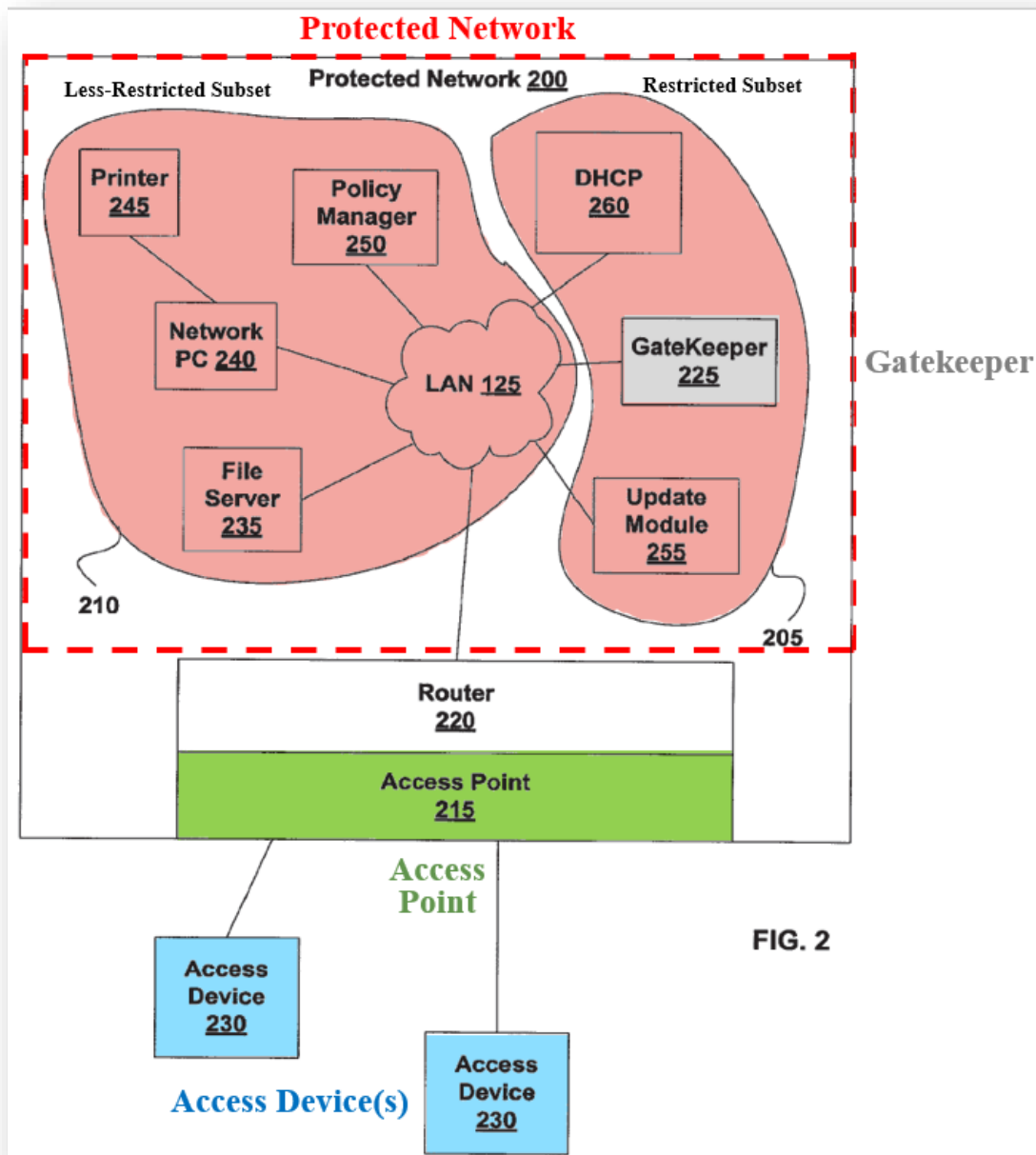
A Person of Ordinary Skill in The Art (“POSITA”) in September 2003 would have had a working knowledge of the telecommunications and networking art that is pertinent to the 460 Patent. A POSITA would have had a bachelor’s degree in computer science, computer engineering, or an equivalent, and two years of relevant experience in networking and network security, and related fields. Lack of professional experience can be remedied by additional education, and vice versa. Ex.1003, ¶21.

C. Overview of the 460 Patent

The 460 Patent describes “a protected network physically or logically divided into a restricted subset and one or more less-restricted subsets.” Ex.1001, 2:53-54. Access to less-restricted networks from a device “are first passed to the restricted subset.” Ex.1001, 2:54-56. Elements of the “restricted subset”—such as a “gatekeeper”—“apply security policies” to the device requesting access. Ex.1001, 2:56-58. If the requesting device satisfies the “security policies,” access is then granted “to a less-restricted subset of the protected network.” Ex.1001,

2:58-60. The 460 Patent explains that both “the passing of access requests to the restricted subset” and the subsequent granting of such requests is “accomplished by configuring and reconfiguring a communication port of an access point.” Ex.1001, 2:61-63.

Figure 2 depicts embodiments of the invention described in the 460 Patent:



Ex.1001, Fig. 2 (annotated); Ex.1003, ¶33.

Figure 2 includes “Protected Network 200,” which is “either physically or logically divided into a Restricted Subset 205 and a Less-Restricted Subset 210.”

Ex.1001, 5:55-58. Access to Protected Network 200 is “under the control of a

GateKeeper 225,” which “enforce[s] a security policy against one or more Access Device 230 requesting access.” Ex.1001, 5:59-64. A security policy may proscribe up-to-date virus software and encryption protocols, (Ex.1001 2:18-26), include requirements related to user identification and passwords or configuration requirements related to the access device (such as aspects of the operating system), (Ex.1001, 6:38-52), or authenticate an access device (or user) of the access device. Ex.1001, 11:35-43, 12:4-6.

VI. CLAIM CONSTRUCTION

Claims are given their “ordinary and customary meaning” as understood by a POSITA and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b). Because a POSITA would find the challenged claims unpatentable under any interpretation consistent with their plain and ordinary meaning in the context of the 460 Patent, the Board need not expressly construe the claim terms. *See Vivid Techs., Inc. v. Am. Sci. & Eng. 'g. Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

VII. PRINCIPAL PRIOR ART

A. Summary of Krantz

U.S. Patent Pub. No. 2004/0111520 to Krantz et al. was filed on December 6, 2002, and published on June 10, 2004. Krantz is prior art to the 460 Patent at least under 35 U.S.C. § 102(e).

Krantz is directed to facilitating controlled access to protected networks and in particular, “increasing the level of automation when provisioning and configuring a computer system to access a network.” Ex. 1005, [0015].

Krantz teaches a system in which a device attempts to access a protected network. Ex.1005, [Abstract]. To gain access to such a protected network, Krantz includes a server which can authorize access to the protected network resources based on credentials supplied by the device or user. Ex.1005, [0016], [0068]-[0071], [0099], [0104], [0107]-[0109]. An embodiment of this network architecture is depicted below:

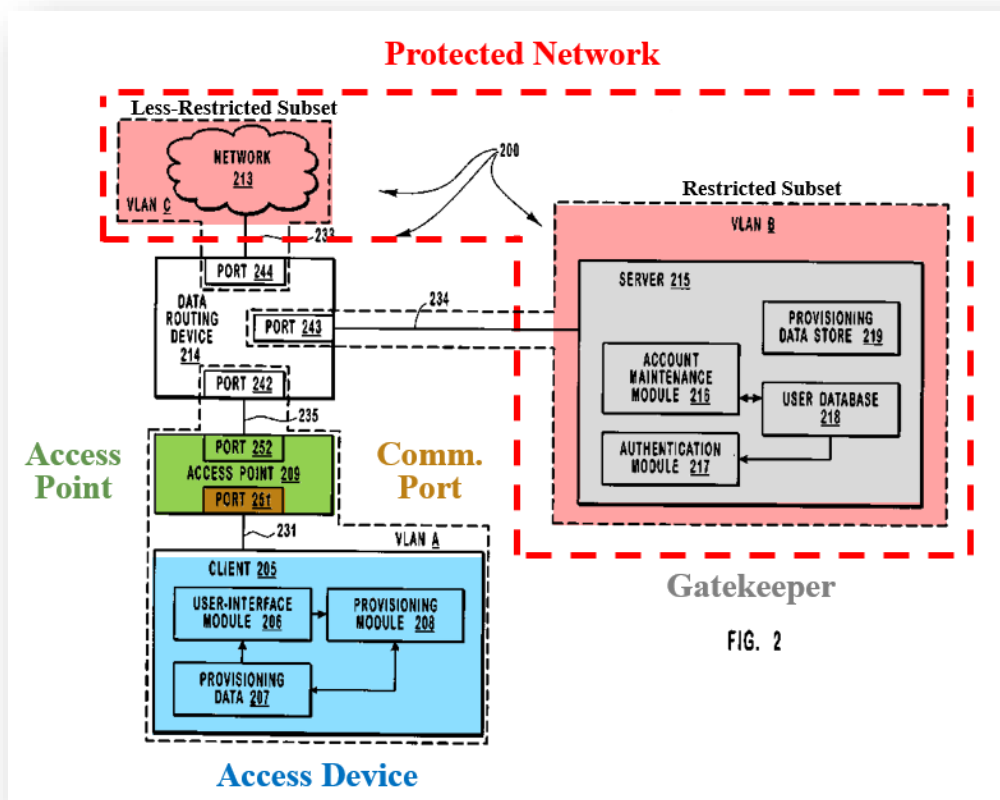


FIG. 2

Ex.1005, Fig. 2 (annotated).

Krantz utilizes Virtual Local Area Network (“VLAN”) techniques. Ex.1005, [0057]. Krantz discloses that “network architecture 200 data routing device 214 is connected to network 213, server 215, and access point 209 by corresponding logical communication links 233, 234, and 235 respectively. Network 213 can be virtually any type of network, such as, for example, a corporate or enterprise-wide network ... [and] data routing device 214 can be a device capable of grouping computer systems together in a single broadcast domain based on criteria other than physical location.” Ex.1005, [0060]. Access Point 209 utilizes ports which can be configured for data transfer. Ex.1005, [0062].

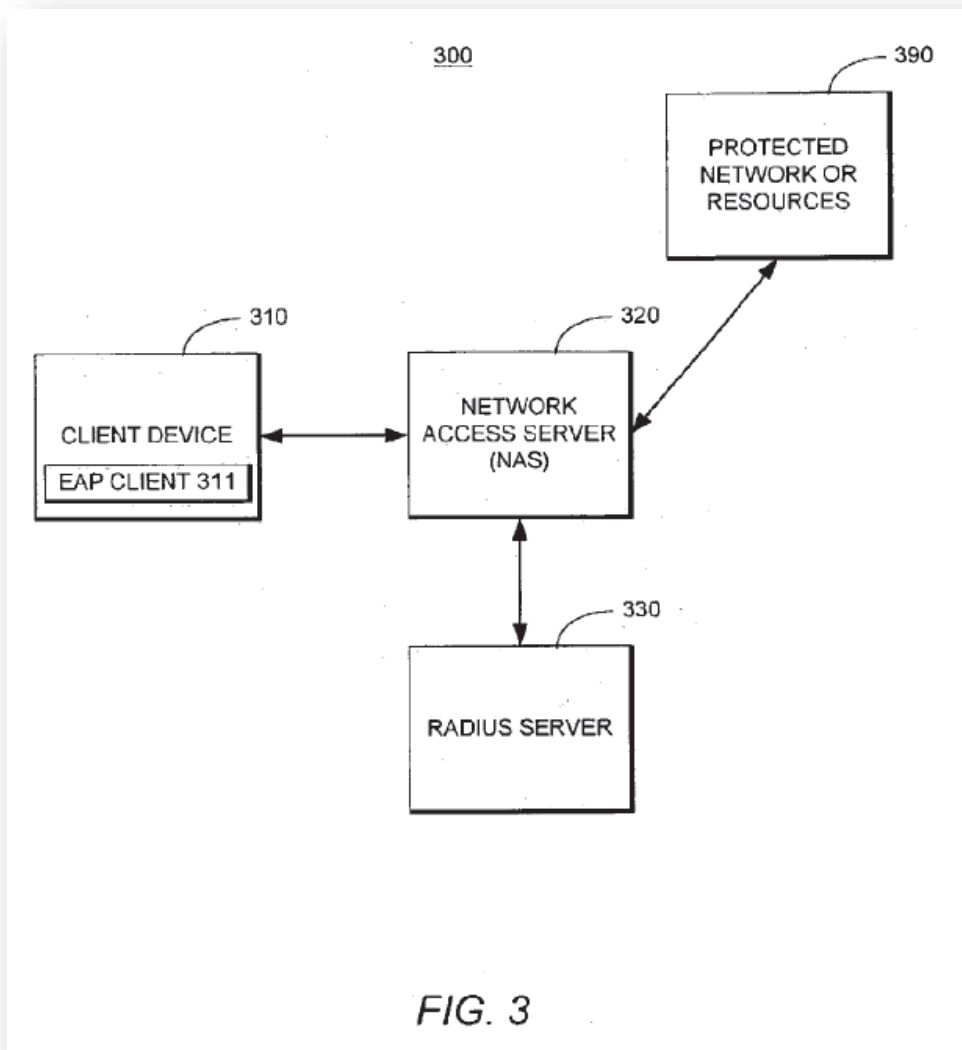
Krantz teaches a client requesting access to the network can send credentials to a server to authenticate the client and user. Ex.1005, [0016]. Based upon the credentials, the server “may authorize the client for at least partial access” or access to the entire network. Ex.1005, [0016], [0104], [0107]-[0109]. Authentication may be made by server 215. Ex.1005, [0068]-[0071], [0099]. The server is also responsible for ensuring that the client device adheres to certain configuration settings—including the established encryption protocol—for gaining access to the network authorized to be accessed. Ex.1005 [0110]-[0111].

B. Summary of Herrmann

U.S. Patent Pub. No. 2004/0107360 to Herrmann et al. was filed on March 13, 2003, and published on June 3, 2004. Herrmann is prior to the 460 Patent at least under 35 U.S.C. § 102(e).

Herrmann describes enforcing security policies when providing access to a network. Herrmann explains that if a client device connected to a network [] is infected with a virus or worm, it may infect other machines on the same network. Ensuring that devices connected to the network are running current anti-Virus programs is particularly important. Ex.1006 [0012].

As a solution, Herrmann proposes the collection of information from a client device to be used during the authentication process to enforce network security policies. For example, Herrmann teaches a system in which a client device attempts to access a network and information is collected to determine whether the client can gain access to protected network resources. Ex.1006, [Abstract], [0063]. The basic architecture of the system includes a client access device, network access server, and protected network and/or resources shown below in Figure 3 of Herrmann. Ex.1005, [0018], [0053], [0063].

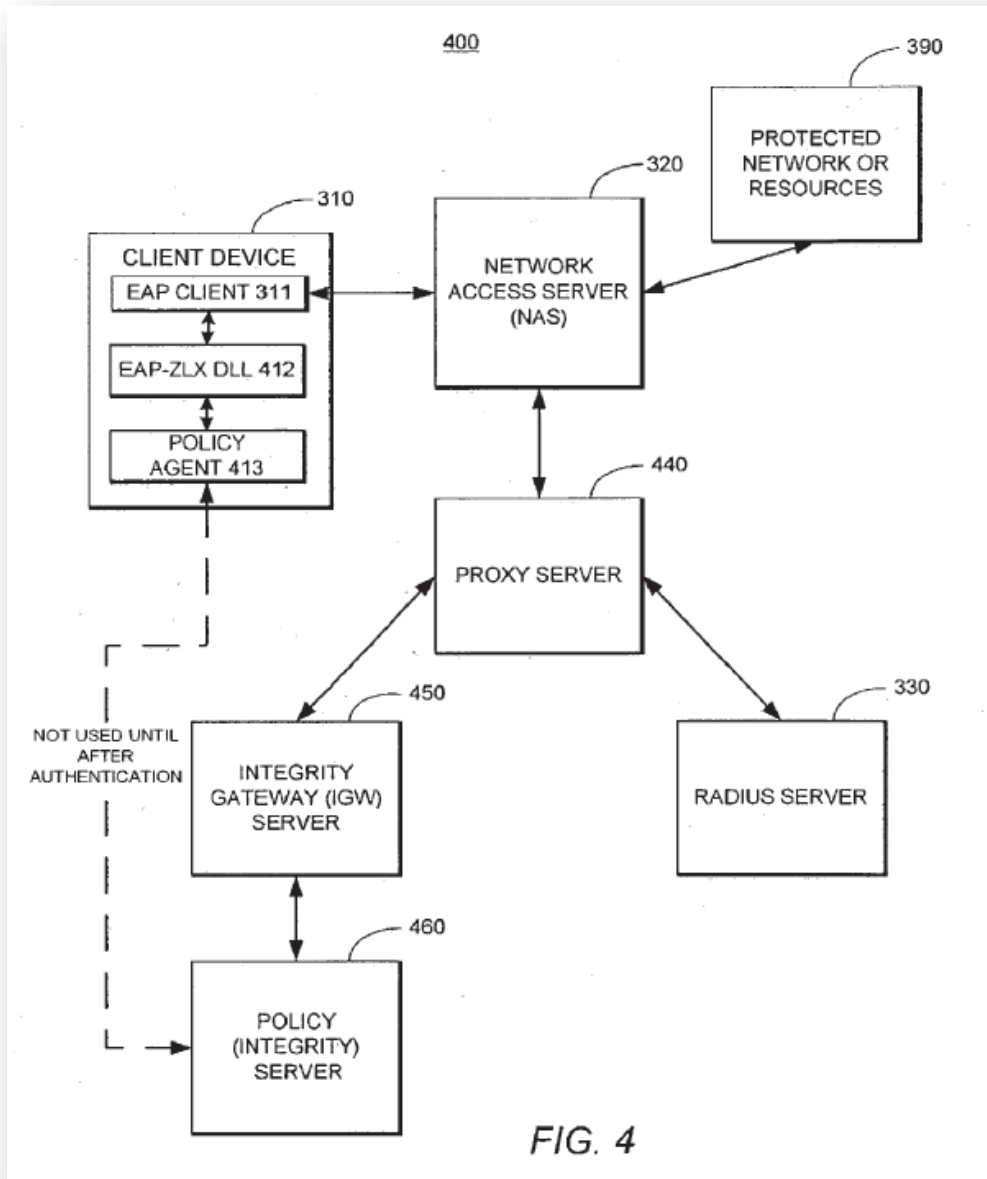


Ex.1006, Fig. 3.

In Figure 4, “a client device 310 connects to the NAS 320 to access the protected network or resources 390.” Ex.1005, [0062]-[0063]. However, the system, includes an additional “policy (integrity) server 460” ... which “ensures that all users accessing a particular system or network comply with specified security policies, including access rights and cooperative anti-virus enforcement”

and can deny network access for access devices that are not in compliance.

Ex.1005, [0062], [0067].



Ex.1006, Fig. 4.

Figure 4 of Herrmann depicts a “policy agent (or integrity agent) 413 to retrieve information about the current security policy in operation on the client

device 310. Ex.1005, [0064]. This allows “the policy server 460 [to] evaluate[] whether or not the client device 310 has a correct, up-to-date version of the applicable security policy.” Ex.1005, [0067].

VIII. CLAIMS 1-6, 10-14, 16-22, 27, and 29-30 ARE UNPATENTABLE

A. Ground 1: Claims 1-2, 10-14, 16-17, 27, and 29-30 are Obvious Based on Krantz

1. Claim 1

i. *[1.0] A method of granting access to a protected network, the method comprising:*

The “*protected network*” of the 460 Patent can include a single or multiple networks. Ex. 1001, 2:52-3:8 (noting that the network can be logical in nature and can consist of multiple VLANs). The 460 Patent explains that “Protected Network 200 includes a corporate network, telephone network, private network, local area network, wide area network, wireless network, communication network, government network, university network, and/or the like.” Ex.1001, 6:5-9. Ex.1003, ¶66.

The network disclosed in Krantz is a “*protected network*”—VLAN B and VLAN C of Krantz (*e.g.*, as depicted in Figure 2) consistent with the “*protected network*” of the 460 Patent. Krantz explains that the disclosed networks “can be implemented using any number of techniques, such as, for example, **Virtual Local Area Networks (“VLANs”), Internet Protocol (“IP”) filtering, Virtual Private**

Networks (“VPNs), or use of IPSecurity (“IPSec) protocols.” Ex.1005, [0017]¹.

Each of these techniques are methods of creating a “*protected network*” because they facilitate the access control capabilities described in Krantz. Ex.1005, [0017]. Ex.1003, ¶67.

Krantz discloses network access protocols whereby “[a] server includes the **functionality to authorize clients to access a second network**” Ex.1005, [0016]. For example, Krantz explains that “[a] client sends credentials to the server to attempt to authenticate with the server. Based on the credentials, the **server may authorize the client for at least partial access to the second network** and/or may deny access to the second network and **authorize the client for at least partial to access to the first network.**” Ex.1005, [0016]. Ex.1003, ¶68.

Based on Krantz, Dr. Houh explains that a POSITA would understand that combining the first and second networks into a logical “*network*” would be done physically or logically. Ex.1005, [0038]. Krantz focuses on logical representations:

[A] “logical communication link” is defined as any communication path that can enable the transport of electronic data between two entities such as computer

¹ Emphasis added in bold throughout unless otherwise stated.

systems **The actual physical representation of a communication path between two entities is not important and can change over time. A logical communication link can include portions of . . . a local area network (e.g., an Ethernet network), a wide area network, the Internet, combinations thereof, or portions of any other path that may facilitate the transport of electronic data. . . .**

Ex.1005, [0038]. Ex.1003, ¶69.

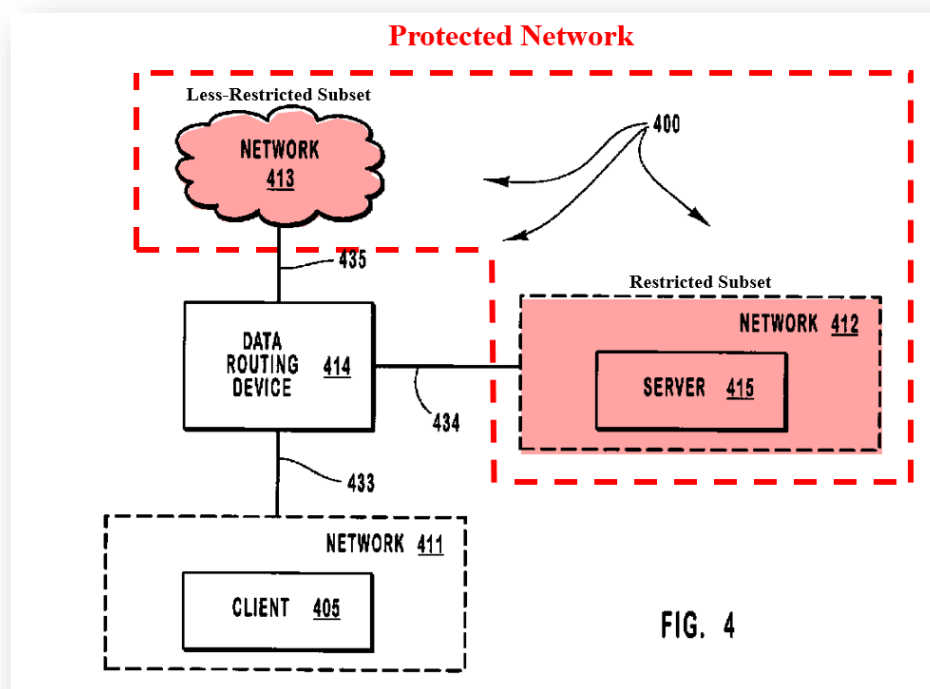
Moreover, as Dr. Houh explains, combining two (or more) physical networks together was a common technique in networking at the time. Ex.1011, 223 (defining “logical network” as “[a] network as it appears to the user. In fact, the network could be composed of two or more physical networks, or portions of these, that are linked and coordinated in a such a way that they appear to be a unit.”); Ex.1012, 317 (explaining the “difference between a network as logical or physical is sometimes subtle because the physical network (the actual layout of hardware and cabling) doesn’t necessarily resemble the logical network (the path followed by transmissions.”). Krantz itself explains that “[l]ogical communication links **can include hardwired links, wireless links, or a combination**” thereof.

Ex.1005, [0038]. Ex.1003, ¶70.

Similarly, the 460 Patent explains that a “*protected network*” may be “**physically or logically divided** into a restricted subset and one or more less-

restricted subsets.” Ex.1001, 2:52-54. The 460 Patent also explains that such restricted and less-restricted subsets “are typically characterized by Virtual Local Area Networks (e.g., VLANs),” (Ex.1001, 2:66-3:4), and further explains that the “*protected network*” may include “access restrictions.” Ex.1001, 6:21-33. Ex.1003, ¶71.

The “*protected network*” described in Krantz is depicted in annotated Figures 4 and 2:



Ex.1005, Figure 4 (annotated).

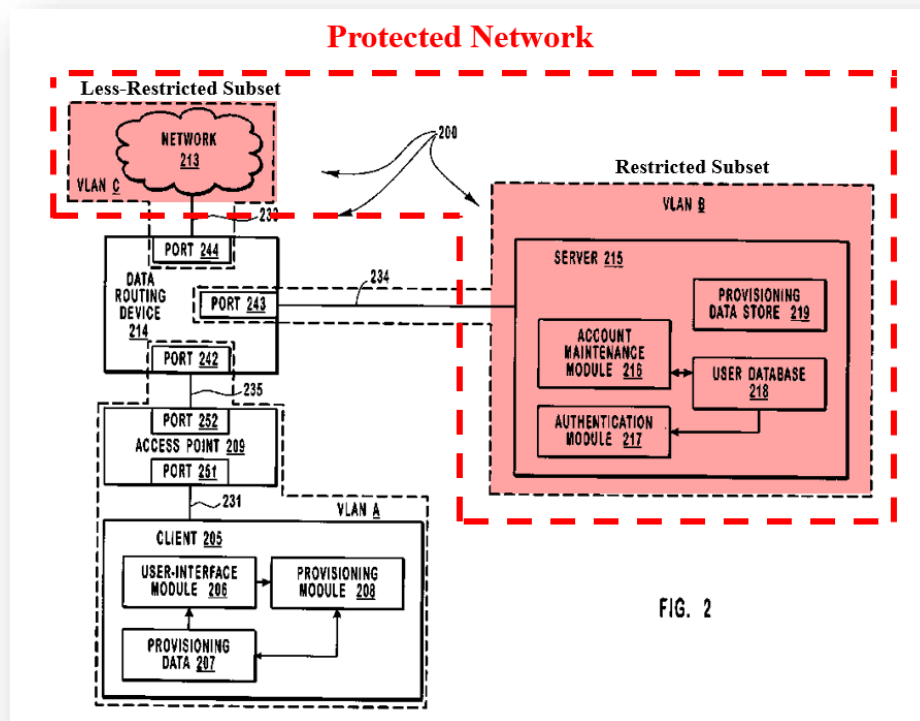


FIG. 2

Ex.1005, Figure 2 (annotated). Ex.1003, ¶72.

Krantz describes Figure 4 as “illustrat[ing] generally an example of a network architecture 400 that can provide access to a first network while restricting access to a second network.” Ex.1005, [0050]. Krantz further explains that “in some embodiments, access to resources located on network 413 can be restricted by the use of Virtual Local Networks (‘VLANs’).” Ex.1005, [0052]. Ex.1003, ¶73.

Figure 2 depicts an embodiment implementing the architecture of Figure 4 and “using VLAN techniques,” which “facilitate increasing the level of automation when provisioning a client.” Ex.1005, [0057]. Figure 2 and its description thus

provide specific techniques to be implemented in Krantz's networking architecture.

See generally Ex.1005, Figures 2 and 4 and related descriptions, [0050]-[0062].

Accordingly, the combination of Network 413 and Network 412 (annotated as VLAN C and VLAN B) constitute a “*protected network*.” Ex.1003, ¶73.

To the extent Patent Owner asserts that the “*protected network*” is required to be a single network, Krantz explains that its “*access*” control techniques can also be used “**within a single network**.” Ex.1005, [0017], [0055]. Ex.1003, ¶74.

As Krantz explains, the disclosed system “**may authorize the client for at least partial access to the single network**” (“*a method of granting access*”), and as explained below, one example of “*granting*” such “*access*” in Krantz is “by authorizing client access to selected computer systems or modules on the single network.” Ex.1005, [0017]; *see also* Ex.1005, [0016], [0071] [0074]-[0076], [0099], e.g., at [0068] (““[a]fter an EAP type is selected . . . **computer systems can attempt to authenticate with one another** through the transfer of EAP messages . . . in accordance with the selected EAP type. For example, when EAP-TLS is selected, **client 205 may communicate with server 215** through a series of EAP messages in accordance with EAP-TLS **so as to be authenticated and possibly authorized to access resources located on VLAN C.**”); [0104], [0107]-[0109]. Ex.1003, ¶75.

Accordingly, Krantz teaches or suggests this claim element. Ex.1003, ¶76.

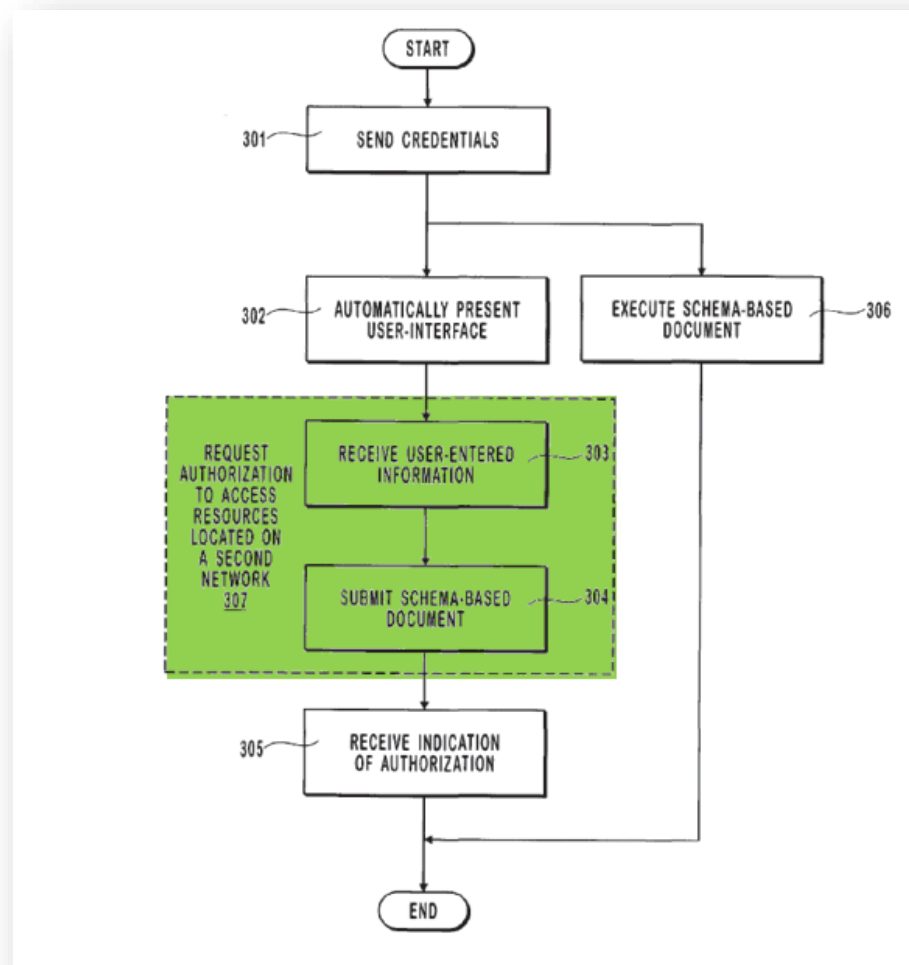
ii. *[1.1] receiving a request for access to a less-restricted subset of the protected network from an access device,*

Krantz discloses that “a server includes the functionality to authorize [] access” to a network and/or selected elements within a network after the client 205 (“access device”) sends credentials to the server (“receiving a request”). *E.g.*, Ex.1005, [0016], [0071]. Krantz discloses that the “server (**based at least in part on received credentials**) may authorize the client for at least partial access to the single network.” Ex.1005, [0017]; *see also* [0068]-[0076], [0099], [0104], [0107]-[0109] (collectively describing techniques for requesting access in a VLAN environment). Ex.1003, ¶78.

Such credentials “can include sending an Extensible Authentication Protocol (“EAP”) Response/Identity message from the client to the server. If the client is attempting to connect to a network via an access point, the EAP Response/Identity message may be encapsulated within some other type of message that can be transferred through the access point.” Ex.1005, [0018]. Other credentials provided by Krantz’s “access device” may include, for example, “user-identifier[s] and password[s].” Ex.1005, [0071], [0074], [0076]. Ex.1003, ¶79.

Krantz also explains that Figure 3 “is a flow diagram illustrating a method 300 for provisioning a computer system,” and that the disclosed “method 300 [is] described with respect to components depicted in network architecture 200.”

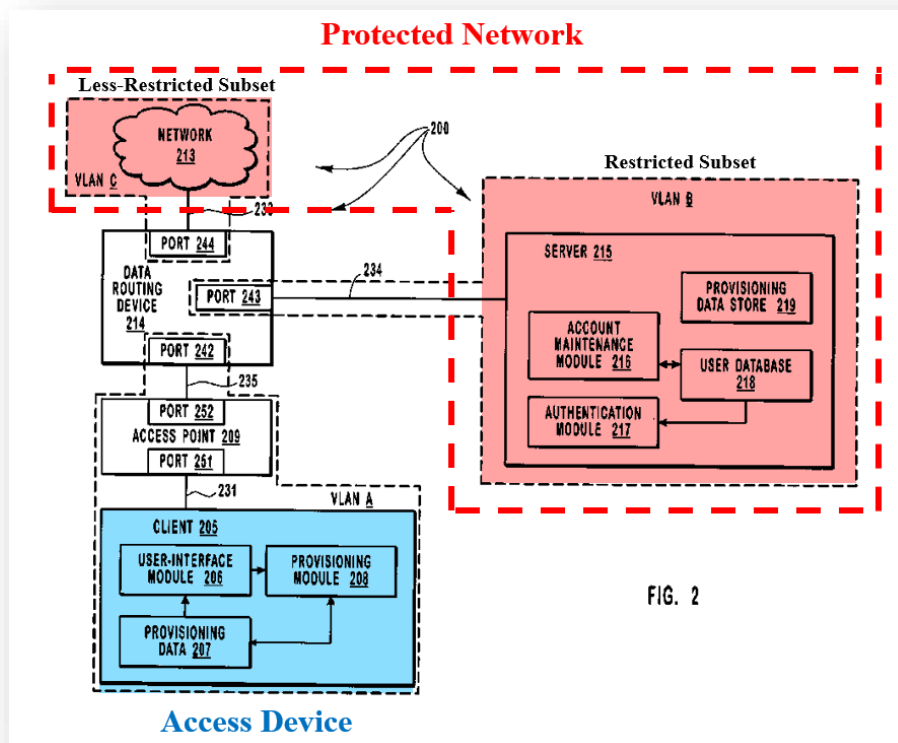
Ex.1005, [0070]. Krantz discloses that “the method 300 includes a functional, result-oriented step for **requesting authorization** (“*receiving a request*”) to **access resources located on a second network (step 307)**” (“*to a less-restricted subset of the protected network*”). Ex.1005, [0104]; [0071]. Krantz further explains that “[s]tep 307 may include any corresponding acts for accomplishing the result of requesting authorization to access resources located on the second network.” Ex.1005, [0104]. Ex.1003, ¶80.



Ex.1005, Figure 3 (annotated). Ex.1003, ¶80.

As depicted in Figure 3, Krantz explains that the “method 300 includes act of [client 205] sending credentials to a server to attempt to authenticate with the server,” (Ex.1005, [0071]), and step 307 “includes [the] corresponding act of receiving user-entered information (act 303)” and may include executing a “schema-based document” according to configuration settings. Ex.1005, [0104], [0110]. Ex.1003, ¶81.

The “*access device*”—“Client 205”—making the “*request*” in Krantz is depicted in annotated Figure 2 in blue:



Ex.1005, Figure 2 (annotated). Ex.1003, ¶82.

Moreover, as described above, *see* § VIII.A.1.i, the combination of second network VLAN C and first network VLAN B constitute a “*protected network*.” Krantz discloses that “[b]ased on [client] credentials, the server **may authorize the client for at least partial access to the second network [VLAN C] and/or may deny access to the second network** and authorize the client for at least partial to access to the first network” (“*a request for access to a less-restricted subset of a protected network*.”). Ex.1005, [0016]; Ex.1005, [0017] (explaining that “the server (based at least in part on received credentials) may authorize the client for at least partial access to the single network, such as, for example, by authorizing client access to selected computer systems or modules on the single network.”). Similarly, Krantz explains that its access methods “include[] a functional, result-oriented step **for requesting authorization to access resources located on a second network**.” Ex.1005, [0104]. Ex.1003, ¶83.

In Krantz, the “second network”—VLAN C—is a “*less-restricted subset of a protected network*” because it provides “full access to [its] resources” to authorized users (Ex.1005, [0019]), like the “*less-restricted subset of a protected network*” of the 460 Patent. The 460 Patent explains that “[t]he less-restricted subset [is] **less restricted** relative to the restricted subset **in terms of what elements may be included in each subset**.” Ex.1001, 5:43-45. The “*less-*

restricted subset of a protected network” provides greater access to elements and/or resources than the “*restricted subset*².” Ex.1003, ¶84.

Accordingly, Krantz teaches or suggests this claim element. Ex.1003, ¶85.

iii. [1.2] the request received through a communication port of an access point,

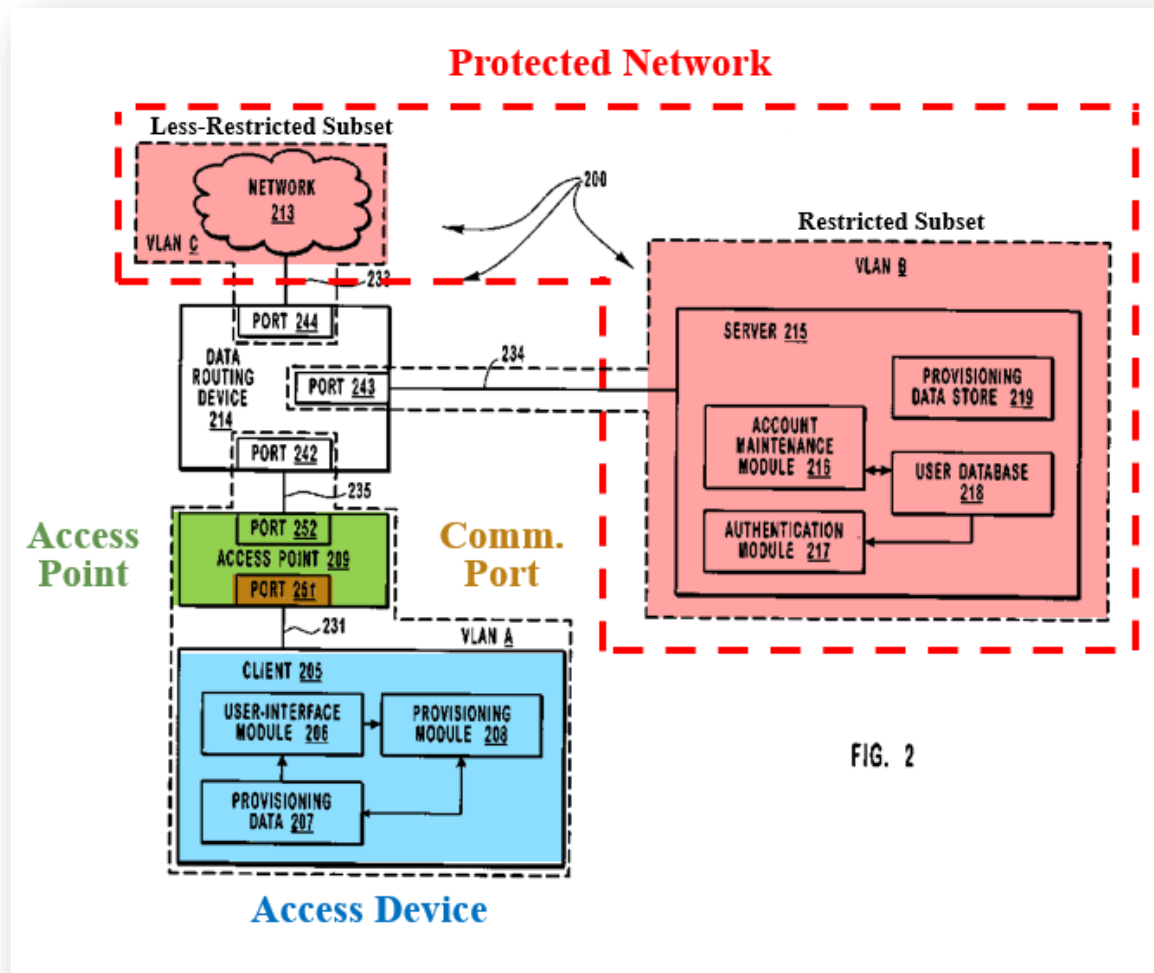
As explained above, *see* §VIII.A.1.ii, Krantz discloses “a request for access to a less-restricted subset of a protected network” because Client 205 requests authorization to access resources on the second network and “*less-restricted subset*”—VLAN C. Ex.1003, ¶87.

The 460 Patent explains that “Access Point 215” can be “a network switch [or] wireless access point,” and “[w]hen embodied in a network switch, [it] includes a series of communication ports . . . configured for communication with . . . Less-Restricted Subset 210 and/or Restricted Subset 205.” 460 Patent, 7:57-65. Ex.1003, ¶88.

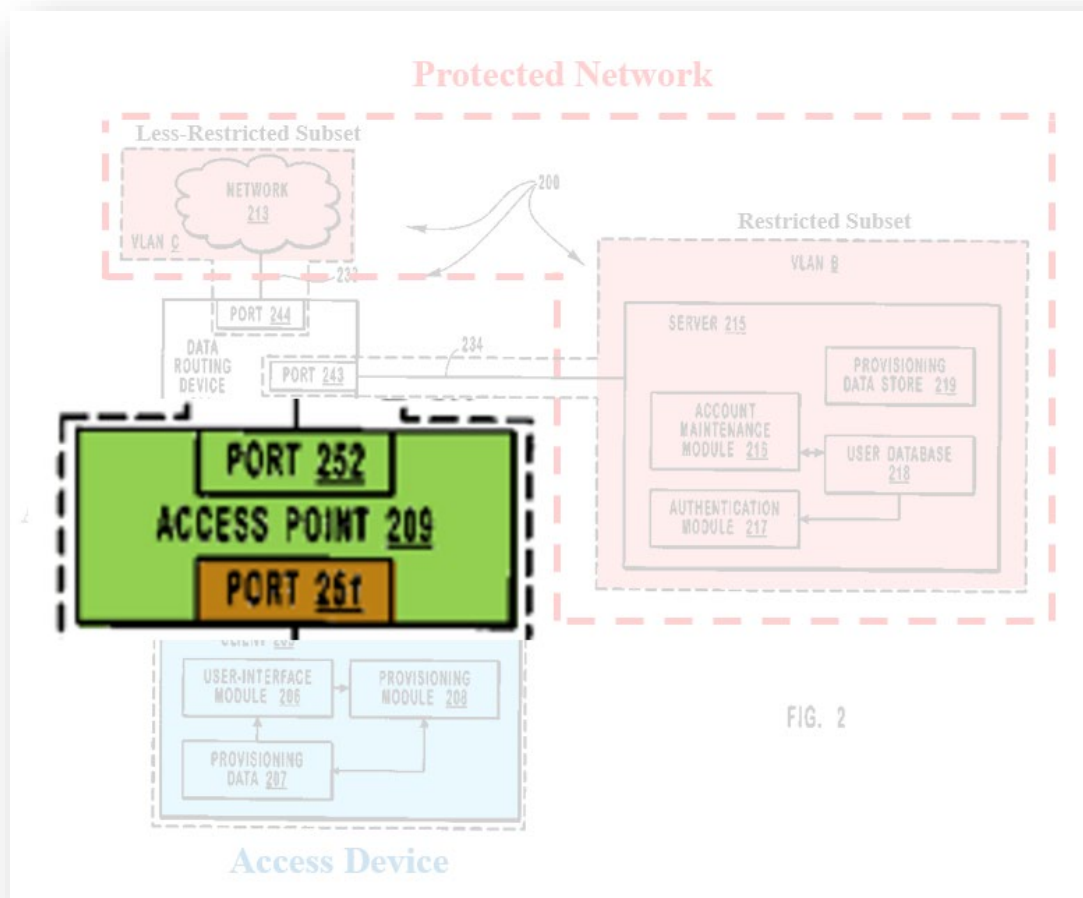
As in the 460 Patent, Krantz’s request is received through a “*communication port*”—annotated in brown as “Port 251”—of an “*access point*”—annotated in

² As described below, the “*restricted subset*” of Krantz’s “*protected network*” is the first network, *i.e.*, VLAN B.

green as “Access Point 209”:

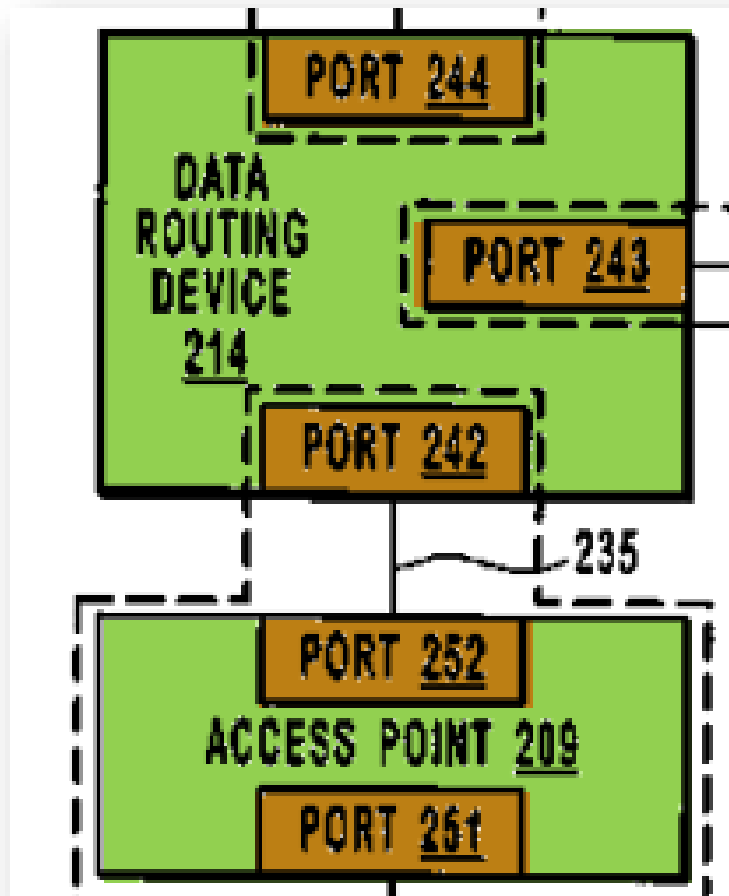


Ex.1005, Figure 2 (annotated). Ex.1003, ¶89.



Ex.1005, Figure 2 (annotated). Ex.1003, ¶89.

Alternately, the claimed “*access point*” can be Routing Device 214 in combination with Access Point 209, as discussed in detail below with respect to limitation [1.3] (**Mapping #3**), in which the claimed “*communication port*” is port 251 in combination with ports 252 and port(s) 242, 243, and/or 244. Ex.1003, ¶90.



Ex.1005, Figure 2 (annotated). Ex.1003, ¶90.

Accordingly, Krantz teaches or suggests this claim element. Ex.1003, ¶91.

- iv. *[1.3] the communication port configured for communicating between the access device and a restricted subset of the protected network,*

The 460 Patent explains that “[a] communication port of the access point is configured such that network traffic directed at the protected network is initially passed through a restricted VLAN rather than through a less-restricted VLAN.”

Ex.1001, 3:8-11. Ex.1003, ¶93.

Krantz discloses the claimed functionality in several alternative ways.

Ex.1003, ¶94.

Mapping #1

First, Krantz explains that “[a]ccess point 209 can be a wired or wireless access point **that facilitates communication between client 205 and data routing device 214**. As depicted in network architecture 200, access point 209 is connected to client 205 by corresponding logical communication link 231. ... Access point 209 includes ports 251 and 252. **Data can be transferred between access port [sic]³ 209 and client 205 through port 251. Likewise, data can be transferred between access point 209 and data routing device 214 through port 252.**” Ex.1005, [0063]. Ex.1003, ¶95.

Krantz discloses that “access point 209 [(“*access point*”)] is a wireless access point that enables access to wired computer systems on VLAN B (e.g., server 215) and VLAN C (e.g., computer systems included in network 213).” Ex.1005, [0064]. Thus, “port 251” (“*the communication port*”) is “*configured for communicating between the access device and restricted subset of the protected network*” because it facilitates the transfer of data between client 205 (“*the access*

³ Typo in original. “Access port 209” should refer to “Access **Point** 209.”

device”) and ultimately VLAN B (the “*restricted subset of the protected network.*”) Ex.1005, [0063]-[0064]. Ex.1003, ¶96.

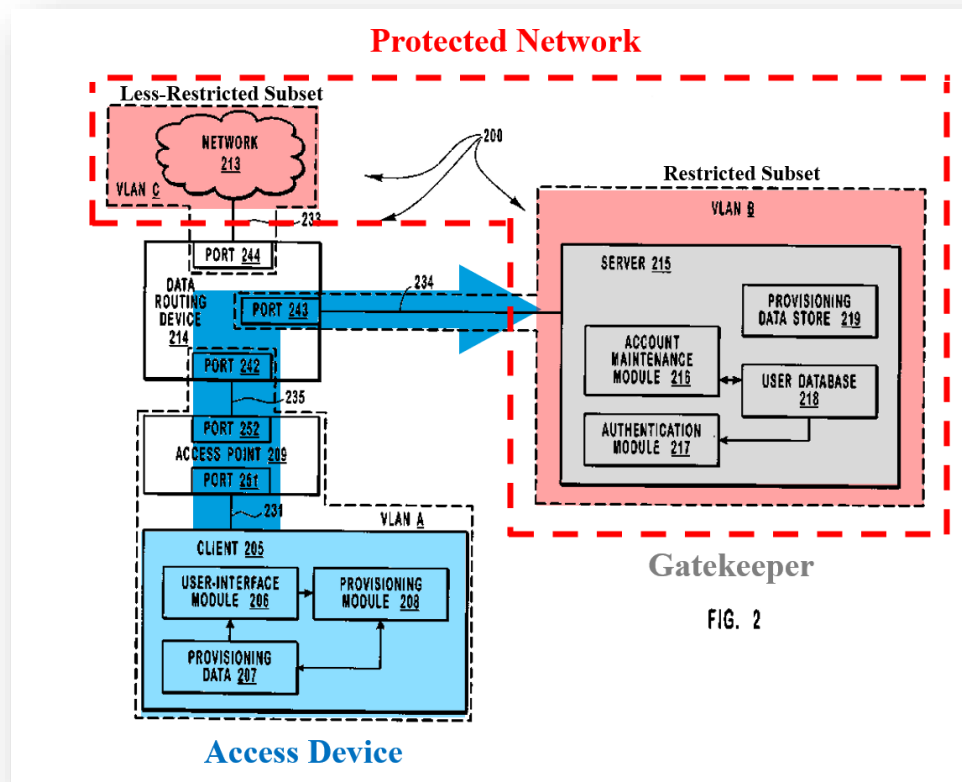
Mapping #2

Second, Krantz explains that “Access point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C. Ex.1005, [0064]. Krantz is therefore explaining that when configured as a “VLAN aware device,” Krantz’s Port 251 (the “*communication port*”) “*is configured for communicating between the access device and a restricted subset of the protected network*” because Access Point 209 configures Port 251 to insert VLAN Tag Headers into incoming data frames from a client that may only access VLAN B—the “*restricted subset.*” Ex.1005, [0064]; Ex.1005, [0072] (“Access point 209 can insert a Tag Header into a [data] packet . . . indicating that the [data] packet is to be transferred to VLAN B.”); [0107] (explaining VLAN tagging generally). Ex.1003, ¶97.

As Dr. Houh confirms, configuring input ports in VLAN aware devices to tag incoming data was a well-known technique to POSITAs by 2003. Ex.1007, 11 at Table 5-1 (explaining, that when the “Reception Port receives as (and does not discard)” untagged data, it “shall support the insertion of tag headers of a format appropriate to the destination MAC, carrying a non-null VID.”); *see also* Ex.1008,

4:42-47 (“[S]ource node A transmits the packet. No VLAN tag information is present in a packet transmitted from a source node. At 415, **the packet is received at switch 305, port 2. Port 2 is configured as a member of LAN 1. Thus, a VLAN tag header is inserted in the packet** with a VID=1.”); *see also* Ex.1009, 16:4-13 (“[E]very time a message **is received by the switch on a local port the VLAN designation of that port is associated with the message.** Association is accomplished by a flow processing element which looks up the VLAN designation in a memory based on the local port where the message originated.”); *see also* Ex.1010, p. 210 (“The **switch that receives the frame from the source station inserts the VLAN ID** and the packet is switched onto the shared backbone network. When the frame exits the switched LAN, a switch strips the header and forwards the frame to interfaces that match the VLAN color.”). Ex.1003, ¶97.

The communication path “*between the access device and a restricted subset of the protected network*” is depicted in Figure 2 and annotated in blue:



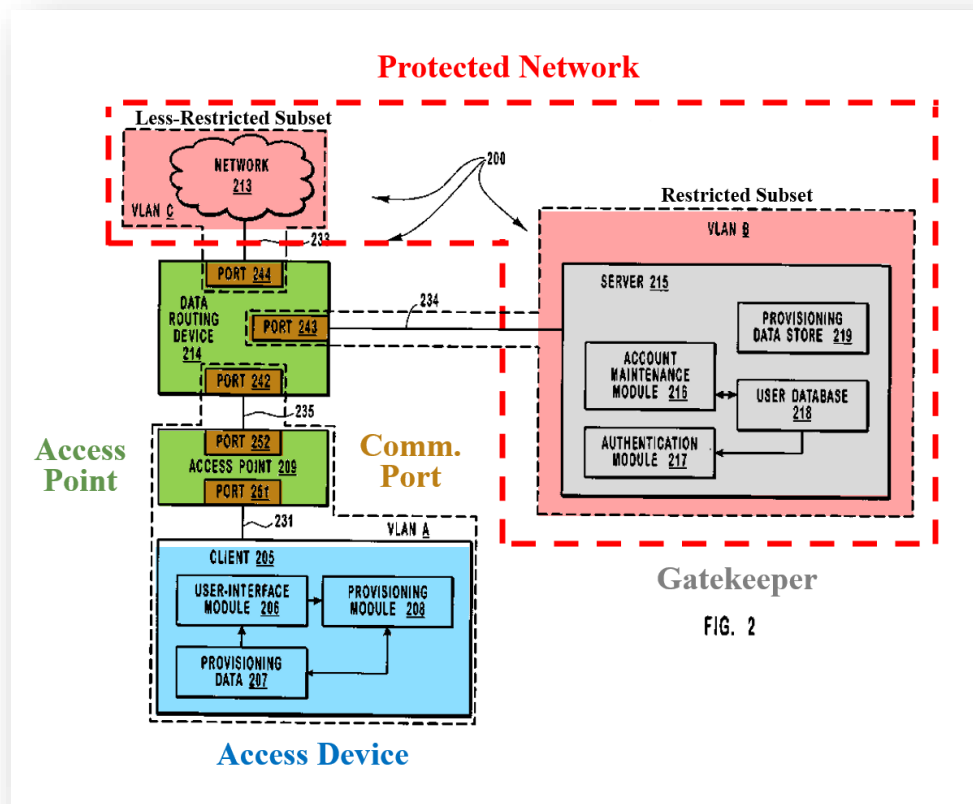
Ex.1005, Figure 2 (annotated). Ex.1003, ¶98.

Accordingly, Krantz teaches or suggests this claim element. Ex.1003, ¶99.

Mapping #3

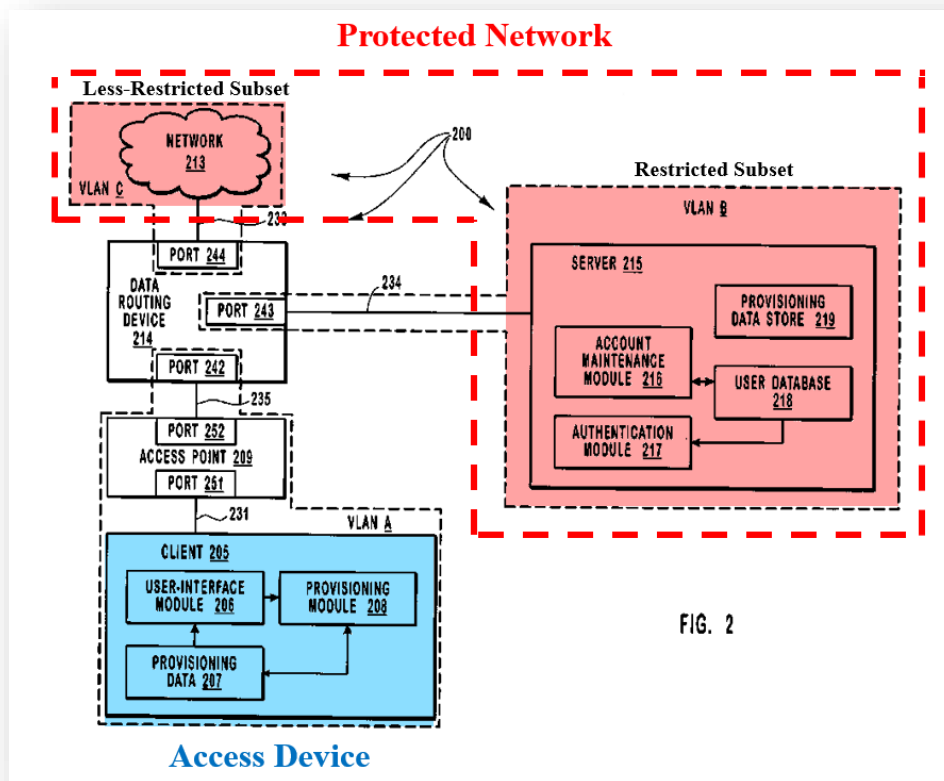
To the extent one may assert that Krantz does not expressly disclose the claimed “communication port configured for communicating between the access device and a restricted subset of the protected network,” it would have been obvious to implement other “configur[ation]” techniques in view of Krantz itself. Ex.1003, ¶100.

For example, Access Point 209 is connected to Data Routing Device 214, both of which include several communication ports (as shown below). In particular, 235 is a logical communication link connecting the two. Ex.1005, [0060]. The claimed “communication port configured for communicating between the access device and a restricted subset of the protected network” in this scenario, shown below, would port 251 in combination with ports 252, 242, and 243 (port 244 connects to the less-restricted subset2). Ex.1003, ¶101.



Ex.1005, Figure 2 (annotated). Ex.1003, ¶101.

Krantz discloses that “data routing device 214 can be configured to separate computer systems into different VLANs. As depicted in FIG. 2, data routing device 214 has been configured to separate network architecture 200 into **VLANs A, B [Restricted Subset], and C [Less-Restricted Subset]**. Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.” Ex.1005, [0060]. VLAN’s B and C are depicted below for reference.



Ex.1005, Figure 2 (annotated). Ex.1003, ¶102.

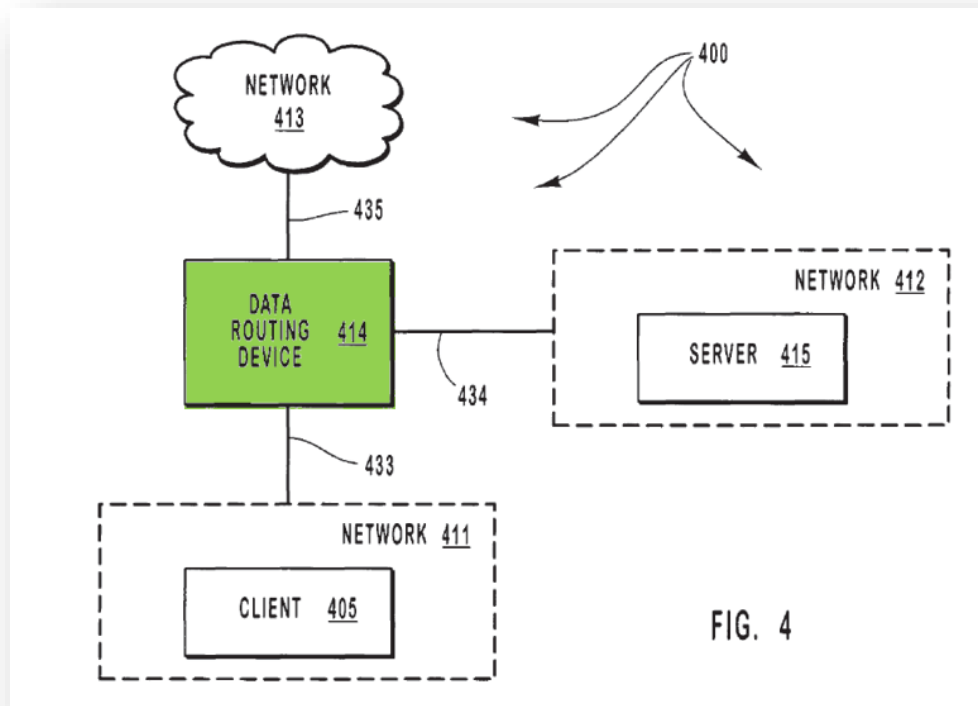
Krantz states that “[n]etwork architecture 200 also includes data routing device 214. **Data routing device 214** logically represents a special-purpose

computer system, such as, for example, **a router and/or a switch, that can determine how to transfer data between the ports included in data routing device 214**. That is, when a portion of data, such as, for example, a data frame, is transferred in at a first port (e.g., port 242) **data routing device 214 can determine, based on configuration rules, that the frame is to be transferred out at a second port** (e.g., port 243). For example, data routing device 214 can determine that a data frame received from access point 209 is to be sent to server 215. It may also be that a data frame is transferred in and out of data routing device 214 at the same port.” Ex.1005, [0059]-[0060]; *see generally*, Ex.1005, [0064]. Ex.1003, ¶103.

Dr. Houh explains that a POSITA would have found it obvious that the technique discussed with respect to the “data routing device 214” could simply be implemented **at the access point itself** as the data routing device is merely a “logical representation” of, e.g., a router and/or switch. Ex.1005, [0059]. He also states that in such a scheme, the Access Point 209 would implement that port configuration and data transfer techniques described with respect to “data routing device 214.” Ex.1003, ¶104.

Moreover, Krantz already contemplates combining the functionality of the “access point” and “data routing device” in a single physical or logical

representation. Figure 4 of Krantz demonstrates that such functionality can be readily combined with the data routing device as the access point, Ex.1003, ¶105:



Krantz explains that:

Data routing device 414 logically represents a computer system ... **when data routing device 414 receives data from network 411, data routing device 414 can determine if the data is to be transferred to network 412 or network 413.** As such, data routing device 414 can be configured to allow access to one network (e.g., network 412) while at the same time restricting access to another network (e.g., network 413).

Ex.1005, [0051]. Ex.1003, ¶106.

With respect to the disclosures in Figure 2, Krantz expressly discloses that “Data routing device 214 **logically represents** a special-purpose computer system, such as, for example, a router and/or a switch, that can determine how to transfer data between the ports included in data routing device 214,” Ex.1005, [0059], so a “logical” architecture could readily be implemented in a single device such as an access point as Dr. Houh demonstrates. Ex.1003, ¶107.

Moreover, Krantz explains that such a logical implementation would include functionality that enables a “data frame” to be “transferred in and out of data routing device 214 **at the same port.**” Ex.1005, [0059]. In fact, Krantz repeatedly describes the “data routing” device and “access point” device as having the same functionality. *Compare, e.g.*, Ex.1005, [0060] (“Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.); [0064] (“Access point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C.”); *see also* [0069], [0073] (describing the same functionality for both the data routing device and access point). Therefore, the functionality described in Krantz can occur at the access point and data routing device combined **or** the access point alone, without having any impact on the

overall functionality of the system. Using one technique or the other would merely have been a matter of design choice and any POSITA would have a reasonable expectation of success. Ex.1003, ¶107.

Thus, it would have been obvious to combine the functionality of the Data Routing Device and Access Point of Krantz in the same device for the reasons described above. Ex.1003, ¶108.

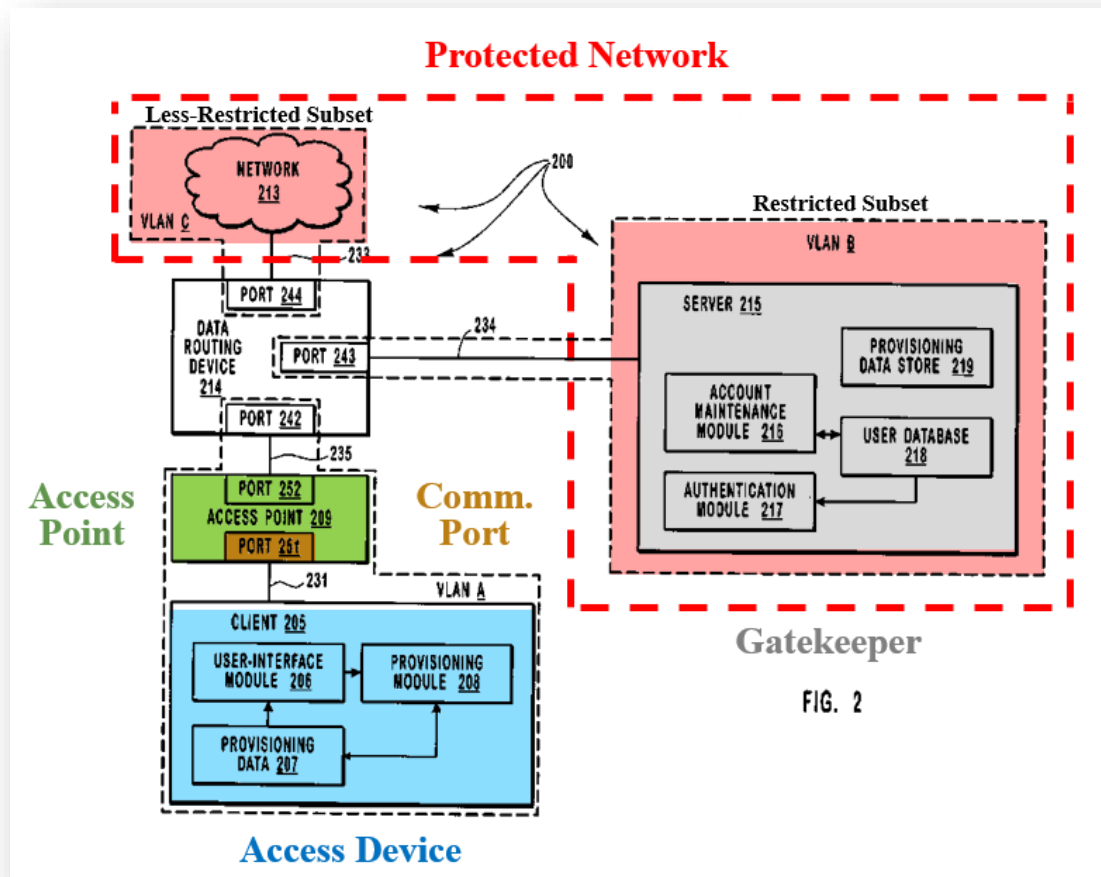
Accordingly, Krantz teaches or suggests this claim element for this additional reason as well. Ex.1003, ¶109.

- v. ***[1.4] the restricted subset including a gatekeeper; applying a security policy to the access device in response to the request; using the gatekeeper to determine if requirements of the security policy are satisfied by the access device, and***

As discussed with respect to limitations [1.1] and [1.2], the client makes a “request.” See §VIII.A.1.ii-iii. Ex.1003, ¶111.

Krantz discloses that “[a] client attempts to become authorized to access resources located on a second network ... [and] sends credentials to an access point that is communicatively coupled to a server (located on a first network or located on the second network) that can authorize access to the second network.” Ex.1005, [0031]; *see also* Ex.1005, [0071]. This can generally be observed with respect to

Figure 2. Ex.1003, ¶112. As seen below, “the restricted subset includ[es] a gatekeeper⁴” (server 215).



Ex.1005, Figure 2 (annotated). Ex.1003, ¶112.

Furthermore, with respect to the Gatekeeper (depicted above), Krantz discloses “applying a security policy.” As an initial matter, the 460 Patent explains

⁴ Applicant admits that a “Gatekeeper” was “practiced in the prior art.” Ex.1001, 2:30-32.

that “the security policies may include requirements for user identification⁵ such as usernames and passwords, configuration requirements relating to the configuration of Access Device 230 application requirements relating to applications running on Access Device 230, or the like.” Ex.1001, 6:40-45. Ex.1003, ¶113.

Krantz discloses several specific examples of “*applying a security policy to the access device in response to the request.*” For instance, Krantz explains that access to the network may be controlled by “configuration settings,” which can include “supported types of encryption” or “supported types of authentication,” which can include an indication for EAP, which is short for “Extensible Authentication Protocol.” Ex.1005, [0066]-[0067]. Ex.1003, ¶114.

Krantz further explains that “[a]fter an EAP type is selected . . . **computer systems can attempt to authenticate with one another** through the transfer of EAP messages . . . in accordance with the selected EAP type. For example, when EAP-TLS is selected, **client 205 may communicate with server 215** through a series of EAP messages in accordance with EAP-TLS **so as to be authenticated and possibly authorized to access resources located on VLAN C.**” Ex.1005, [0068]. The use of EAP-TLS (*e.g.*, Ex.1005, [0067]-[0074], [0100]) was a known

⁵ Krantz’s disclosure of “User Identification” as part of “*applying a security policy* . . . ” is described in detail in claim 2 below.

authentication protocol that would be used to authenticate client devices. Ex.1016 [RFC2716] at 1; *see also*, Ex.1016 [RFC2716] at 2 (“The Extensible Authentication Protocol (EAP) ... provides a standard mechanism for support of additional authentication methods within PPP ... [and] support for a number of authentication schemes may be added, **including smart cards, Kerberos, Public Key, One Time Passwords, and others. To date however, EAP methods such as [6] [Security Considerations] have focussed [sic] on authenticating a client to a server.**”) Ex.1003, ¶114

Krantz similarly discloses that “[w]hen EAP-MSChap V2 is indicated, the “MS Chap V2 Parameters element at line 67 can be included in a configuration sub-file to indicate whether **or not operating system credentials should be used for authentication.**” Ex.1005, [0099]. Ex.1003, ¶115.

Krantz also explains that both EAP-TLS and EAP-MSCHAP V2 can both be required from a client seeking access and authorization. Ex.1005, [0099] (“[B]oth of the elements . . . can be included in a configuration sub-file to indicate different EAP types, such as, for example, EAP-TLS and EAP Microsoft/Challenge/Replay Handshake Protocol Version (“EAP-MSChapV2”). Accordingly, a POSITA would understand that each of the above techniques in Krantz would be used to authenticate the client 205 (“*applying a security policy to the access device in*

response to the request.”) before authorization is granted. E.g., Ex.1017, at 2. Ex.1003, ¶116.

Furthermore, Krantz discloses “*using the gatekeeper to determine if requirements of the security policy are satisfied by the access device.*” In particular each of the techniques described above would involve server 215 (“*gatekeeper*”) authenticating the client device in order to authorize it to access the protected network. Ex.1005, [0068]-[0074] (describing transferring client authentication information to authentication module 217); *see also* Ex.1005, [0067]-[0074], [0099]-[0100] (describing the use of EAP). Based on the credentials exchanged a “*determin[ation]*” is made if the client 205 (“*access device*”) has satisfied the requirements of a security policy—whether the “*access device*” is authenticated and therefore authorized “*for access to a less-restricted subset of the protected network.*” Ex.1005, [0068], [0071], [0099]. Ex.1003, ¶117.

Accordingly, Krantz teaches or suggests this claim element. Ex.1003, ¶118.

- vi. ***[1.5] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when the requirements of the security policy are satisfied.***

Krantz discloses that “access point 209 is a wireless access point that enables access to wired computer systems on VLAN B (e.g., server 215) and

VLAN C (e.g., computer systems included in network 213).” Ex.1005, [0064].

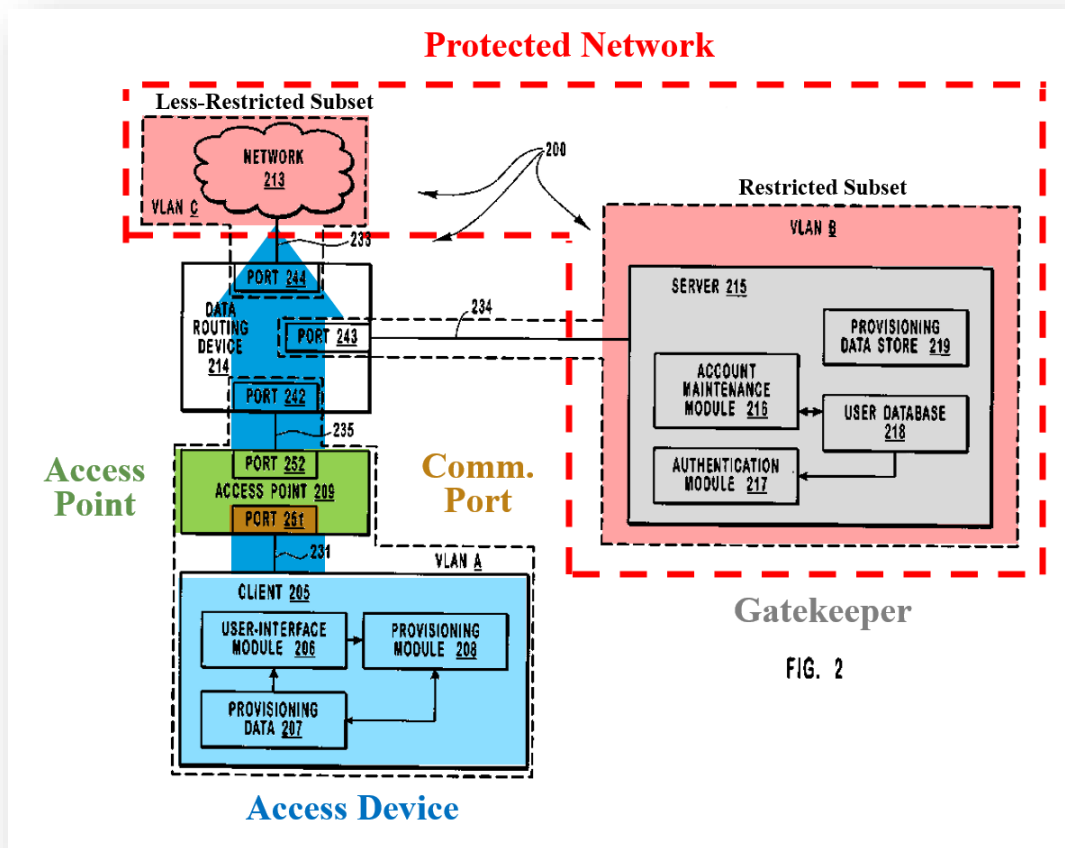
Ex.1003, ¶120.

Krantz explains that after the client is authenticated (“*the requirements of the security policy are satisfied,*”) *see* claim [1.4] *above*, “client 205 can then be authorized to access resources located on VLAN C.” Ex.1005, [0076]; *see also* Ex.1005, [0031]. Ex.1003, ¶121.

As explained above, Krantz teaches or suggests the claimed configuring (including reconfiguring) in several ways.

Mapping #1

First, “port 251” (“*the communication port*”)—after the “requirements of the security policy are satisfied”—facilitates the transfer of data between client 205 (“*the access device*”) and ultimately VLAN C (“*the less-restricted subset of the protected network without passing the data through the gatekeeper.*”) Ex.1005, [0063]-[0064]. Port 251 is “*reconfigured*” because it was previously configured to only transfer data to VLAN B for the reasons described above. *See* § VIII.A.1.iv. The path to VLAN C is depicted below—which would include transferring data “*without passing the data through the gatekeeper,*” server 215:



Ex.1005, Figure 2 (annotated). Ex.1003, ¶122.

Mapping #2

Second, Krantz explains that “[a]ccess point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C.” Ex.1005, [0064]; *see also* Ex.1005, [0061]-[0062].

As Krantz describes:

In VLAN embodiments, when a client is authorized to access resources located on the second network, **the access point may insert Tag Headers into client data to indicate to the data routing device that client data is to be transferred to the second network.**

Ex.1005, [0023]. Ex.1003, ¶123.

Dr. Houh explains that Krantz is describing that when configured as a “VLAN aware device,” Krantz’s “*access point*” is “*reconfiguring the communication port [Port 251 of Krantz] for communicating data between the access device and the less-restricted subset of the protected network*” because Access Point 209 (via Port 251) will insert VLAN Tag Headers into incoming data frames from a client **that may now access VLAN C**, i.e., the “*less-restricted subset*.” Ex.1005, [0107]; Ex.1003, ¶124. Port 251 is “*reconfigur[ed]*” by Access Point 209 because it was previously tagging incoming data from client 205, as described above, with headers that enabled access to VLAN B, i.e., the “*restricted subset*” only. Put another way, Access Point 209 “*reconfigure[s]*” Port 251 to tag incoming data for transfer to VLAN C rather than VLAN B. Ex.1003, ¶124.

Specifically, Krantz discloses “[w]hen client 205 is authorized to access resources located on VLAN C, access point 209 may enable any protocols that are currently blocked for port 251 and may insert Tag Headers indicating that data from client 205 is to be transferred to VLAN C [the “*less-restricted subset*”].

Server 215 can send commands to access point 209 to cause access point 209 to enable protocols and cause access point 209 to insert appropriate Tag Headers.”

Ex.1005, [0107]. Ex.1003, ¶125.

Moreover, as already demonstrated above, *see* § VIII.A.1.iv [claim 1.3], configuring input ports in VLAN aware devices to tag incoming data was a well-known technique to POSITAs by 2003. Ex.1003, ¶125.

In addition, Krantz also discloses that data is communicated in its system from authorized clients “*without passing the data through the gatekeeper, when the requirements of the security policy are satisfied.*” Ex.1003, ¶126.

For example, with reference to Figure 2 (below), the “*gatekeeper*” (server 215) in Krantz is shown in gray, while the “*access point*”—including Access Point 209—is shown in green with “*communication port[s]*” shown in brown. As Dr. Houh confirms, upon a client’s authorization, data flows directly from “client 205” to VLAN C—i.e., it does not flow through the “*restricted subset*” (VLAN B) or the “*gatekeeper.*” Ex.1005, [0059], [0064], [0107] (describing the way data is transferred in the Krantz system).

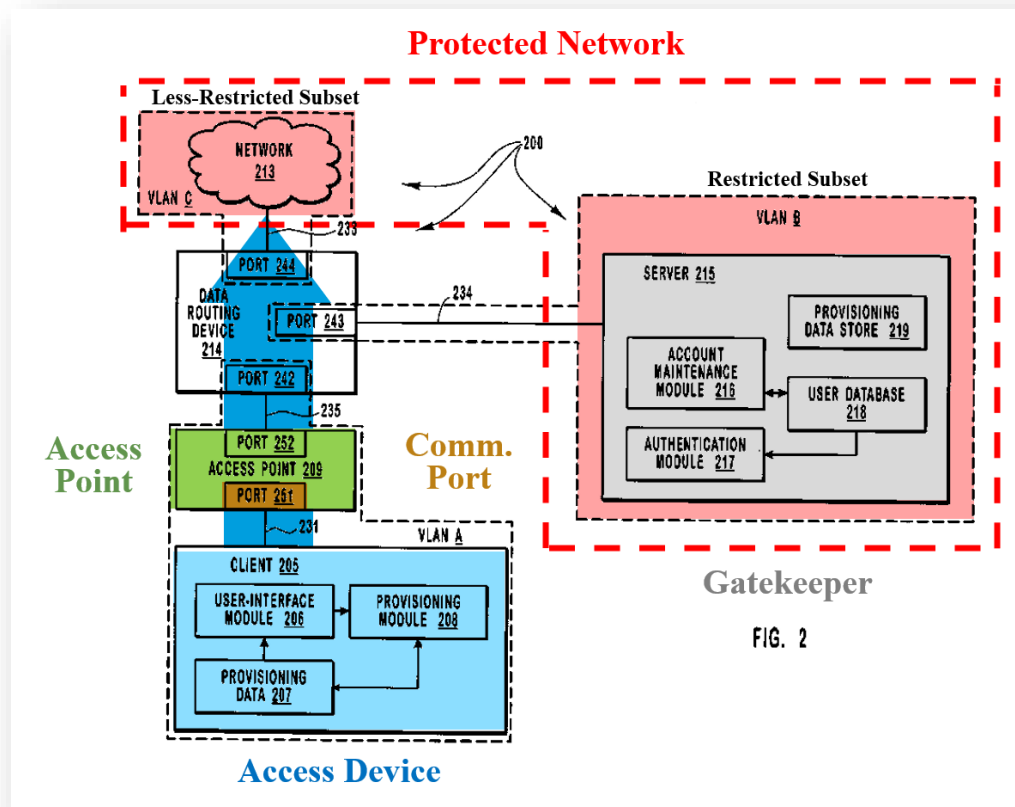


FIG. 2

Ex.1005, Figure 2 (annotated). Ex.1003, ¶127.

Krantz explains that “data routing device 214 can be configured to separate computer systems into different VLANs. As depicted in FIG. 2, **data routing device 214 has been configured to separate network architecture 200 into VLANs A, B, and C.** Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.” Ex.1005, [0060]; [0064] (“Access point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B

and/or VLAN C.”). Accordingly, by configuring the flow of data in this manner, the “*gatekeeper*” (server 215) need only apply security policies to authorize the access device access to data—such as the resources on VLAN C—but not actually have data pass through it. Ex.1005, [0062] (“Any of the ports included in data routing device 214 (e.g., ports 242, 243, and 244) can be configured to transfer tagged data frames but drop untagged data frames.”). Ex.1003, ¶128.

Based on Krantz’s disclosure, the communication path for an authorized “*access device*” would flow through “*communication port*” 244, as depicted in the annotated figure above. Ex.1003, ¶129.

Accordingly, Krantz teaches or suggests this claim element. Ex.1003, ¶130.

Mapping #3

To the extent one may assert that Krantz does not disclose “*reconfiguring the communication port*”—Port 251 on Access Point 209—it would have been obvious to do so based on Krantz itself for the reasons already explained above. *See* §VIII.A.1.iv. For example, as already explained, it would have been obvious to combine the functionality of the Data Routing Device and Access Point of Krantz in the same device. Ex.1003, ¶131.

In such a combined device, as Krantz explains, “when a portion of data, such as, for example, a data frame, is transferred in at a first port . . . **based on**

configuration rules, that the frame is to be transferred out at a second port (e.g., port 243). For example, data routing device 214 can determine that a data frame received from access point 209 is to be sent to server 215. **It may also be that a data frame is transferred in and out of data routing device 214 at the same port.** Ex.1005, [0059]. The combined device would be further enabled to “reconfigure” as necessary the “communication port” for transfer of data from an authenticated client to VLAN C. Ex.1005, [0060] (“Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.”); Ex.1005, [0064] (“Access point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C.”). Ex.1003, ¶132.

Accordingly, Krantz teaches or suggests this claim element for this additional reason as well. Ex.1003, ¶133.

Therefore, Krantz renders obvious claim 1. Ex.1003, ¶134.

2. Claim 2

i. [2.0] *The method of claim 1, further comprising authenticating a user of the access device.*

Krantz discloses that “[w]hen credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and

password) and compare the credentials to entries in **user database 218**. If credential information matches an entry in user database 218, **the identity of a user is authenticated** (server 215 believes that the user represented by the user-identifier is the user who entered the credential information). If an authenticated user of client 205 [the user of the access device] is authorized to access resources located on VLAN C (e.g., **the user is up to date on payments for their account**), client 205 can then be authorized to access resources located on VLAN C.”

Ex.1005, [0076]; *see also* Ex.1005, [0074] (describing using EAP to authenticate user, including through exchange of “certificates, keys, and supported cipher suites.” Krantz’s disclosure is consistent with the disclosure of the 460 Patent that describes requirements related to user identification and passwords or configuration requirements related to the access device (such as aspects of the operating system), (Ex.1001, 6:38-52), or authenticate an access device, or user, of the access device. Ex.1001, 11:35-43, 12:4-6. Ex.1003, ¶135.

Accordingly, Krantz renders obvious claim 2. Ex.1003, ¶136.

3. Claim 10

- i. ***[10.0] The method of claim 1, wherein the access point is a network switch.***

With respect to Krantz’s “*access point*”—the obvious combination of Access Point 209 and Data Routing Device 214 described above, *see* §VII.A.1.iv—Krantz

explains that “Data routing device 214 logically represents a special-purpose computer system, such as, for example, a router and/or a **switch**, that can determine how to transfer data between the ports included in data routing device 214.” Ex.1005, [0059]. Ex.1003, ¶164.

Accordingly, Krantz renders obvious claim 10. Ex.1003, ¶165.

4. Claim 11

- i. *[11.0] The method of claim 1, wherein the access point is a wireless access point.*

With respect to Krantz’s “*access point*”—Access Point 209—Krantz explains that “Network architecture also includes access point 209. **Access point 209 can be a wired or wireless access point** that facilitates communication between client 205 and data routing device 214.” Ex.1005, [0063]; *see also* Ex.1005, [0064] (“In some embodiments, **access point 209 is a wireless access point** that enables access to wired computer systems on VLAN B (e.g., server 215) and VLAN C (e.g., computer systems included in network 213). Ex.1003, ¶166.

Accordingly, Krantz renders obvious claim 11. Ex.1003, ¶167.

5. Claim 12

- i. *[12.0] The method of claim 1, wherein the access point is a remote access virtual private network.*

With respect to Krantz’s “*access point*”—Access Point 209—Krantz explains that the disclosed networks “can be implemented using any number of

techniques, such as, for example, . . . **Virtual Private Networks (“VPNs”).**”

Ex.1005, [0017]. Krantz, however, does not expressly disclose that the access point could comprise a “*remote access virtual private network*,” but it would have been obvious to implement that functionality in view of Krantz. Krantz recognizes the importance of security and access-control techniques, and a VPN was a well-known technique for preventing unauthorized access. Ex.1013 (a virtual private network is “a network where data is transferred over the Internet **using security features preventing unauthorized access.**”); Ex.1012 (a virtual private network is [a] highly secure network for transmitting sensitive data . . . that used the public Internet as a transmission medium....VPNs use encryption and protocol tunnelling.”). Krantz explicitly states that any secure methods, including VPNs, can be used to restrict access consistent with the disclosed methods. Ex.1005, [0055] (“It would be apparent to one skilled in the art, after having reviewed this description, that other techniques, in addition VLAN, IP filtering, and VPN techniques, can be used to allow access to one network, while restricting access to another network.”). Thus, it would have been obvious for the access point to be a “*remote access [VPN]*” because of the emphasis in Krantz on the use of security techniques and preventing unauthorized access as well as its actual disclosure of VPNs for components of the disclosed network. Ex.1005, [0017], [0032], [0038]. Ex.1003, ¶168.

Accordingly, Krantz renders obvious claim 12. Ex.1003, ¶169.

6. Claim 13

- i. *[13.0] The method of claim 1, wherein the gatekeeper is accessible to elements of the less-restricted subset of the protected network.*

See claim [1.0]. Ex.1003, ¶170.

In addition, the 460 Patent explains that “*elements*” are devices or software modules or similar—like Network PCs—that exist on the network. Ex.1001, 6:21-53. Such “*elements*” in Krantz would include “computer systems included in network 213.” Ex.1005, [0064]. Krantz explains that “[i]t may be that server 215 sets a **session timeout**, such as, for example, one hour, after which access point 209 **will request client 205** (“computer systems included in network 213”) **to re-authenticate** [with Server 215 “*gatekeeper*”)]. Ex.1005, [0108]. Thus, “*the gatekeeper is accessible to elements of the less-restricted subset of the protected work*” (*i.e.*, “computer systems included in network 213”) at least to re-authenticate their subscription. Ex.1003, ¶171.

Accordingly, Krantz renders obvious claim 13. Ex.1003, ¶172.

7. Claim 14

- i. ***[14.0] The method of claim 1, wherein the restricted subset of the protected network is characterized by an access control list.***

Krantz explains that “[d]ata routing device 414, components in network 411, or components in logical communication link 433 can filter Internet Protocol (‘IP’) address to limit client 405’s access to resources with particular IP addresses.”

Ex.1005, [0053]. Krantz further explains “[w]hen client 405 is not authorized to access resources located on network 413, IP addresses can be filtered such that client 405 is exposed to IP addresses of resources located on network 412 but is not exposed to IP addresses of resources located on network 413.” Ex.1005, [0053]. Ex.1003, ¶174.

Krantz further explains that “a server located on network 413 **may implement IP filtering to provide client 405 with limited access to network 413** [“*the restricted subset*”]. Included in the limited access can be access to computer systems or modules that store provisioning files needed for gaining full access to network 413.” Ex.1005, [0056]. Dr. Houh explains that limiting access to server resources for specific clients through IP filtering is a form of an “*access control list*,” and that it would have been obvious to use an “*access control list*” in a VLAN embodiment because such an embodiment has client access control

considerations. Ex.1005, [0052] (“For example, **when client 405 is not authorized to access resources** located network 413 . . .”) Ex.1003, ¶175.

Accordingly, Krantz renders obvious claim 14. Ex.1003, ¶176.

8. Claim 16

- i. *[16.0] A non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor to perform a method for controlling access to a computer network, the method comprising:*

See claim [1.0] (describing an authorization procedure for “granting”/“controlling access” to a protected “network” of computers). Ex.1003, ¶¶65-76, 177.

Additionally, Krantz discloses “[a] non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor” to perform the functionality addressed with respect to claim 16. Ex.1003, ¶178.

In Krantz, this can include “computer program products, and data structures” that can increase the level of automation for provisioning and configuring an access device (e.g., a computer system) to access a computer network. Ex.1005, [0014]. Numerous forms of non-transitory computer readable storage media are described in Krantz such as floppy disk and flash cards (*id.*, [0021]) as well as “RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk

storage or other magnetic **storage devices**, or any other medium which can be used to carry or store desired program code.” Ex.1005, [0036]; Ex.1003, ¶179.

Krantz uses the term “computer-readable medium” as it would be understood to a POSITA. Krantz states that “[w]hen information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a computer system, the computer system properly views the connection as a **computer-readable medium**. Thus, any such connection is properly termed a computer-readable medium.” Ex.1005, [0037]. Ex.1003, ¶180.

Krantz discloses that “[t]he drives and their associated **computer-readable media provide nonvolatile storage** of computer-executable instructions, data structures, program modules and other data for the computer 120” as seen in Fig. 1. Ex.1005, [0043]. Ex.1003, ¶181.

Krantz explains how “portions of such modules and portions of associated program data may be included in operating system 135, application programs 136, program modules 137 and/or program data 138, for storage in **system memory** 122 ... [and] [e]xecution of such modules may be performed in a distributed environment as previously described.” Ex.1005, [0049]. Ex.1003, ¶182.

Accordingly, Krantz teaches or suggests this claim element. Ex.1003, ¶183.

- ii. *[16.1] receiving a request for access to a less-restricted subset of the protected network from an access device,*

See claim [1.1]. Ex.1003, ¶¶77-85, 184.

- iii. *[16.2] the request being received through a communication port of an access point,*

See claim [1.2]. Ex.1003, ¶¶86-91, 185.

- iv. *[16.3] the communication port configured for communicating between the access device and a restricted subset of the protected network,*

See claim [1.3]. Ex.1003, ¶¶92-109, 186.

- v. *[16.4] the restricted subset including a gatekeeper; applying a security policy to the access device in response to the request; and*

See claim [1.4]. Ex.1003, ¶¶110-118, 187.

- vi. *[16.5] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when requirements of the security policy are satisfied.*

See claim [1.5]. Ex.1003, ¶¶119-134, 188.

9. Claim 17

- i. *[17.0] The non-transitory computer readable storage medium of claim 16, wherein the program is further executable by a processor to authenticate a user of the access device.*

See claims [16.0], [2.0]. Ex.1003, ¶¶135-136, 189.

10. Claim 27

- i. ***[27.0] The non-transitory computer readable storage medium of claim 16, wherein the program is further executable to update the access device when requirements of the security policy are not satisfied.***

Krantz explains that “[w]hen full access to resources located on the second network is not authorized, the server can authorize limited access to the first network or second network such that the client can download provisioning files for gaining full access [to] resources located on the second network.” Ex.1005, [0032]; *see also* Ex.1005, [0056]; Ex.1005, [0110] (“[T]he method 300 also includes an act of executing a schema-based document (act 306). This can include executing a third schema-based document to configure a client for accessing the second network [*“the program is further executable”*]. For example, provisioning module 208 can execute an XML document . . . to configure client 205 for accessing resources located on VLAN C [*“update the access device when requirements of the security policy are not satisfied”*]. Provisioning module 208 can retrieve previously downloaded XML documents, such as [], a configuration sub-file, from provisioning data 207.”). For example, Krantz explains that “[i]f credentials do not authorize full access to the second network (e.g., credentials cannot be authenticated, credentials are guest credentials, or an authenticated user is not authorized)” the server can notify the client and send a “configuration sub-file” that “can be executed to configure connection type, communication protocols,

authentication type, encryption type, etc.” Ex.1005, [0019]-[0020], [0024].

Ex.1003, ¶206.

Accordingly, Krantz renders obvious claim 27. Ex.1003, ¶207.

11. Claim 29

- i. *[29.0] The non-transitory computer readable storage medium of claim 16, wherein the restricted subset of the protected network is characterized by an access control list.*

See claim [14.0]. Ex.1003, ¶¶173-176, 208.

12. Claim 30

- i. *[30.0] The non-transitory computer readable storage medium of claim 29, wherein access to the restricted subset of the protected network is responsive to a VLAN configured to communicate with the protected network subject to the access control list.*

See claim [14.0]. Ex.1003, ¶¶173-176, 209.

Krantz further describes that client 205 is a component of VLAN A. Ex.1005 [0052]; FIG 2. Thus, a POSITA understood that when client 205 accesses VLAN B using an access control list as described with respect to limitation [14.0], VLAN A is “*configured to communicate with the protected network subject to the access control list.*” Ex.1003, ¶210.

B. Ground 2: Claims 1-6, 10-14, 16-22, 27, and 29-30 are Obvious Based on Krantz and Herrmann

1. Claims 1-2, 10-14, 16-17, 27, and 29-30

As demonstrated above, Krantz teaches or suggests each element of claims 1-2, 10-14, 16-17, 27, and 29-30. To the extent one may assert that Krantz does not teach or suggest “*applying a security policy . . .*” or “*using the gatekeeper to determine if requirements of the security policy are satisfied by the access device*” in claim elements [1.4] (and [16.4] with respect to “*applying a security policy . . .*”), those elements would have been obvious based on the teachings of Krantz and Herrmann. Ex.1005, ¶211.

Specifically, it would have been obvious to include Herrmann’s techniques related to enforcing security policies and obtaining system data from an access device (including checking for anti-virus protection at the client) in the system of Krantz for the reasons explained below. In particular, the Krantz system already discloses that “access point 209 may block [] protocols ... from being transferred **until client 205 is authenticated (and authorized).**” Ex.1005, [0072].

Specifically, Krantz explains that as part of its security policies, client devices are authenticated, (Ex.1005, [0067]-[0074], [099]) and users of client devices are authenticated, Ex.1005, [0074], [0076]. Krantz’s disclosure is consistent with the disclosure of the 460 Patent that the security policy may proscribe encryption protocols, (Ex.1001 2:18-26), and may include requirements related to user

identification and passwords or configuration requirements related to the access device (such as aspects of the operating system), (Ex.1001, 6:38-52), or authenticate an access device (or user) of the access device. Ex.1001, 11:35-43, 12:4-6. Ex.1003, ¶51.

A POSITA would recognize that checking for anti-virus software as part of a security policy would merely be an additional item for server 215 to check in the process disclosed by Krantz. Ex.1005, [Fig. 3], [0068]-[0076] (describing the steps of authenticating client devices and users). Like Krantz, Herrmann discloses a “policy server 460 [which] may enforce a variety of different types of security policies or rules.” Ex.1006, [0068]. One such rule, to be authorized for network access, would be “a policy requiring that a **specific virus protection program** is operational on each client device that is connected to a network.” Ex.1006, [0012]. Herrmann recites that the policy server determines whether the client device 310 complies with applicable security policies. Ex.1006 [0066]. Ex.1003, ¶52.

A POSITA would also be motivated to modify the teachings of Krantz to include determining whether the requirements of a security policy that include checking for virus protection are satisfied as taught by Herrmann for several reasons. As explained above, *see* §VII.A.1.v & §VII.A.2, Krantz already describes a security policy that includes requiring authentication of a client device and users. Krantz also teaches providing a configuration file with the proper encryption

protocol (and other necessary configuration information), the client device is configured to for compatible operation with the network. Herrmann discloses that it is “particularly important” that devices connected to the network are running current anti-virus programs, and that one way of ensuring this is implementing a “policy requiring that a **specific virus protection program.**” Ex.1006, [0068]; *see also*, Ex.1006, [0012] (noting it is critical that all machines in a network maintain updated antivirus software so the network is not infiltrated by newly released viruses). Herrmann expressly recites that the policy server determines whether the client device 310 complies with applicable security policies, which would include specific virus detection. Ex.1006, [0066]. Thus, a POSITA would be motivated to modify the teachings of Krantz to include a security policy’s requirements that a specific virus protection program be utilized, and to determine if the client device satisfies the applicable security policies before allowing the client device to access protected networks in order to prevent viruses from infecting the protected network and to ensure network compatibility. Ex.1003, ¶53.

Krantz’s server 215, which already compares the credentials of the client through authentication techniques (Ex.1005, [0068]-[0074], [099], and a user against a database (Ex.1005, [0076]), as modified by Herrmann, would additionally compare a virus protection program on an access device against approved antivirus programs (Ex.1006, [0057]). Information regarding approved

antivirus software and approved connected devices could be stored in the user database or an additional database could be added. Moreover, Krantz's provisioning data store 219 would be modified to include virus protection software which would be included in a configuration file sent to the client device with the other configuration information to ensure the client device has the most up-to-date virus protection. In addition, if Krantz first determined the client device was already provisioned with the required virus protection (and any other configuration settings such as encryption), it would avoid the need to send the configuration file to the client device as reconfiguration would be unnecessary. This results in a more efficient use of resources since it avoids unnecessarily sending a configuration file and needlessly reconfiguring the client device that was already determined to be compliant with the security policy. Ex.1003, ¶54.

The 460 Patent confirms that a POSITA would recognize the need for the system of Krantz to check for up-to-date and approved antivirus programs or encryption protocols. It explains that “GateKeeper 110 may make certain that Access Device 160 has up-to-date virus software and encryption protocols as proscribed by [a] security policy.” Ex.1001, 2:23-26. Ex.1003, ¶55.

Both Krantz and Herrmann are analogous art to the 460 Patent for at least two reasons. *First*, Krantz and Herrmann are both directed toward the same field

of endeavor of the 460 Patent—network security. Ex.1001, 1:23-24; Ex.1005, Abstract; Ex.1006, Abstract. Ex.1003, ¶56.

Second, both Krantz and Herrmann are reasonably pertinent to a problem described by the 460 Patent: the reliance “on mere user authentication” and the need to “assure that **an access device** used by the authenticated user meets network security policies” such as current anti-virus software. Ex.1001, 1:45-60. Both references teach additional aspects to a security policy. Ex.1003, ¶57.

Krantz discloses a security policy beyond user authentication and encryption protocols. For instance, “[a]fter an EAP type is selected . . . **computer systems can attempt to authenticate with one another** through the transfer of EAP messages . . . in accordance with the selected EAP type. For example, when EAP-TLS is selected, **client 205 may communicate with server 215** through a series of EAP messages in accordance with EAP-TLS **so as to be authenticated and possibly authorized to access resources located on VLAN C.**” Ex.1005, [0068]. The use of EAP-TLS (*e.g.*, Ex.1005, [0067]-[0074], [0100]) was a known authentication protocol that would be used to authenticate client devices. Ex.1016 [RFC2716] at 1, 2. Krantz further discloses that the security policy can include “a configuration sub-file to indicate whether or not **operating system credentials** should be used for authentication.” Ex.1005, [0099]. Ex.1003, ¶58.

Krantz discloses that “[i]n some embodiments, a server on a network can provide a client with limited access to the network. For example, a server located on network 413 may implement IP filtering to provide client 405 with limited access to network 413. Included in the limited access can be access to computer systems or modules that store **provisioning files needed for gaining full access to network 413.**” Ex.1005, [0056]. Krantz explains that a “[a] configuration sub-file can be executed to configure connection type, communication protocols, authentication type, encryption type, etc.” Ex.1005, [0110]-[0111]. Ex.1003, ¶59.

Herrmann similarly discloses a “policy agent (or integrity agent) 413 to retrieve information about the current security policy in operation on the client device 310. The information [is] collected by the policy agent 413...” Ex.1006, [0064]. “In response to a message from the IGW server 450 (or a subsequent message from the policy agent 413 on the client device 310), the policy server 460 evaluates whether or not **the client device 310 has a correct, up-to-date version of the applicable security policy.**” Ex.1006, [0067]. The policy server is notified by the client, containing policy agent 413, through periodic status messages called “IA_HEARTBEAT(s)” to authenticate the access device. Ex.1006, [0080], [0098]. Ex.1003, ¶60.

Herrmann further discloses that “[i]t becomes critical . . . to promptly update **anti-virus applications on all machines in a network** in a timely fashion before

the network is infiltrated by a newly released virus.” Ex.1006, [0012]. Herrmann also discloses that “a network administrator may require all users accessing the network to implement a **virus definition update (e.g., DAT file)** that is targeted at a particular virus.” Ex.1005, [0071]; *see also* Ex.1006, [0068]. Ex.1003, ¶61.

It would have been obvious to combine Herrmann’s techniques related to determining whether an access device is authorized for network access (including checking its antivirus software) with the authentication and authorization system of Krantz. Each performs the same function (authentication and authorization to access network resources) with each yielding not more than what one would expect from such an arrangement (automated network access techniques including a higher level of security by checking antivirus software), as the Krantz/Herrmann system demonstrates. Ex.1003, ¶62.

A POSITA would have been motivated to combine Herrmann with Krantz based on the teachings of Krantz. For example, Krantz explains that its system relates to a server that “includes the functionality to authorize clients to access a second network” EX.1005, [0016]. Similarly, Herrmann explains that “[t]he present invention relates [] to ... policy enforcement on **computer systems** connected to one or more networks...” EX.1006, [0003]. Ex.1003, ¶63.

A POSITA would have also been motivated to apply Herrmann’s technique of checking connecting computer systems for antivirus software as it would not

only provide **added security** but **increase automation** when connecting to a network. Ex.1006, [0068]. These are two stated goals of Krantz. Ex.1005, [0014], [0019]. Thus, a POSITA would have recognized that Herrmann's disclosure of a policy server checking that a computer device complies with, e.g., an antivirus security policy, would be complimentary to the system of Krantz, which seeks an automated process for providing network security. In addition, a POSITA would have had a reasonable expectation of success in implementing these techniques into a combined Krantz/Herrmann system as doing would involve minimal changes to the existing Krantz system. Ex.1003, ¶64.

In the combined Krantz/Herrmann system, server 215 (“*gatekeeper*”) of Krantz would include within its own “*security policy*”—*i.e.*, the authentication of both the client device and the user—a requirement for a virus protection program as taught by Herrmann. In the Krantz/Herrmann system, server 215 would make determination as to whether the client complies with the security policies. Ex.1003, ¶212.

Accordingly, Krantz and Herrmann render obvious claims 1-2, 10-14, 16-17, 27 and 29-30. Ex.1003, ¶213.

2. Claim 3

- i. *[3.0] The method of claim 1, further comprising obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.*

Krantz does not expressly disclose all of the elements of claim 3, but it would have been obvious in view of Herrmann. Ex.1003, ¶137. A POSITA would have been motivated to combine Krantz with Herrmann for the reasons described above. *See* §B.1.

It would have been obvious to include Herrmann's techniques for “*obtaining system data from an access device*” (e.g., evaluating whether the access device includes antivirus software) in the system of Krantz. The Krantz system already discloses that “access point 209 may block [] protocols ... from being transferred **until client 205 is authenticated (and authorized)**.” Ex.1005, [0072]. Furthermore, “[w]hen credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) **and compare the credentials to entries in user database 218.**” Ex.1005, [0076]; Ex.1003, ¶138.

A POSITA would recognize that checking for anti-virus software would merely be an additional item for server 215 (“*gatekeeper*”) to check in the authentication process already disclosed by Krantz. Like Krantz, Herrmann discloses that a “policy server 460 [which] may enforce a variety of different types

of security policies or rules.” Ex.1006, [0068]. One such rule, to be authorized for network access, would be “a policy requiring that a **specific virus protection program** is operational on each client device that is connected to a network.” Ex.1006, [0012] (noting it is critical that all machines in a network maintain updated antivirus software so the network is not infiltrated by newly released viruses). Moreover, Dr. Houh explains that a POSITA would be motivated to modify the system of Krantz to include the additional policy requiring a specific virus protection program because Krantz is specifically focused on network authentication and security. Ex.1005, [Abstract]. Ex.1003, ¶139.

Krantz’s authentication module and server 215, which already authenticated the client device and compares the credentials of a user against a database (e.g., user-identifier and password), as modified by Herrmann, would additionally compare a virus protection program on an access device against approved antivirus programs (“*using the system data to determine that the access device satisfies the requirements of the security policy*”). Information regarding approved antivirus software and approved connected devices could be stored in the User Database of Krantz, for example. A POSITA would have had a reasonable expectation that this additional provision would be successful because Krantz already discloses conditions for client access, such as “signup” or “renewal” conditions to authorize access to network resources. Ex.1005, [0019]. Ex.1003, ¶140.

Accordingly, Krantz and Herrmann render obvious claim 3. Ex.1003, ¶141.

3. Claim 4

- i. ***[4.0] The method of claim 3, wherein the system data includes antivirus software status.***

Krantz identifies that one problem in prior art systems was that “software incompatibilities must be worked out by a user that may lack the technical expertise or desire to **re-configure software for compatibility with the service.**” Ex.1005, [0013]; Ex.1003, ¶142.

Krantz also specifically discusses how a connecting device may be required to have “provisioning files [] for gaining full access to network 413.” Ex.1005, [0056]; Ex.1005, [0032], [0078] (discussing provisioning clients for gaining access to the network). A POSITA would have understood that in practice, provisioning files generally relate to network connectivity and security, *see, e.g.*, Ex.1005, [0079]; *see also* Ex.1005, [0016], [0087], although Krantz does not explicitly mention antivirus software as a kind of “*system data*.” However, it would have been obvious in view of Herrmann for the reasons already stated above with respect to claim 3. A POSITA would have been motivated to combine Krantz with Herrmann for the reasons described above. *See* §B.1. Ex.1003, ¶143.

Herrmann, for example, specifically discloses that “[n]ew viruses are frequently released . . . [it] **becomes critical, therefore, to promptly update anti-**

virus applications on all machines in a network in a timely fashion before the network is infiltrated by a newly released virus.” Ex.1006, [0012]. Ex.1003, ¶144.

Herrmann further discloses that “a network administrator **may require all users accessing the network to implement a virus definition update (e.g., DAT file)** that is targeted at a particular virus.” Ex.1006, [0071]. This may be implemented using security rules and checking system data for connecting devices to ascertain compliance (confirming the “*antivirus software status*”). Ex.1006, [0068] (“[A] system administrator may establish a policy requiring that **a specific virus protection program is operational on each client device ...**”). In other words, checking “*system data*” to confirm the “*status*” of required “*antivirus software*” on the “*access device*.” Ex.1003, ¶145.

As discussed with respect to claim 3, a POSITA would be motivated to modify the system of Krantz to include the additional policy requiring a specific virus protection program because Krantz is specifically focused on network authentication and security. Ex.1005, [Abstract]. Further, a POSITA would have had a reasonable expectation that this additional provision would be successful because Krantz already discloses conditions for client access, such as “signup” or “renewal” conditions to authorize access to network resources. Ex.1005, [0019]. Requiring the client to update antivirus software would merely be an additional condition. Ex.1003, ¶146.

Accordingly, Krantz and Herrmann render obvious claim 4. Ex.1003, ¶147.

4. Claim 5

- i. *[5.0] The method of claim 1, further comprising communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and*

Claim 5 is obvious over Krantz in view of the disclosures in Herrmann. As explained above with respect to claims 1 and 3, Krantz discloses obtaining system data from an access device and the application of a security policy to determine if access requirements are satisfied. A POSITA would have been motivated to combine Krantz with Herrmann for the reasons described above. See §B.1. Ex.1003, ¶148.

The 460 Patent explains that “Access Device 230 includes an agent configured to monitor code running on Access Device 230 and report any suspicious code to GateKeeper 225.” Ex.1001, 7:21-26; *see also* Ex.1001, 7:26-30. Ex.1003, ¶149.

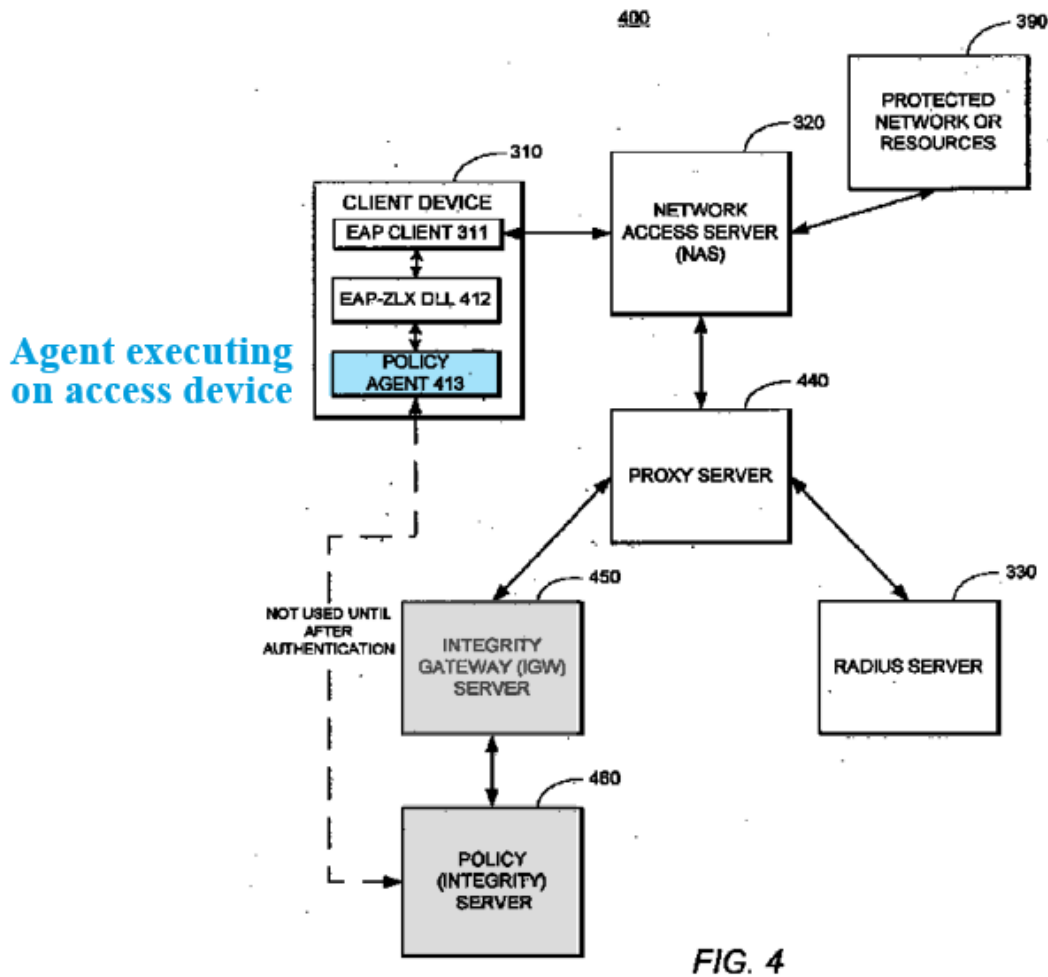
Krantz discloses that “client 205 and server 215 **exchange EAP-messages** to pass certificates, keys, and supported cipher suites. Depending on the EAP type, other credential information may also be exchanged between client 205 and server 215.” Ex.1005, [0074]. With respect to the XML configuration schema disclosed in [0091] of Krantz, a handshake protocol may be used between the access device

and the gatekeeper. Ex.1005 [0099] (“a configuration sub-file to indicate a type of EAP [is] used to authenticate a server with a client and/or to authenticate a client with a server. Either or both of the elements at lines 61 and 62 can be included in a configuration sub-file to indicate different EAP types, such as, for example, EAP-TLS and EAP Microsoft Challenge/Replay Handshake Protocol Version (‘EAP-MSChapV2’). When EAP-MSChapV2 is indicated, the ‘MSChapV2 Parameters’ element at line 67 can be included in a configuration sub-file to indicate whether or not **operating system credentials should be used for authentication.**”)

(“*communicating between the gatekeeper and ...*”). Ex.1003, ¶150.

A POSITA would have understood that one way that credentials (e.g., operating system credentials, certificates, keys, and supported cipher suites, etc.) such as those disclosed in Krantz would be retrieved and/or sent would be by utilizing a client agent, although Krantz does not expressly state that such an agent is used. Ex.1006, [0028], [0067]. However, it would have been obvious in view of Herrmann to do so. Ex.1003, ¶151.

For example, Herrmann discloses a “POLICY AGENT 413” (an “*agent*”) (emphasized in blue) executing on the client device (“*executing on the access device*”), interacting with a “POLICY (INTEGRITY) SERVER 460” and “INTEGRITY GATEWAY (IGW) SERVER 450” (collectively emphasized in gray) as shown below. Ex.1003, ¶152.



Ex.1006, Fig. 4 (annotated). Ex.1003, ¶152.

Herrmann discloses that “policy agent (or integrity agent) 413 []retrieve[s] information about the current security policy in operation on the client device 310 [“to obtain system data from the access device”].” Ex.1006, [0064].

Herrmann further explains: “In response to a message from the IGW server 450 (or a subsequent message from the policy agent 413 on the client device 310), the

policy server 460 evaluates whether or not the client device 310 has a correct, up-to-date version of the applicable security policy.” Ex.1006, [0067]. The policy server is notified by the client, containing policy agent 413, through periodic status messages called “IA_HEARTBEAT(s)” to authenticate the access device. Ex.1006, [0080], [0098]. Ex.1003, ¶153.

A POSITA would be motivated to add the security policy agent of Herrmann to the client device of Krantz for several reasons. As explained previously, two of the stated goals of Krantz involve automation and security. Ex.1005, [0014]; [0019]. Thus, a POSITA would have recognized that the policy *agent* of Herrmann would be complimentary to the system of Krantz, as it would provide an automated means of providing network security. Ex.1003, ¶154.

Moreover, there would be a reasonable expectation of success for adding the policy agent of Herrmann to the client device of Krantz, as Herrmann itself describes the policy agent as a “client-side component” that can communicate with an “EAP-ZLX extension DLL [which] is an implementation of the EAP protocol that is utilized to provide support for security policy negotiation and enforcement.” Ex.1006, [0064]; [Fig. 4]. This is the same protocol utilized in Krantz. Ex.1005, [0018]. Ex.1003, ¶155.

Accordingly, Krantz and Herrmann render obvious this claim element. Ex.1003, ¶156.

- ii. *[5.1] wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.*

See claim [3.0]. Ex.1003, ¶157.

5. Claim 6

- i. *[6.0] The method of claim 5, wherein the system data includes information regarding devices connected to the access device.*

As explained above with respect to claim 3, Krantz in view of Herrmann discloses obtaining *system data* from an access device and the application of a security policy to determine if access requirements are satisfied. Ex.1003, ¶158.

Krantz does not expressly disclose “*wherein the system data includes information regarding devices connected to the access device,*” but it would have been obvious in view of Herrmann. Ex.1003, ¶159. A POSITA would have been motivated to combine Krantz with Herrmann for the reasons described above. See §B.1.

It would have been obvious to include Herrmann’s techniques for obtaining system data from an access device (e.g., whether or not the access device includes antivirus software) in the system of Krantz. Herrmann also discloses the use of Local Area Networks, (e.g., a corporate LAN). Ex.1006, [0012]. Herrmann discusses how “[a]n infected computer that is **connected to a particular network (e.g., a corporate LAN)** may be infected with a virus that intentionally tries to

spread itself to other machines in the network. One machine that is not running the correct anti-virus engine or is not equipped with current virus signature definition files may jeopardize the security of the entire network.” *Id.* Ex.1003, ¶159.

Because of these risks, Herrmann discloses various well-known techniques such as an “agent [that] monitors and controls the interaction of the local machine **with other machines and devices that are connected on a LAN** or a larger wide area network (WAN), such as the Internet, in order to provide security to the machine.” Ex.1006, [0028]. Because any single connected device on, e.g., a corporate LAN, may jeopardize all local connected devices (including the access device), a POSITA would recognize that the policy server 460 would need to be aware of all devices connected to the access device on the LAN to ensure they each have up to date antivirus software. Ex.1006, [0057], [0067]; *see also* Ex.1015, 12:46-13:15 (additional security features include “alarm/lockout functions” and “audit trail[s]” “of all systems to which the device is attached.”) Ex.1003, ¶160.

Additionally, Herrmann incorporates by reference U.S. Pat. No. 5,987,611 titled “System and Methodology for Managing Internet Access on a Per Application Basis for Client Computers Connected to the Internet” to Freund. Ex.1014 (“Freund”). Freund differentiates from “people” and “computers” on a network and how “groups” can be created for either people or computers, e.g., as depicted in Fig. 7F.

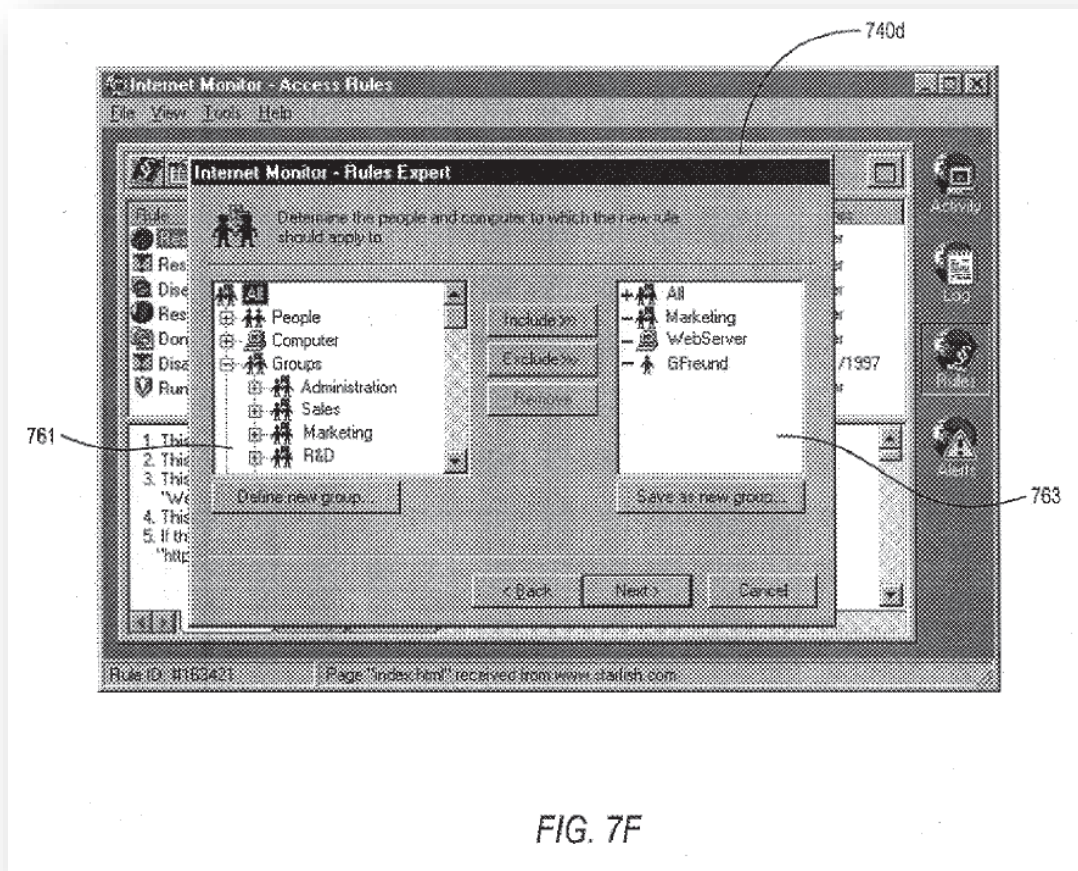


FIG. 7F

Ex.1014, Figure 7F. Ex.1003, ¶161.

Thus, for all these reasons, Dr. Houh explains that a POSITA would recognize that in order to create such “groups” on a LAN, there would need to be an awareness (e.g., by the policy server 460) of *devices connected to an access device*. Ex.1003, ¶162.

Accordingly, Krantz and Herrmann render obvious claim 6. Ex.1003, ¶163.

6. Claim 18

- i. *[18.0] The non-transitory computer readable storage medium of claim 16,*

See claim [16.0]. Ex.1003, ¶¶177-183, 190.

- ii. *[18.1] wherein the program is further executable by a processor to obtain system data from the access device, and*

See claim [5.0]. Ex.1003, ¶¶148-156, 191.

- iii. *[18.2] wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.*

See claim [3.0]. Ex.1003, ¶¶137-141, 192.

7. Claim 19

- i. *[19.0] The non-transitory computer readable storage medium of claim 18, wherein the system data includes antivirus software version data.*

See claim [4.0]. Ex.1003, ¶¶142-147, 193.

8. Claim 20

- i. *[20.0] The non-transitory computer readable storage medium of claim 16,*

See claim [16.0]. Ex.1003, ¶¶177-183, 194.

- ii. *[20.1] wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and*

See claim [5.0]. Ex.1003, ¶¶148-156, 195.

- iii. *[20.2] wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.*

See claim [3.0]. Ex.1003, ¶¶137-141, 196.

9. Claim 21

- i. *[21.0] The non-transitory computer storage readable medium of claim 20, wherein the system data includes information regarding devices connected to the access device.*

See claim [6.0]. Ex.1003, ¶¶158-163, 197.

10. Claim 22

- i. *[22.0] The non-transitory computer readable storage medium of claim 16, wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset.*

See claims [5.0], [16]. Ex.1003, ¶¶148-156, 198.

Krantz discloses that “the security status of the access device” is “monitor[ed] . . . after reconfiguring the communication port for communicating between the access device and the less-restricted subs.” Krantz explains that:

It may be that server 215 sets a **session timeout**, such as, for example, one hour, after which access point 209 **will request client 205 to re-authenticate**. If a subscription is still valid at the time of re-authentication, client 205 can re-authenticate **in the background** by submitting appropriate credentials to server 215. ... **A subscription period can expire after a specified period of time ... or after a specified number of connections ... After appropriate completion of the renewal user-interface client 205 can be re-authenticated.**

Ex.1005, [0108]. Ex.1003, ¶201.

Krantz does not disclose all the elements of claim 22, but it would have been obvious over Krantz in view of Herrmann. Ex.1003, ¶159. A POSITA would have been motivated to combine Krantz with Herrmann for the reasons described above. See §B.1.

Herrmann discloses continuous monitoring by an “*agent executing on the access device*,” including “*after reconfigur[ation]*.” Herrmann explains that “[a]lternatively, if the NAS supports the ability to remove the restrictive filter, then the IGW server can direct the NAS to remove the restrictive filter once the client has established compliance with the required policy. When the client has taken the necessary steps to comply with the policy, **the policy server is notified by the client (e.g., through an ‘IA_HEARTBEAT’ message, which is a periodic status**

message sent from the client directly to the policy server). If the policy server verifies that the client is indeed in compliance with the assigned policy, it sends an ‘ISS_AUTH_OK’ message to the IGW server to indicate that the session should be unrestricted. In response to receiving the ‘ISS_AUTH_OK’ message from the policy server, the IGW server directs the NAS to remove the restrictive filter.”

Ex.1006, [0080]. Ex.1003, ¶202.

Because of known risks in a networked environment, a POSITA would have looked to some of the well-known security techniques disclosed in Herrmann such as an “**agent** [that] monitors and controls the interaction of the local machine **with other machines and devices that are connected on a LAN** or a larger wide area network (WAN), such as the Internet, in order to provide security to the machine.” Ex.1006, [0028]. Because any single connected device on, e.g., a corporate LAN, may jeopardize all local connected devices (including the access device), a POSITA would recognize that the policy server 460 would need to be aware of all devices connected to the access device on the LAN to ensure they each have up to date antivirus software. Ex.1006, [0057], [0067]. Ex.1003, ¶203.

Accordingly, Krantz and Herrmann renders obvious claim 22. Ex.1003, ¶204.

IX. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION AND DENY INSTITUTION

A. The Board Should Not Deny Institution Under 35 U.S.C. § 325(d)

Denial under § 325(d) is not warranted because the grounds advanced are neither cumulative nor redundant to the prosecution of the 460 Patent (or related patents), as neither Krantz nor Herrmann was cited or considered by the Examiner during prosecution of the 460 Patent. Further, the 460 Patent has not been previously challenged in an IPR. In addition, the Examiner also did not have the benefit of Dr. Houh’s detailed expert testimony and the further evidence of record.

B. The Board Should Not Deny Institution Under 35 U.S.C. § 314(a)

1. No Evidence Regarding a Stay

Factor 1, for example, is **neutral** because no request for stay has been filed. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15 at 12 (May 13, 2020) (informative) (explaining that factor 1 generally “does not weigh for or against discretionary denial” when neither party has requested a stay); *Amazon Web Services et al. v. Zentian Ltd.*, IPR2023-01194, Paper 10 at 11 (Jan. 10, 2024).

2. Parallel Proceeding Trial Date

No trial date has been set. According to the most recent statistics⁶ on median time-to-trial for civil actions in the Northern District of California, the median time from filing to trial was 48.9 months. The related litigations were filed in May and August of 2023, so trial can be expected in approximately May 2027 and August of 2027. Any Final Written Decision can be expected in August of 2025, likely over a year before trial. Accordingly, this factor **weighs against** discretionary denial.

3. Parallel Proceeding Investment

Factor 3 **weighs against** discretionary denial. The related litigations are in its early stages of discovery, a motion to dismiss has been filed, and the investment by the parties has been relatively minimal. In addition, claims 13 and 14 are not at issue in the related litigations. *Samsung Bioepis Co. Ltd v. Regeneron Pharmaceuticals, Inc.*, IPR2023-00739, Paper 9 at 57 (Oct. 20, 2023) (“[B]ecause certain of the challenged claims, . . . are not expressly at issue in the district court litigation, *Fintiv* factor 3 favors institution.”)

⁶ <https://www.uscourts.gov/statistics-reports/federal-court-management-statistics-december-2023>

4. Overlapping Issues with the Parallel Proceeding

Regarding factor 4, the Patent Owner is only asserting a subset of the claims that are being challenged in this Petition. Thus, this factor also **weighs against** discretionary denial. *See Fintiv* Factor 3 analysis.

5. Overlapping Parties

Factor 5 is **neutral**. The Petitioner are both defendants in related litigations. As *Fintiv* demonstrates, this factor should play a role only where a Petitioner is unrelated to a defendant in a district court proceeding. *Fintiv*, IPR2020-00019, Paper 11 at 13-14. *Fintiv* “says nothing about situations in which the petitioner is the same as, or is related to, the district court defendant.” *Id.*

6. Strength of Petition and Other Considerations

Other circumstances **weigh against** discretionary denial. Here, the merits of the Petition are particularly compelling—for example, Krantz (and Herrmann) is a strikingly similar disclosure to that of the 460 Patent, is directed at the same problem and proposes the same solutions as the 460 Patent and discloses nearly identical architecture. The evidence presented, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.

X. CONCLUSION

Claims 1-6, 10-14, 16-22, 27 and 29-30 of the 460 Patent are unpatentable for the reasons demonstrated above.

Dated: March 5, 2024

Respectfully Submitted,

/Scott M. Border/

Scott M. Border

Reg. No. 77,744

Winston & Strawn LLC

1901 L Street, N.W.

Washington, D.C. 20036

T: 202-282-5054

sborder@winston.com

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with the type-volume limitations of 37 C.F.R. § 42.24, because it contains 13,955 words (as determined by the Microsoft Word word-processing system used to prepare the brief and including annotations to the figures), excluding the parts of the brief exempted by 37 C.F.R. § 42.24.

Dated: March 5, 2024

Respectfully Submitted,

/Scott M. Border/
Scott M. Border
Reg. No. 77,744
Winston & Strawn LLC
1901 L Street, N.W.
Washington, D.C. 20036
T: 202-282-5054
sborder@winston.com

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I hereby certify that on this 5th day of March, 2024, I caused to be served a true and correct copy of the foregoing and any accompanying exhibits by priority mail on the following:

Lewis Roca Rothgerber Christie LLP
PO BOX 29001
Glendale, CA

Brian R. Michalek
SAUL EWING LLP
161 N. Clark St., Suite 4200
Chicago, IL 60601

InfoExpress, Inc.
2975 Bowers Ave #323
Santa Clara, CA 95051

with a Courtesy Copy by electronic mail to Patent Owner's Litigation Counsel:
Tosti, Jacob A. jacob.tosti@saul.com; Michalek, Brian R.
brian.michalek@saul.com; Grabenstein, Casey Casey.Grabenstein@saul.com;
Schwerin, Andrew andrew.schwerin@saul.com; Kuo, Joseph M.
joseph.kuo@saul.com; mflynnobrien@bdiplaw.com; bentzminger@bdiplaw.com

Dated: March 5, 2024

Respectfully Submitted,

/Scott M. Border/
Scott M. Border
Reg. No. 77,744
Winston & Strawn LLC
1901 L Street, N.W.
Washington, D.C. 20036
T: 202-282-5054
sborder@winston.com