

Filed: April 18, 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.

IPR2024-00675
U.S. Patent No. 7,523,484

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 7,523,484**

TABLE OF CONTENTS

	Page
<u>EXHIBIT LIST</u>	i
<u>CLAIM LISTING</u>	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 Information	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 484 PATENT	4
A. Effective Filing Date	4
B. Person of Ordinary Skill in the Art.....	4
C. Overview of the 484 Patent	4
VI. CLAIM CONSTRUCTION	6
VII. PRINCIPAL PRIOR ART	7
A. Summary of Krantz	7
B. Summary of Herrmann.....	9
C. The Combination of Krantz and Herrmann	13
VIII. THE CHALLENGED CLAIMS ARE UNPATENTABLE	19
A. Ground 1: Claims 1–5, 11, 12, 16-19 and 23-25 are Obvious Based on Krantz.....	19
1. Claim 1	19
i. [1.0] A network gatekeeper comprising:	19

ii.	[1.1] at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network;	25
iii.	[1.2] a policy auditor configured to audit the access device using the at least one security policy, in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device to the gatekeeper via a communication device; and	32
a.	a policy auditor...	32
b.	in response to.	36
iv.	[1.3] an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy, 40	
a.	...if the audit results.	40
b.	an access control configured...	41
v.	[1.4] the restricted subset of the protected network including the gatekeeper	55
2.	Claim 2	56
3.	Claim 3 - <i>wherein the network gatekeeper is further configured to update the access device using an update module.</i>	59
4.	Claim 4 - <i>wherein the network gatekeeper is further configured to obtain system data from the access device.</i>	60
5.	Claim 5 - <i>wherein the network gatekeeper is further configured to use the system data to determine if the access device meets requirements of a security policy, and to issue commands responsive to this determination, the commands being configured to grant access to the less-restricted subset.</i>	61
6.	Claim 11 - <i>wherein the at least one security policy is responsive to an identity of the access device.</i>	61
7.	Claim 12 - <i>wherein the at least one security policy is selected by the policy auditor responsive to a part of the less-restricted subset of the protected network to which access is requested.</i>	62

8.	Claim 16 - <i>wherein the communication device includes a wireless access point.</i>	62
9.	Claim 17 - <i>wherein the communication device includes a wireless access point configured to support an 802.1x standard.</i>	63
10.	Claim 18 - <i>wherein the communication device includes a network switch</i> and Claim 19 - <i>wherein the communication device includes a router.</i>	63
11.	Claim 23 - <i>wherein the network gatekeeper is further configured to authenticate a user of the access device.</i>	63
12.	Claim 24 - <i>wherein the network gatekeeper is configured to update the access device if requirements of the security policy are not satisfied.</i>	64
13.	Claim 25 - <i>wherein the communication device includes a remote access virtual private network.</i>	64
B.	Ground 2: Claims 1–6, 11–13, 15–19, and 23–25 are Obvious Based on Krantz and Herrmann	65
1.	Claim 1	65
i.	[1.1]-[1.3]	65
2.	Claim 3 - <i>wherein the network gatekeeper is further configured to update the access device using an update module.</i>	67
3.	Claim 4 - <i>wherein the network gatekeeper is further configured to obtain system data from the access device.</i>	68
4.	Claim 5	69
5.	Claim 6 - <i>wherein the system data includes antivirus software version data.</i>	70
6.	Claim 11 - <i>wherein the at least one security policy is responsive to an identity of the access device.</i>	70
7.	Claim 12 - <i>wherein the at least one security policy is selected by the policy auditor responsive to a part of the less-restricted subset of the protected network to which access is requested.</i>	71
8.	Claim 13 - <i>wherein the audit is responsive to antivirus software executing on the access device.</i>	72
9.	Claim 15 - <i>wherein the policy auditor is configured to request data from an agent on the access device.</i>	72

10.	Claim 24 - <i>wherein the network gatekeeper is configured to update the access device if requirements of the security policy are not satisfied</i>	76
IX.	THE BOARD SHOULD NOT EXERCISE ITS DISCRETION AND DENY INSTITUTION.....	80
A.	The Board Should Not Deny Institution Under 35 U.S.C. § 325(d) ...	80
B.	The Board Should Not Deny Institution Under 35 U.S.C. § 314(a)....	80
1.	No Evidence Regarding a Stay	80
2.	Parallel Proceeding Trial Date	81
3.	Parallel Proceeding Investment.....	81
4.	Overlapping Issues with the Parallel Proceeding.....	82
5.	Overlapping Parties.....	82
6.	Strength of Petition and Other Considerations	82
X.	CONCLUSION.....	83

TABLE OF AUTHORITIES

	Page(s)
 Cases	
<i>Amazon Web Services et al. v. Zentian Ltd.</i> , IPR2023-01194, Paper 10 (Jan. 10, 2024).....	80
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 15 (May 13, 2020).....	80, 81, 82
<i>Fintiv</i> , IPR2020-00019, Paper 11	82
<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)	81
<i>Vivid Techs., Inc. v. Am. Sci. & Eng.'g. Inc.</i> , 200 F.3d 795, 803 (Fed. Cir. 1999)	7
 Statutes	
35 U.S.C. § 102(e)	7, 9
35 U.S.C. §103	1, 3
35 U.S.C. § 314(a)	80
35 U.S.C. § 325(d)	80
 Other Authorities	
37 C.F.R. § 42.100(b)	6
https://www.uscourts.gov/statistics-reports/federal-court-management-statistics-december-2023	81

EXHIBIT LIST

No.	Exhibit Description
1501	U.S. Patent No. 8,347,484
1502	U.S. Patent No. 8,347,484 File History
1503	Declaration of Henry Houh, Ph.D
1504	CV of Henry Houh, Ph.D
1505	U.S. Patent Pub. No. 2004/0111520 to Krantz et al
1506	U.S. Patent Pub. No. 2004/0107360 to Herrmann et al
1507	IEEE Std 802.1Q-1998 – IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
1508	U.S. Patent No. 6,430,621 to Srikanth et al.
1509	U.S. Patent No. 6,032,194 to Gai et al.
1510	Cisco IOS 12.0 Switching Services (1999)
1511	Microsoft Computer Dictionary 5 th Edition (2002)
1512	Webster’s New World Computer Dictionary (2001)
1513	[Reserved]
1514	[Reserved]
1515	[Reserved]
1516	RFC 2716 – PPP EAP TLS Authentication Protocol
1517	Wireless security with 802.1x and PEAP (2003)

CLAIM LISTING

Claim No.	Claim
1.0	A network gatekeeper comprising:
1.1	at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network;
1.2	a policy auditor configured to audit the access device using the at least one security policy, in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device to the gatekeeper via a communication device; and
1.3	an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy,
1.4	the restricted subset of the protected network including the gatekeeper
2	The network gatekeeper of claim 1, wherein the network gatekeeper is communicatively coupled with a router configured to limit access to only the restricted subset using an access control list.
3	The network gatekeeper of claim 1, wherein the network gatekeeper is further configured to update the access device using an update module.
4	The network gatekeeper of claim 1, wherein the network gatekeeper is further configured to obtain system data from the access device.
5	The network gatekeeper of claim 4, wherein the network gatekeeper is further configured to use the system data to

	determine if the access device meets requirements of a security policy, and to issue commands responsive to this determination, the commands being configured to grant access to the less-restricted subset.
6	The network gatekeeper of claim 4, wherein the system data includes antivirus software version data.
11	The network gatekeeper of claim 1, wherein the at least one security policy is responsive to an identity of the access device.
12	The network gatekeeper of claim 1, wherein the at least one security policy is selected by the policy auditor responsive to a part of the less-restricted subset of the protected network to which access is requested.
13	The network gatekeeper of claim 1, wherein the audit is responsive to antivirus software executing on the access device.
15	The network gatekeeper of claim 1, wherein the policy auditor is configured to request data from an agent on the access device.
16	The network gatekeeper of claim 1, wherein the communication device includes a wireless access point.
17	The network gatekeeper of claim 1, wherein the communication device includes a wireless access point configured to support an 802.1x standard.
18	The network gatekeeper of claim 1, wherein the communication device includes a network switch.
19	The network gatekeeper of claim 1, wherein the communication device includes a router.
23	The network gatekeeper of claim 1, wherein the network gatekeeper is further configured to authenticate a user of the access device.
24	The network gatekeeper of claim 1, wherein the network gatekeeper is configured to update the access device if requirements of the security policy are not satisfied.

25	The network gatekeeper of claim 1, wherein the communication device includes a remote access virtual private network.
----	---

I. INTRODUCTION

Petitioner Cisco Systems, Inc. and Fortinet, Inc. submits this Petition for *Inter Partes* Review of claims 1–6, 11–13, 15–19, and 23–25 (the “Challenged Claims”) of U.S. Patent No. 7,523,484 (the “484 Patent” (Ex.1501)), assigned to Patent Owner, InfoExpress Inc. Petitioner respectfully submits that the Challenged Claims of the 484 Patent are unpatentable under 35 U.S.C. §103 in view of the prior art references discussed herein. Accordingly, it is respectfully requested that the Board institute an *inter partes* review of the 484 Patent.

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 484 Patent is asserted by PO 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 Information

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 484 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 484 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 484 Patent.

B. Identification of Challenged Claims

Ground 1: Claims 1-5, 11-12, 16-19, and 23-25 are unpatentable as obvious under 35 U.S.C. § 103 based on Krantz (Ex.1505).

Ground 2: Claims 1-6, 11-13, 15-19, and 23-25 are unpatentable as obvious under 35 U.S.C. § 103 based on Krantz and Herrmann (Ex.1506).

V. THE 484 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

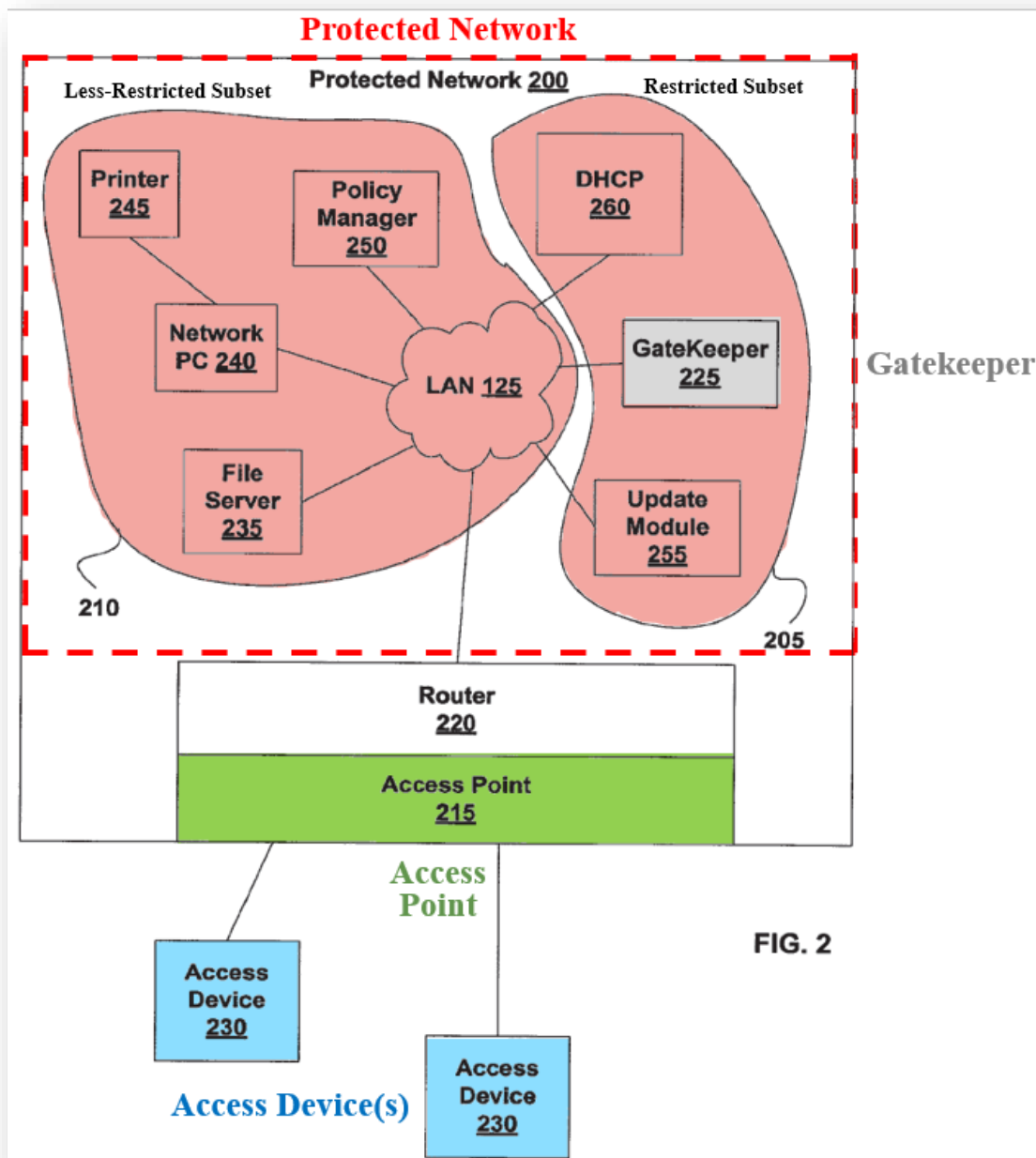
A Person of Ordinary Skill in The Art (“POSITA”) in September 2003 would have had a working knowledge of the telecommunications and networking art that is pertinent to the 484 Patent. A POSITA would have had a bachelor’s degree in computer science, computer engineering, or an equivalent, and two years 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.1503, ¶21.

C. Overview of the 484 Patent

The 484 Patent describes “a protected network physically or logically divided into a restricted subset and one or more less-restricted subsets.” Ex.1501, 2:48-50. Access to less-restricted networks from a device “are first passed to the restricted subset.” Ex.1501, 2:50-52. Elements of the “restricted subset”—such as a “gatekeeper”—“apply security policies” to the device requesting access. Ex.1501, 2:52-54. If the requesting device satisfies the “security policies,” access is then granted “to a less-restricted subset of the protected network.” Ex.1501, 2:54-56.

“[A] policy auditor [is] configured to audit an access device using at least one security policy, in response to a request to access the less-restricted subset of the protected network.” Ex.1501, 3:64-66. The 484 Patent explains “Authenticate User Step [] is considered part of the security policy audit.” Ex.1501, 11:67-12:2; *see also*, Ex.1501, 11:44-50 (giving examples of audit/system data including, operating system status, antivirus software status, information about devices connected to the Access Device, MAC address, IP address, etc.).

Figure 2 depicts embodiments of the invention described in the 484 Patent:



Ex.1501, Fig. 2 (annotated); Ex.1503, ¶36.

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).

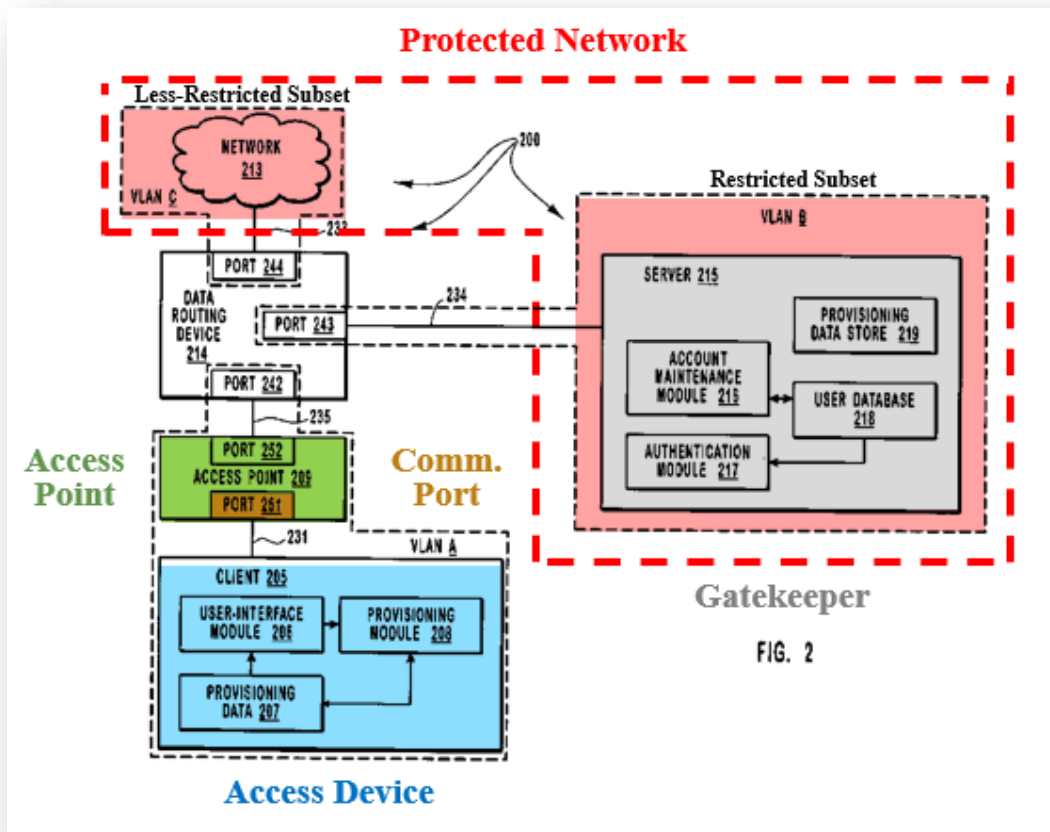
Because a POSITA would find the challenged claims unpatentable under any interpretation consistent with their plain and ordinary meaning in the context of the 484 Patent, the Board need not expressly construe the claim terms. *See Vivid Techs., Inc. v. Am. Sci. & Eng. 'g. Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

VII. PRINCIPAL PRIOR ART

A. Summary of Krantz

U.S. Patent Pub. No. 2004/0111520 to Krantz et al. (Ex.1505) was filed on December 6, 2002, and published on June 10, 2004. Krantz is prior art to the 484 Patent at least under pre-AIA 35 U.S.C. § 102(e).

Krantz describes a system in which a device attempts to access a protected network. Ex.1505, [Abstract]. To gain access, Krantz includes a server which can authorize access to the protected network resources based on credentials supplied by the device or user. Ex.1505, [0016], [0068]-[0071], [0099], [0104], [0107]-[0109]. An embodiment of this network architecture is depicted below with respect to annotated Figure 2:



Ex.1505, Fig. 2 (annotated).

Krantz utilizes Virtual Local Area Network (“VLAN”) techniques. Ex.1505, [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.1505, [0060]. Access Point 209 utilizes ports which can be configured for data transfer. Ex.1505, [0062].

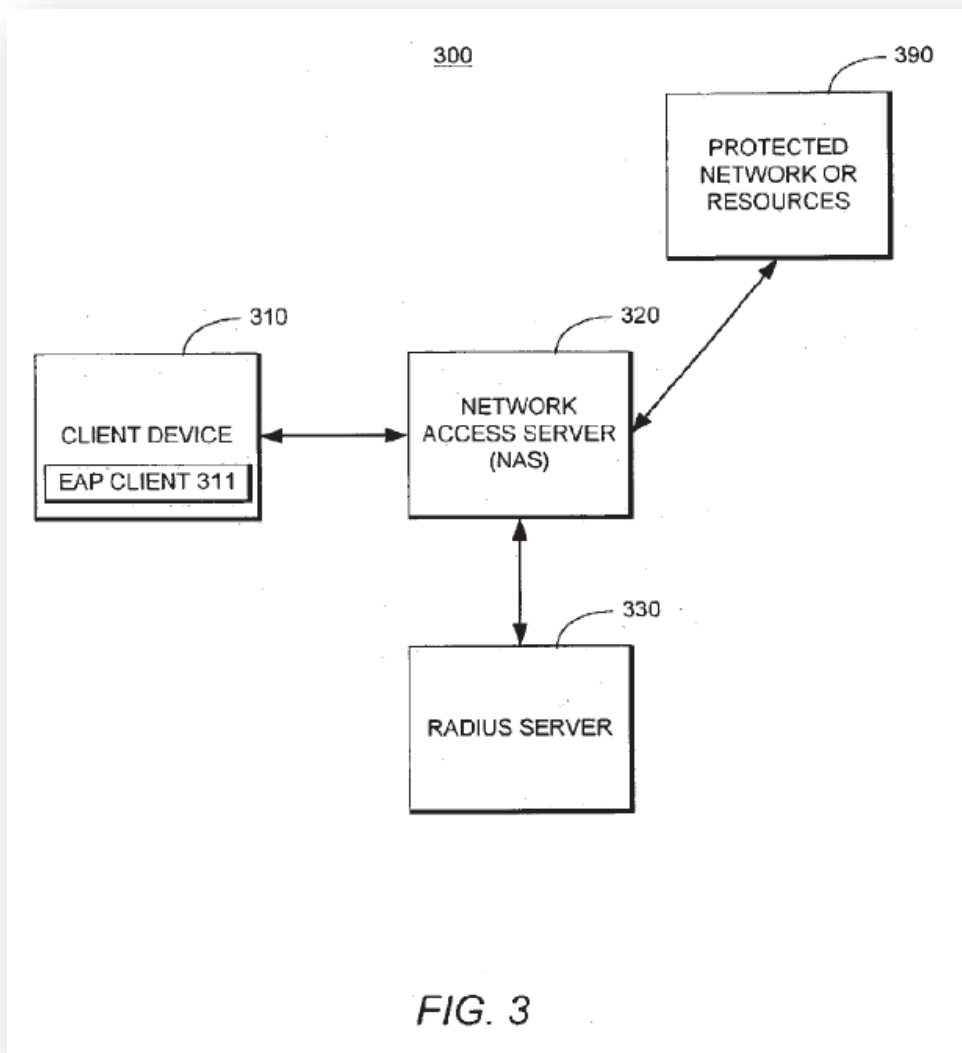
Krantz teaches a client requesting access to the network can send credentials to a server for authentication. Ex.1505, [0016]. Based upon the credentials supplied, the server “may authorize the client for at least partial access” or access to the entire network. Ex.1505, [0016], [0104], [0107]-[0109]. Authentication may be made by server 215. Ex.1505, [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.1505 [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 484 Patent at least under pre-AIA 35 U.S.C. § 102(e).

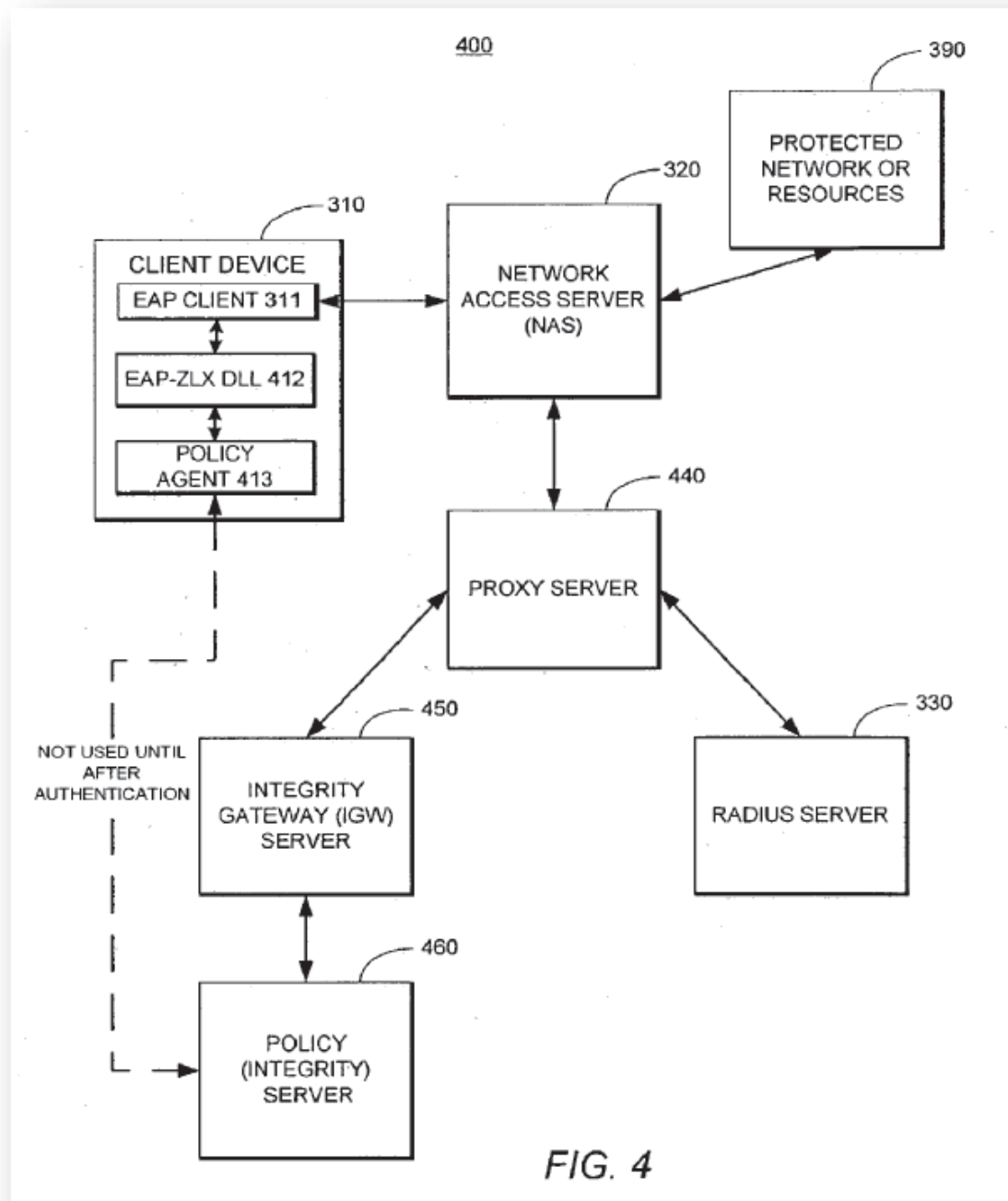
Herrmann describes enforcing security policies when providing access to a network. Herrmann explains that if a client device connected to a network . . . [and] is infected with a virus or worm, it may infect other machines on the same network. Ensuring that devices connected to the network are running current anti-virus programs is particularly important. Ex.1506 [0012].

Hermann 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.1506, [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.1505, [0018], [0053], [0063].



Ex.1506, Fig. 3.

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.1505, [0062], [0067].



Ex.1506, 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.1506, [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.1506, [0067].

C. The Combination of Krantz and Herrmann

It would have been obvious to include Herrmann’s techniques related to enforcing security policies (including checking for anti-virus protection at the client) and obtaining system data from an access device 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).**”¹ Ex.1505, [0072]. Specifically, Krantz explains that as part of its security policies, client devices are authenticated, (Ex.1505, [0067]-[0074], [0099]) and users of client devices are authenticated, Ex.1505, [0074], [0076]. Ex.1505, [0076]. Ex.1503, ¶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 already disclosed by Krantz. Ex.1505, [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

¹ Emphasis added throughout unless otherwise indicated.

security policies or rules.” Ex.1506, [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.1506, [0012]. Herrmann expressly recites that the policy server determines whether the client device 310 complies with applicable security policies. Ex.1506 [0066]. Ex.1503, ¶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 in detail below, 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 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.1506, [0068]; *see also*, Ex.1506, [0012]. 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.1506, [0066]. Thus, a POSITA would be motivated to modify the teachings of Krantz to

include in 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 to prevent viruses from infecting the protected network and to ensure network compatibility. Ex.1503, ¶53.

Krantz's server 215/authentication module, which 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. Information regarding approved antivirus software and approved connected devices could be stored in the User Database or an additional Database could be added. Ex.1503, ¶54.

The 484 Patent itself confirms that a POSITA would recognize the need for the server/authentication module of Krantz to check for up-to-date and approved antivirus programs. In the background section of the 484 Patent, it discusses GateKeeper 110 (Ex.1501, 2:14-15) and articulates 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.1501, 2:19-22. Ex.1503, ¶55.

Both Krantz and Herrmann are analogous art to the 484 Patent for at least two reasons. *First*, Krantz and Herrmann are both directed toward the same field of

endeavor of the 484 Patent—network security. Ex.1501, 1:19-20; Ex.1505, Abstract; Ex.1506, Abstract. Ex.1503, ¶56.

Second, both Krantz and Herrmann are reasonably pertinent to a problem described by the 484 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. *E.g.*, Ex.1501, 1:42-44; *see also, id.*, 1:53-56. Ex.1503, ¶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.1505, [0068]. The use of EAP-TLS (*e.g.*, Ex.1505, [0067]-[0074], [0100]) was a known authentication protocol that would be used to authenticate client devices. Ex.1516, 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.1505, [0099]. Ex.1503, ¶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.1505, [0056]. Ex.1503, ¶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 collected by the policy agent 413...” Ex.1506, [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.1506, [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.1506, [0080], [0098]. Ex.1503, ¶60.

Herrmann further 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.” Ex.1506, [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.1506, [0071]. Ex.1503, ¶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.1503, ¶62.

It would have been obvious to combine Herrmann with Krantz because a POSITA would have been motivated to do so 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.1505, [0016]. EX.1505, [0002]. Similarly, Herrmann explains that “[t]he present invention relates to ... policy enforcement on **computer systems** connected on one or more networks...” EX.1506, [0003]. Ex.1503, ¶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. *Id.*,

[0068] (“a system administrator may establish a policy requiring that **a specific virus protection program is operational on each client device** that is connected to a network. **The policy server would then evaluate whether or not each client device was in compliance** with the specified policy before approving the client device for network access.”). These are two stated goals of Krantz—added security and increased automation. EX.1505, [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 so would involve minimal changes to the existing Krantz system. Ex.1503, ¶64.

VIII. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1–5, 11, 12, 16-19 and 23-25 are Obvious Based on Krantz

Krantz teaches or suggests each claim and claim element as described below.

1. Claim 1

i. [1.0] *A network gatekeeper comprising:*

The “*network*” of the 484 Patent can include multiple networks as opposed to single network implementation. Additionally, the network disclosed in Krantz is a

“*network*”/“*protected network*”² as explained in the 484 Patent as described in detail below with respect to VLAN B and VLAN C of Krantz (depicted in Figures 2 and 4). Ex.1503, ¶66.

Krantz’s networks “can be implemented using any number of techniques, such as, for example, **Virtual Local Area Networks (“VLANs”), Internet Protocol (“IP”) filtering, [or] Virtual Private Networks (“VPNs”).**” Ex.1505, [0017]. Ex.1503, ¶67.

Krantz discloses network protocols whereby “[a] server includes the **functionality to authorize clients to access a second network**” and explains that “[b]ased on the [client] 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.1505, [0016]. Ex.1503, ¶68.

Based on Krantz, Dr. Houh confirms that a POSITA would understand that combining the first and second networks into a logical “*network*” would be done either physically or logically, although Krantz focuses on logical representations:

The actual physical representation of a communication path between two entities is not important and can

² Claim 1 of the 484 Patent claims both a “*network*” and “*protected network*.” Krantz’s “*network*” is also a “*protected network*,” as described in detail below, and given “*protected network[s]*” narrower coverage, that term is used herein.

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.1505, [0038]. Ex.1503, ¶69.

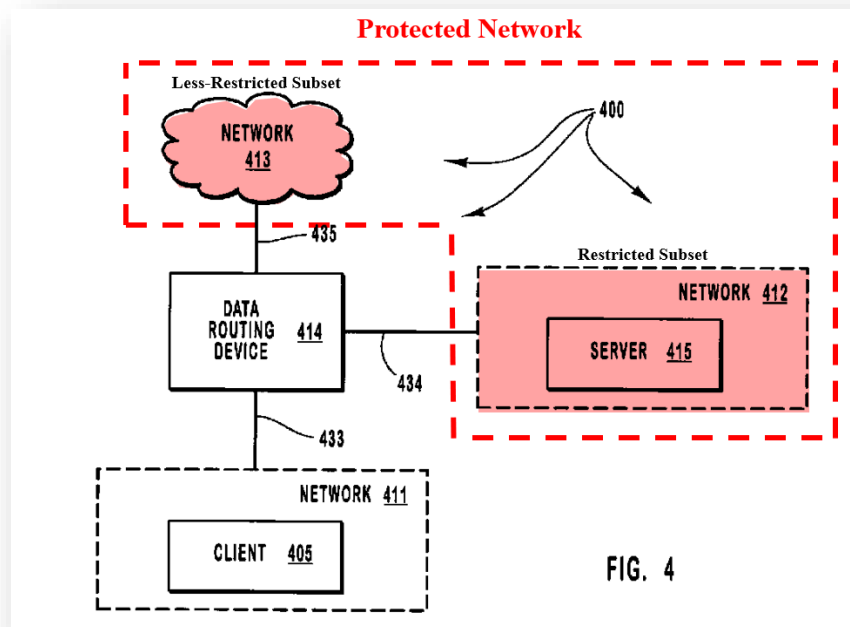
Combining multiple physical networks together was a common technique in networking at the time. Ex.1503, ¶70 (citing Ex.1511, 223, Ex.1512, 317).

Similarly, Krantz explains that “[l]ogical communication links **can include hardwired links, wireless links, or a combination**” thereof. Ex.1505, [0038].

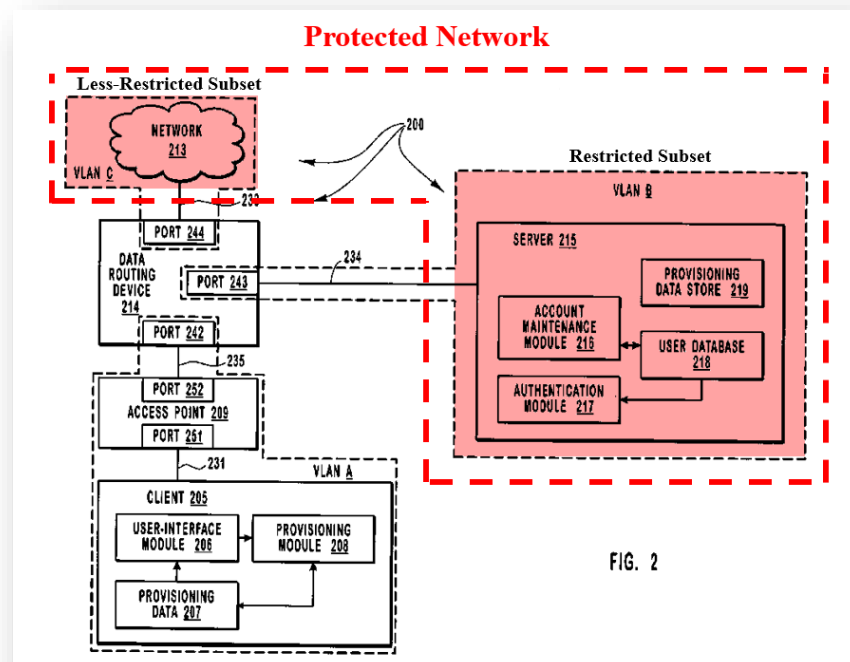
Ex.1503, ¶70.

The 484 Patent describes some of the “*protected network[s]*” characteristics—it may be “**physically or logically divided** into a restricted subset and one or more less-restricted subsets.” Ex.1501, 2:48-50. The 484 Patent also explains that such restricted and less-restricted subsets are typically “characterized by [VLANs],” (Ex.1501, 2:62-67), and further explains that the “*protected network*” may include “access restrictions.” Ex.1501, 6:21-33. Ex.1503, ¶71.

The “*protected network*” described in Krantz is depicted below.



Ex.1505, Figure 4 (annotated). Ex.1503, ¶72.



Ex.1505, Figure 2 (annotated). Ex.1503, ¶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.1505, 5:65-6:2. Krantz further explains that “in some embodiments, access to resources located in network 413 can be restricted by the use of Virtual Local Networks (“VLANs”).” Ex.1505, [0052]; *see also* [0054]. Ex.1503, ¶73.

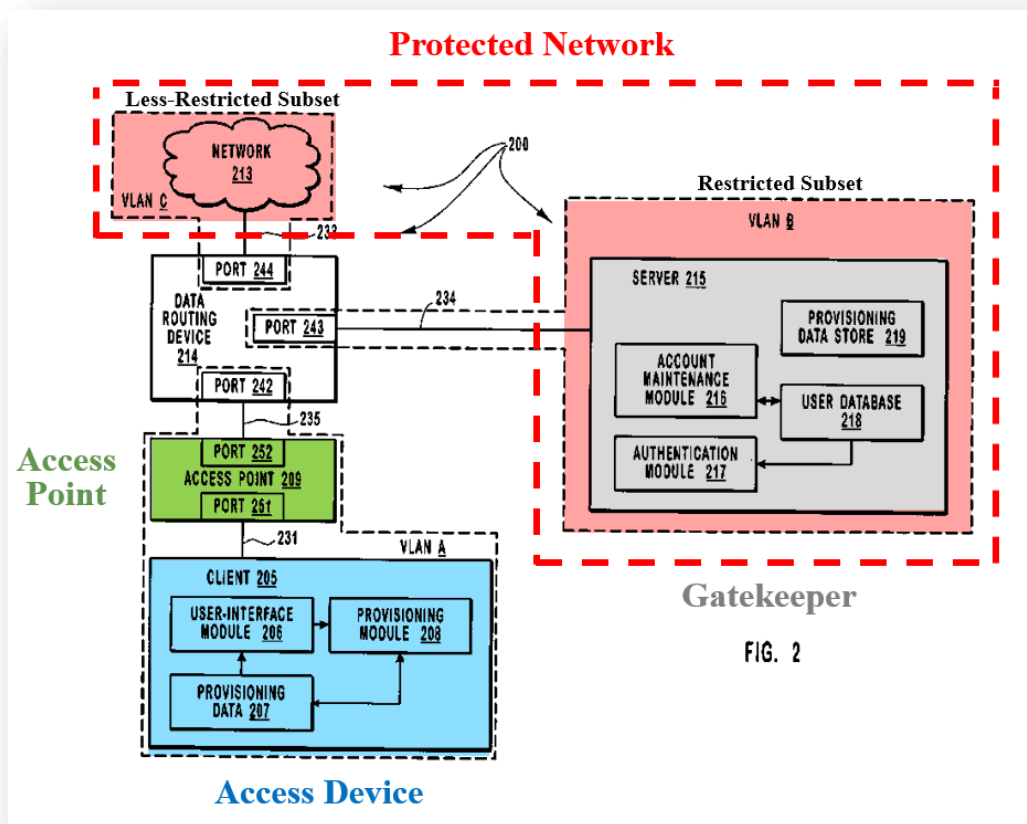
Figure 2 provides an example of such an embodiment implementing the general architecture of Figure 4 and “using VLAN techniques,” which “can facilitate increasing the level of automation when provisioning a client.” Ex.1505, [0057]. Figure 2 and its description thus provide certain specific techniques to be implemented in Krantz’s networking architecture. *See generally* Ex.1505, Figures 2 and 4 and related descriptions. Accordingly, and as depicted above, the combination of Network 413 and Network 412 (also annotated as VLAN C and VLAN B) constitute a single logical “*protected network*.³” Ex.1503, ¶73.

To the extent the “*protected network*” is required to be a single network, Krantz explains that its access control techniques can also be used “**within a single**

³ Given the similarity in disclosure between Figure 2 and the 484 Patent, the analysis will focus on Figure 2 and its corresponding description, although Figure 4 is referenced throughout.

network.” Ex.1505, [0017] (“In some embodiments, similar techniques can also be used **within a single network....**); *see also* Ex.1505, [0055]. Ex.1503, ¶74.

Krantz further discloses “a network gatekeeper”—server 215 in Figure 2. The Abstract of the 484 Patent notes that “[t]he gatekeeper⁴ is configured to enforce a security policy ... before granting access to a less-restricted subset of the computing network.” Ex.1501, Abstract. Ex.1503, ¶75.



⁴ The Gatekeeper is prior art. Ex.1501, 2:26-28.

Ex.1505, Figure 2 (annotated).

Krantz discloses that “[s]erver 215 [*‘gatekeeper’*] **may request that client 205 provide a password** that is associated with a user-identifier. A user of client 205 can respond by providing a password to server 215. **It may also be 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.1505, [0074]. Ex.1503, ¶75.

- ii. *[1.1] at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network;*

Krantz discloses several specific “*security polic[ies]*” that take place under the control of the “*gatekeeper*” and “*includ[e] requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network.*” For instance, Krantz discloses that “[d]epending on the particular EAP type, server 215 [*‘gatekeeper’*] can respond to the EAP-Response/Identity message in a variety of ways. **Server 215 may request that client 205 provide a password that is associated with a user-identifier** [(*‘at least one security policy including requirements. . . .’*)]. A user of client 205 can respond by providing a password to server 215” Ex.1505, [0074]. Ex.1503, ¶78.

Krantz discloses other examples of this claim element. For instance, “[w]hen EAP-MSChapV2 [Extensible **Authentication** Protocol] 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** [‘*at least one security policy including requirements that must be satisfied . . .*’]. Ex.1505, [0099]; *see also* exemplary XML configuration schema at [0091]; *see also* Ex.1505 [0013], [0032], [0072], [0078] (outlining other security policies that may be implemented such as requiring a user to download provisioning files for gaining access to resources). Ex.1503, ¶79.

Krantz also discloses that:

When 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.** [“*at least one security policy*”] 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)** [“*including requirements that must be satisfied*”]. If an authenticated user of client 205 [the user of the “*access device*”] is authorized to access resources located on VLAN C . . . **client 205 can then be authorized to access resources located on VLAN C** [“

before an access device is granted access to a less-restricted subset of a protected network” as discussed further below].

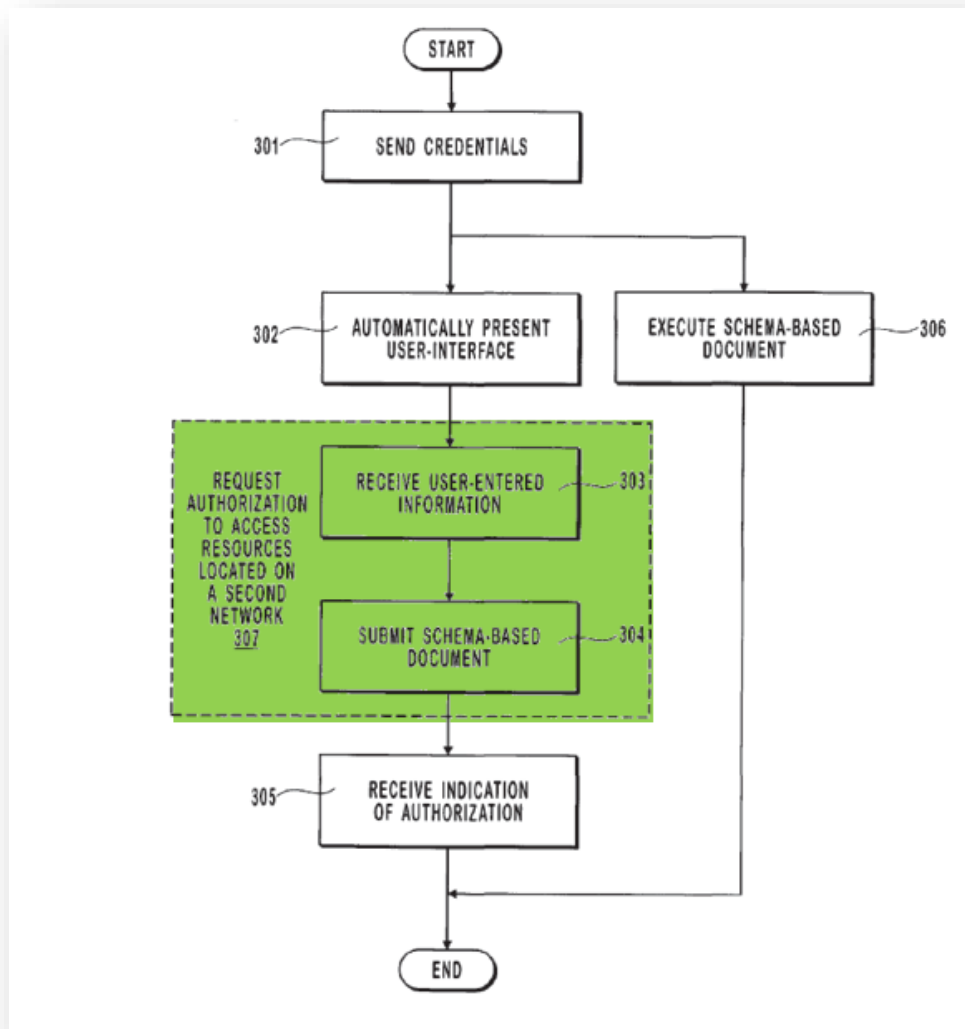
Ex.1505, [0076]; *see also* Ex.1505, [0074] (describing using EAP to authenticate user, including through exchange of “certificates, keys, and supported cipher suites.”). Krantz’s disclosure is consistent with the disclosure of the 484 Patent that describes security policies having requirements related to user identification and passwords or configuration requirements related to the access device (such as aspects of the operating system), (Ex.1501, 6:34-48), or to authenticate an access device or user. Ex.1501, 11:31-38. Ex.1503, ¶73.

For example, Krantz discloses that “a server has 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.” Ex.1505, [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.1505, [0017]; *See also* [0068]-[0076], [0099], [0104], [0107]-[0109] (collectively describing techniques for requesting access in a VLAN environment). Ex.1503, ¶81.

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.1505, [0018]. Other credentials provided by Krantz’s “*access device*” may include, for example, “user-identifier[s] and password[s].” Ex.1505, [0076]. Ex.1503, ¶82.

Krantz’s 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.1505, [0070]. Krantz discloses that “the method 300 includes a functional, result-oriented step for **requesting authorization to access resources located on a second network (step 307)**” (“*to a less-restricted subset of the protected network*”). Ex.1505, [0104]; *see also* Ex.1505, [0071] (describing the client sending credentials to server to authenticate). 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.1505, [0104]. Ex.1503, ¶83.



Ex.1505, Figure 3 (annotated). Ex.1503, ¶83.

Krantz explains that step 307 “includes [the] corresponding act of receiving user-entered information (act 303). A presented user-interface can be used to receive user-entered information (e.g., user-identifier, password, name, address, credit card information, etc.) from a user at client 205.” Ex.1505, [0104]. Ex.1503, ¶84.

The “*access device*”—Client 205—making the request to be granted access in Krantz is depicted below:

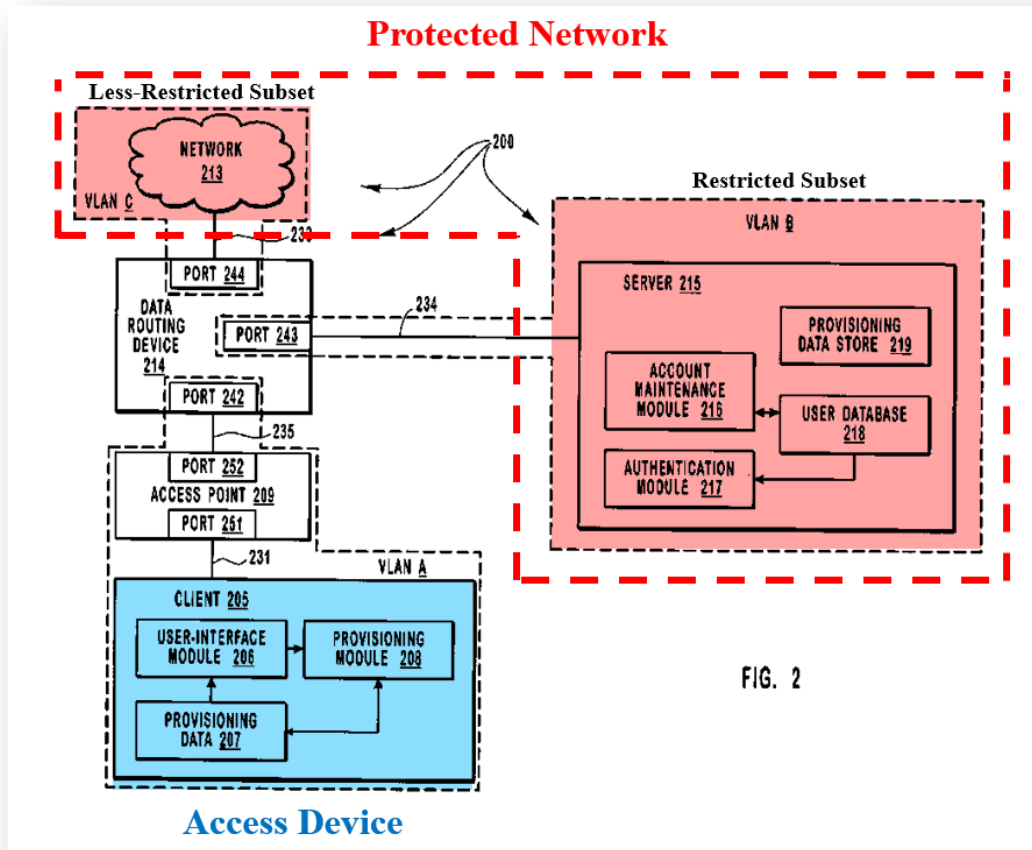


FIG. 2

Ex.1505, Figure 2 (annotated). Ex.1503, ¶85.

Moreover, as described above, *see* [1.0], the combination of VLAN C and 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]**” (“*requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network.*”)

Ex.1505, [0016]; *see also* Ex.1505, [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 [and being granted] authorization to access resources located on a second network.**” Ex.1505, [0104]. Ex.1503, ¶86.

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.1505, [0019]—precisely as the “*less-restricted subset of a protected network*” is described in the 484 Patent. Ex.1501, 5:39-41. Put another way, the “*less-restricted subset of a protected network*” as described in the 484 Patent provides greater access to elements and/or resources than the “*restricted subset*”⁵. Ex.1503, ¶87.

⁵ As described in greater detail below, the “*restricted subset*” of Krantz’s “*protected network*” is VLAN B.

- iii. *[1.2] a policy auditor configured to audit the access device using the at least one security policy, in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device to the gatekeeper via a communication device; and*
 - a. **a policy auditor...**

Krantz discloses receiving audit data from a client 205 (“*access device*”). For example, Krantz discloses that “a server has 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. Ex.1505, [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.1505, [0017]; *see also* [0074]-[0076], [0104], [0107]-[0109] (collectively describing techniques for requesting access in a VLAN environment). Ex.1503, ¶95.

Credentials supplied by the “*access device*” in the Krantz system are used to control access to the “*protected network*” resources (“*configured to audit the access device using the at least one security policy*”). Ex.1505, [0016], [0068]-[0071], [0099], [0104], [0107]-[0109]. Dr. Houh confirms this is an example of “*audit[ing] the access device*” because server 215 (“*gatekeeper*”)—and its various components including authentication module 217 (“*a policy auditor*”)—of Krantz is inspecting credentials (Ex.1505, [0016], [0071]) and can authorize access based on the inspection results (Ex.1505, [0076], [0104], [0106]-[0109]), e.g., by matching

entries in a database (Ex.1505, [0076]). The 484 Patent confirms that auditing an access device includes authenticating a user. Ex.1501, 11:67-12:2 (“In some embodiments, **Authenticate User Step 440** is considered part of the **security policy audit**”); *see also* Ex.1501, 11:31-38. Ex.1503, ¶96.

Such credentials “can include sending an Extensible Authentication Protocol (“EAP”) Response/Identity message from the client to the server.” Ex.1505, [0018]. Other “*audit*” data provided by Krantz’s “*access device*” may include, for example, “user-identifier[s] and password[s].” Ex.1505, [0076]. Ex.1503, ¶97.

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.1505, [0068]. The use of EAP-TLS (Ex.1505, [0067]-[0074], [0100]) was a known authentication protocol that would be used to authenticate client devices. Ex.1516, 1-2; *see also*, Ex.1516 [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.”). *See also* Ex.1505, [0099] (describing EAP-MSChap V2). Ex.1503, ¶98.

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.1505, [0099]. Ex.1503, ¶99.

Krantz also explains that EAP-TLS and EAP-MSCHAP V2 can both be required from a client seeking access and authorization. Ex.1505, [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 (“*using the at least one security policy.*”) before authorization is granted. *E.g.*, Ex.1517, at 2 (“EAP-TLS. TLS (SSL) is the encryption method used to protect the EAP exchange. In Windows, TLS uses certificates for machine logon and user logon. The computer first authenticates to the network using a machine certificate; this allows for computer policies in the Active Directory and SMS packages to be applied before a user logs on.”) (“In Windows, PEAP supports MS-CHAPv2 in addition to TLS. PEAP-MSCHAPv2 uses machine and user credentials

for authentication. MSCHAPv2 uses rotating keys to encrypt both machine and user password hashes. Certificates are still required for the authentication server (IAS) and are used for server-to-client authentication; credentials, carried inside MSCHAPv2, are used for client-to-server authentication.”). Ex.1503, ¶100.

Krantz explains that the credentials are audited **at the server** (“*gatekeeper*”) as:

[A]uthentication module 217 [“a policy auditor”] 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 (i.e., 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 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.1505, [0076]. Indeed, Krantz discloses that a client (“*access device*”) requesting access to the network can send credentials to a server for authentication. Ex.1505, [0016]. Based upon the credentials supplied, the server “may authorize the client for at least partial access.” Ex.1505, [0016]. This can include “at least partial access

to [a] single network, such as, for example, by authorizing client access to selected computer systems or modules on the single network.” Ex.1505, [0017]. Authentication may be made by authentication module 217 in server 215 (“*a policy auditor configured to audit the access device using the at least one security policy.*”) Ex.1505, [0073], [0076]. Ex.1503, ¶101.

b. in response to. . .

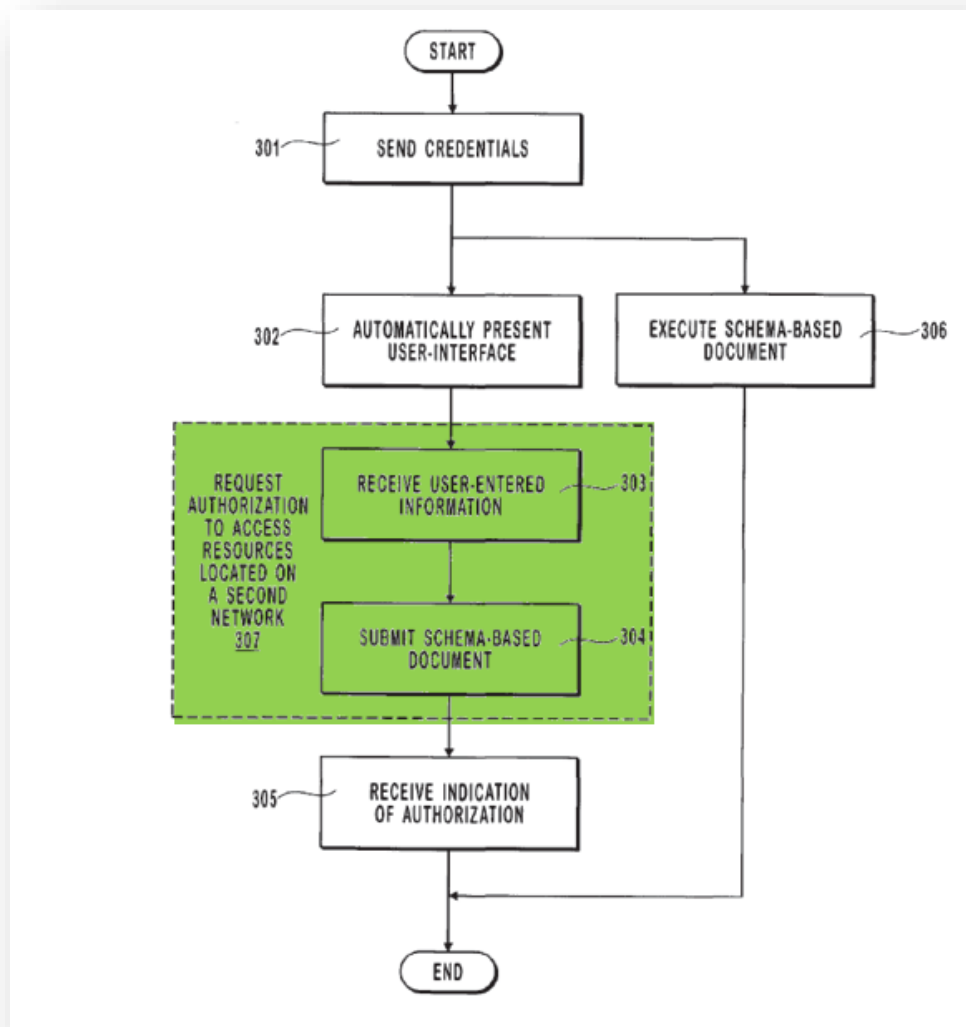
The “*access device*”—Client 205—making the request to be granted access in Krantz is depicted below. Dr. Houh explains that any “*request to access*” a less-restricted subset (VLAN C) (“*less-restricted subset of the protected network*”) from client 205 (“*access device*”) sent to the server (“*gatekeeper*”) must be received at access point 209 (“*via a communication device*”), which is annotated in green:

requesting access in a VLAN environment). 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** [(“in response to a request to access the less-restricted subset of the protected network”)].” Ex.1505, [0016]. Ex.1503, ¶105.

Such credentials “can include sending an Extensible Authentication Protocol (“EAP”) Response/Identity message from the client to the server [“gatekeeper”]. If the client is attempting to connect to a network via an access point [“via [the] communication device”], the EAP Response/Identity message may be encapsulated within some other type of message that can be transferred through the access point.” Ex.1505, [0018]. Other credentials provided by Krantz’s “access device” may include, for example, “user-identifier[s] and password[s].” Ex.1505, [0076]. Ex.1503, ¶106.

Moreover, Krantz 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.1505, [0070]. Krantz discloses that “the method 300 includes a functional, result-oriented step for **requesting authorization to access resources located on a second network (step 307)**” (“a request to access the less-restricted subset of the protected network”). Ex.1505, [0104]; see also Ex.1505, [0071] (describing the client sending

credentials to server to authenticate). 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.1505, [0104].



Ex.1505, Figure 3 (annotated). Ex.1503, ¶107.

In the example depicted in Figure 3, Krantz explains that step 307 “includes [the] corresponding act of receiving user-entered information (act 303). A presented

user-interface can be used to receive user-entered information (e.g., user-identifier, password, name, address, credit card information, etc.) from a user at client 205.”

Ex.1505, [0104]. Ex.1503, ¶108.

- iv. *[1.3] an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy,*

- a. **...if the audit results. . .**

Krantz discloses that “access point 209” (“*the communication device*”) 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.1505, [0064]. Ex.1503, ¶112.

As explained in Krantz and above, *see* Claim [1.2.i], **“if an authenticated user of client 205 is authorized to access resources located on VLAN C [“ . . . if the audit results in a determination that the access device meets the requirements of the at least one security policy”] . . . client 205 can then be authorized to access resources located on VLAN C.”** Ex.1505, [0076]. As also explained above, *see* Claim [1.2.i], Krantz discloses utilizing other security policies including the use of user-identifiers and passwords. Ex.1505, [0076] (“[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.1503, ¶113.

b. **an access control configured...**

Krantz explains that after the client is audited (“*if the audit results in a determination that the access device meets the requirements of the at least one security policy,*”) see claim [1.2]-[1.3i], “client 205 can then be authorized to access resources located on VLAN C” (“*an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network.*”) Ex.1505, [0076]; see also Ex.1505, [0031]. Ex.1503, ¶115.

Krantz discloses how “server 215 [“*gatekeeper*”] logically represents a Remote Authentication Dial-In User Service (‘RADIUS’) server. That is, although visually depicted by a single system, server 215 may include a separate Network Access Server (‘NAS’), a separate authentication server, and a separate shared accounting server.” Ex.1505, [0058]. Krantz explains that “[t]he servers logically represented by server 215 can be configured to communicate using the RADIUS protocol and, more specifically, may support the RADIUS attributes EAP-Message and Message-Authenticator. **Server 215 may have modules from a variety of different services loaded into system memory**, such as, for example, Internet

Information Services (“IIS”) modules, Internet Authentication Services (“IAS”) modules, Dynamic Host Control Protocol (“DHCP”) modules, and Active Directory (“AD”) modules, **so as to facilitate implementation of the principles of the present invention** (“*access control configured to . . .*”). Ex.1505, [0058]. For example, Krantz explains that “[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. **Server 215 (and/or its authentication modules) can send commands** [*“an access control”*] **to access point 209** [*“the communication device”*] **to cause access point 209 to enable protocols and cause access point 209 to insert appropriate Tag Headers** [*“configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network.”*]. Ex.1505, [0107]. Ex.1503, ¶116.

Krantz discloses the functionality in several ways. Ex.1503, ¶117.

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]⁶ 209 and client 205 through port 251. Likewise, data can be transferred between access point 209 and data routing device 214 through port 252.”** Ex.1505, at [0063]. In other words, Krantz is disclosing it “*reconfigure[s] the communication device*” in order to transfer “*data sent from the access device.*” Ex.1503, ¶118.

Krantz further discloses that “access point 209” (“*the communication device*”) 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.1505, [0064]. Access Point 209 is the communication path between the “*device*” and a **VLAN B**—the restricted subset of the protected network—is depicted below:

⁶ Typo in original. “Access port 209” should refer to “Access **Point** 209.”

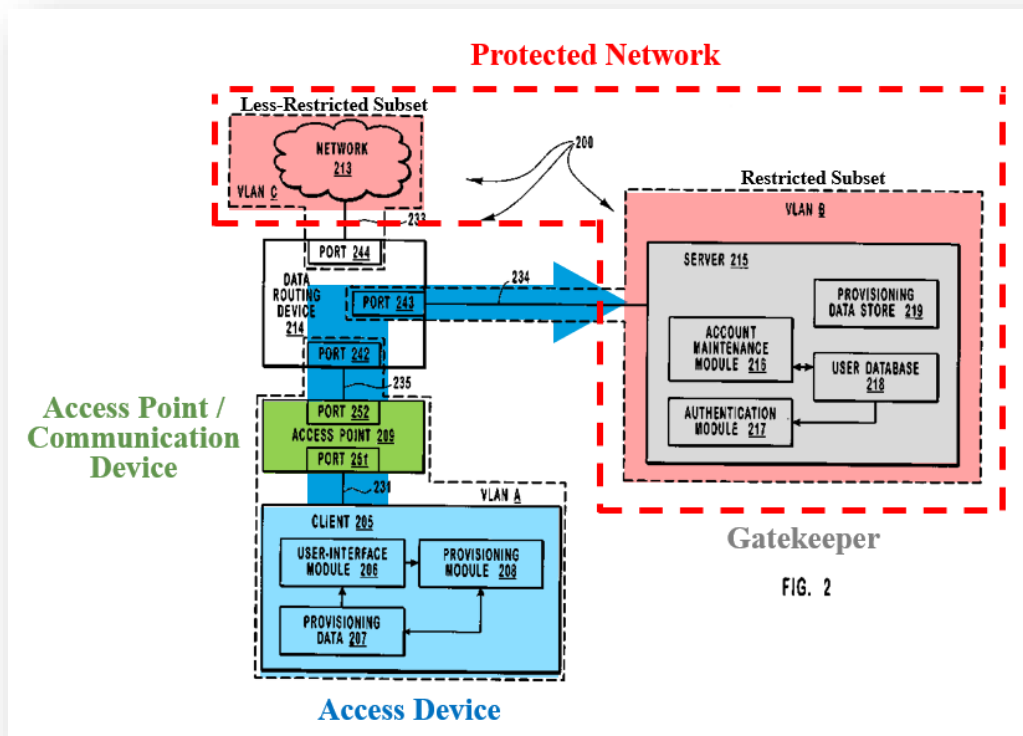
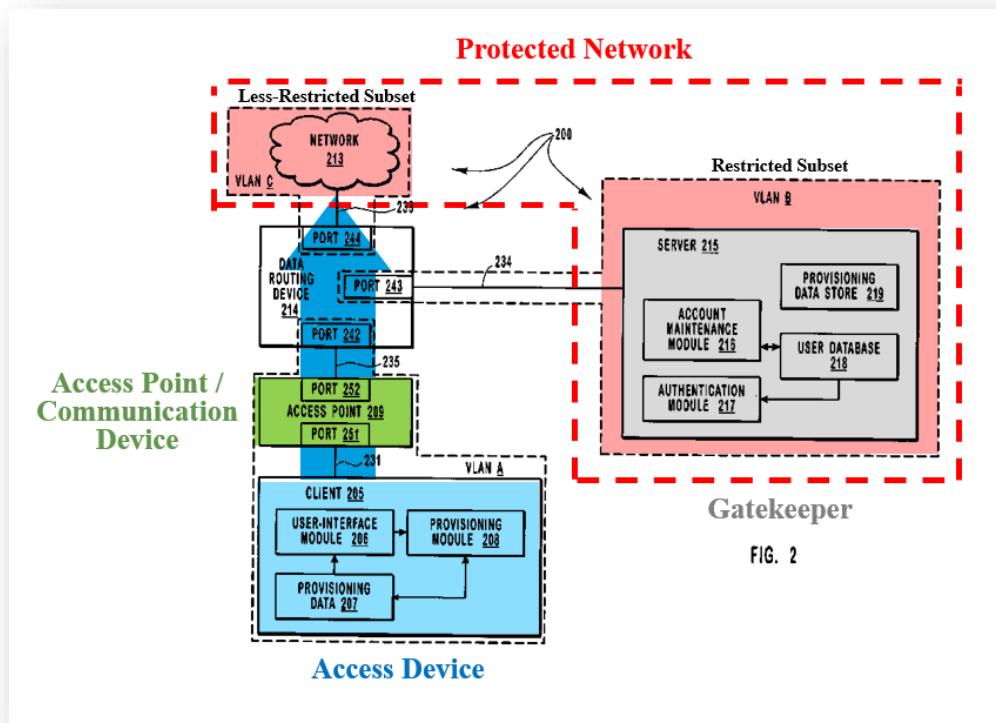


FIG. 2

Ex.1505, Figure 2 (annotated). Ex.1503, ¶119.

In Krantz, access point 209 is initially configured to allow access only to VLAN B—the restricted subset of the protected “*network*.” Access point 209, including “port 251” can be “*reconfigur[ed]*” in a way “*such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network*” because it facilitates the transfer of data between client 205 (“*the access device*”) and ultimately VLAN C (the “*less-restricted subset of the network*.”) as depicted below. Ex.1505, at [0063]-[0064], Access point 209 does so “*if the audit results in a determination that the access device meets the requirements of the at least one security policy.*” As

explained, Krantz describes that “[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. **Server 215 (and/or its authentication modules) can send commands** [*“an access control”*] **to access point 209** [*“the communication device”*] **to cause access point 209 to enable protocols and cause access point 209 to insert appropriate Tag Headers** [*“configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network.”*]. Ex.1505, [0107]. Ex.1503, ¶120.



Ex.1505, Figure 2 (annotated). Ex.1503, ¶120.

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.1505, at [0064]. Access Point 209 is initially configured to insert Tag Headers into data frames destined for VLAN B. Ex.1505, [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.1503, ¶121.

Configuring ports in VLAN aware devices to tag incoming data was a well-known technique to POSITAs by 2003, as Dr. Houh confirms. Ex.1507, 11 Table 5-1 (explaining, for example, 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.”); Ex.1508, 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.1509, 16:4-13; Ex.1510, p.210. Ex.1503, ¶122.

As Krantz also 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.1505, [0023]. Ex.1503, ¶123.

Krantz is therefore explaining that when configured as a “VLAN aware device,” Krantz’s “*communication device*” is “*reconfigur[ed]*” by “*an access control configured*” to do such reconfiguration such that “*data*” from the “*access device*” is “*is received by the less-restricted subset of the protected network rather than merely*

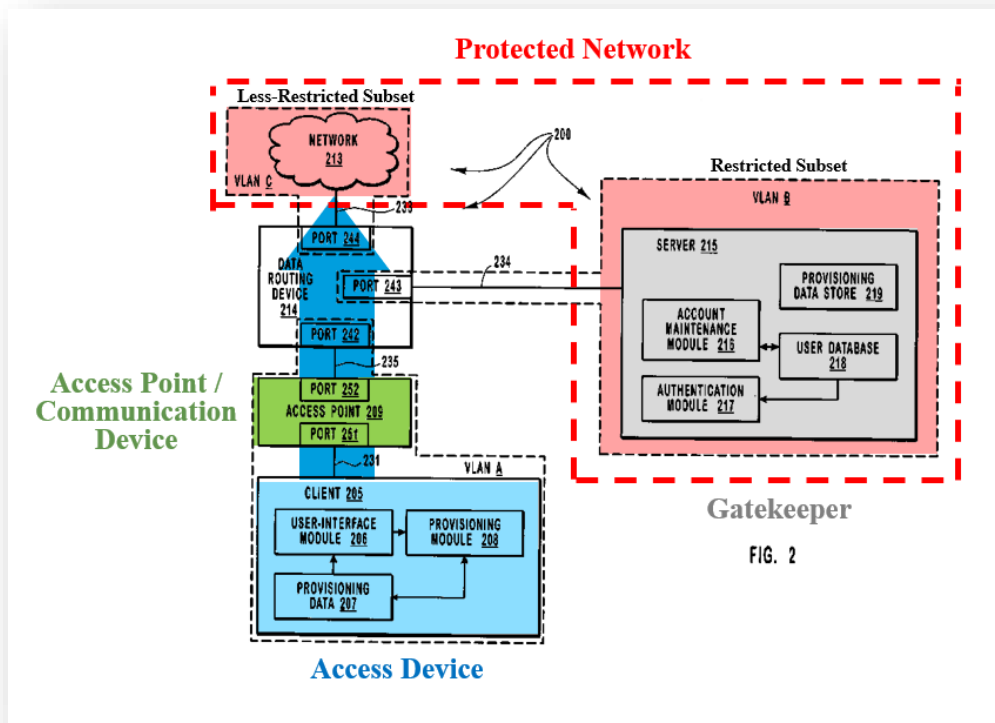
a restricted subset of the protected network” because Access Point 209 (via Port 251) will insert VLAN Tag Headers into incoming data frames from a client **that may now access VLAN C** (*“less-restricted subset.”*) Ex.1505, [0107]. Port 251 is *“reconfigur[ed]”* by Access Point 209 because it was previously 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 *“the communication device”* is *“reconfigur[ed]”* because Port 251 tags incoming data for transfer to VLAN C rather than VLAN B. Ex.1503, ¶124.

In particular, Krantz discloses “[w]hen client 205 is authorized to access resources located on VLAN C, **access point 209 may enable 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 of the protected network”*]. **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.1505, [0107]. Ex.1503, ¶125.

Lastly, this reconfiguration is *“if the audit results in a determination that the access device meets the requirements of the at least one security policy.”* 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.1505, [0017]. As explained in Krantz, credentials are audited at the server as

“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 (i.e., **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 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.1505, [0076]. In addition, this “*security policy*” is applied in response to the client requesting access to resources on VLAN C. Ex.1505, [0016-0018], [0071]-[0072], [0076], [0104]-[0109]. Ex.1503, ¶126.

Thus, Access Point 209—“*if the audit results in a determination that the access device meets the requirements of the at least one security policy*”—facilitates the transfer of data between client 205 (“*the access device*”) and, ultimately VLAN C (“*the less-restricted subset of the protected network.*”). Ex.1505, [0063]-[0064]. It does so based on commands from the “*gatekeeper.*” Ex.1505, [0107]. Access Point 209 is “*reconfigur[ed]*” because it did not previously permit client 205 access to “*the less-restricted subset of the protected network.*” The “*reconfigured*” communication path is shown below:

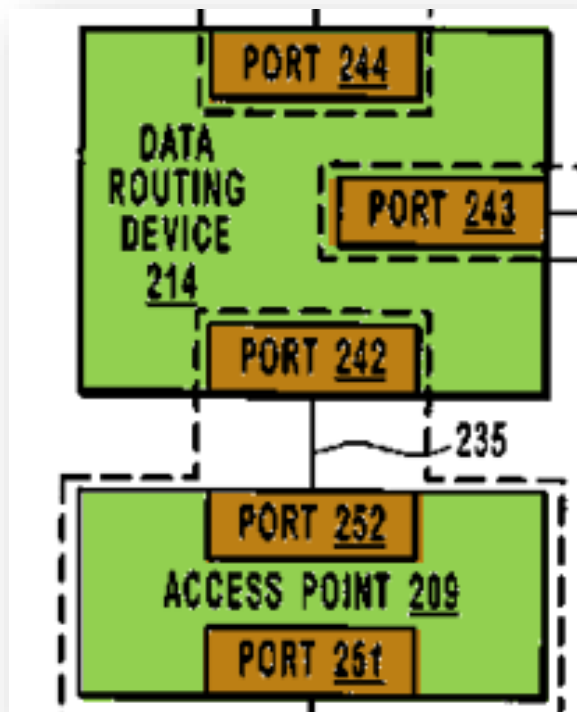


Ex.1505, (annotated). Ex.1503, ¶127.

Mapping #3

To the extent one may assert that Krantz does not expressly disclose this claim element, it would have been obvious to implement other “*reconfiguring*” techniques in view of Krantz itself. Ex.1503, ¶129.

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.1505, [0060]. Ex.1503, ¶130.



Ex.1505, Figure 2 (annotated).

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.1505, [0061]. Ex.1503, ¶131.

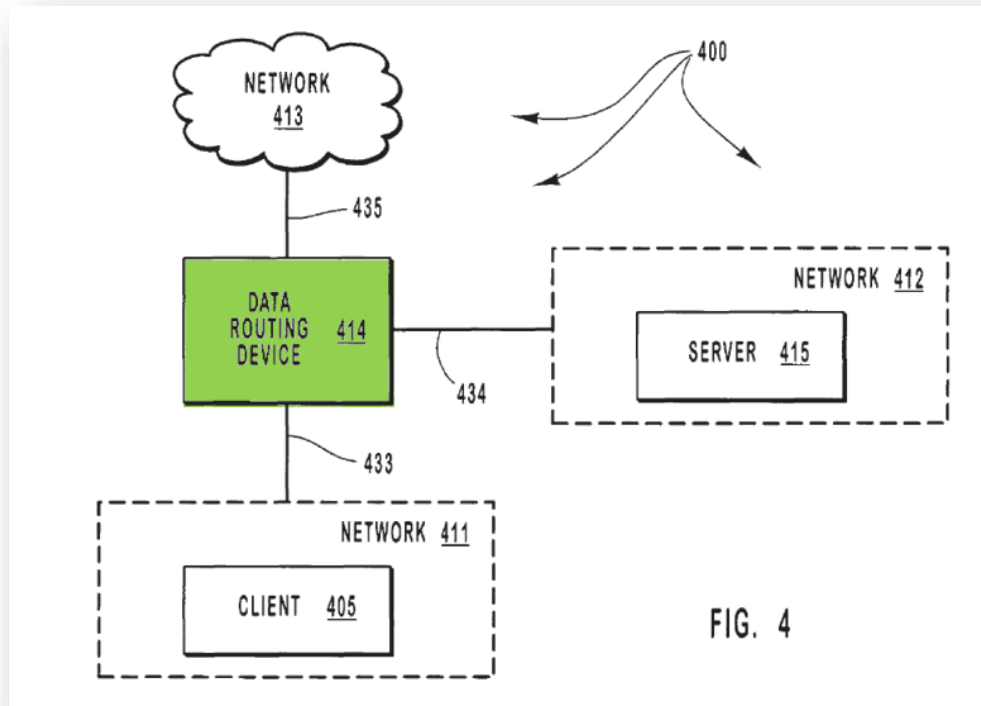
For example, Krantz states that “[n]etwork architecture 200 also includes data routing device 214. **Data routing device 214** logically represents a special-purpose computer system, such as, for example, **a router and/or a switch, that can**

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.1505, [0059]; *see also* Ex.1505, [0060] (“Thus, data routing device 214 can be configured to separate computer systems into different VLANs.); *see also generally*, Ex.1505, [0064]. Ex.1503, ¶132.

Dr. Houh explains that it 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.1505, [0059]. 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.1503, ¶133.

In fact, Krantz already contemplates combining the functionality of the “access point” and “data routing device” in a single physical or logical representation. For example, Figure 4 of Krantz demonstrates that such functionality

can be readily combined with the data routing device as the access point. Ex.1503, ¶134.



In particular, Krantz explains that:

Data routing device 414 logically represents a computer system that can determine where to transfer data received from network 411, such as, for example, data received from client 405. That is, 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.1505, [0051]. Ex.1503, ¶135.

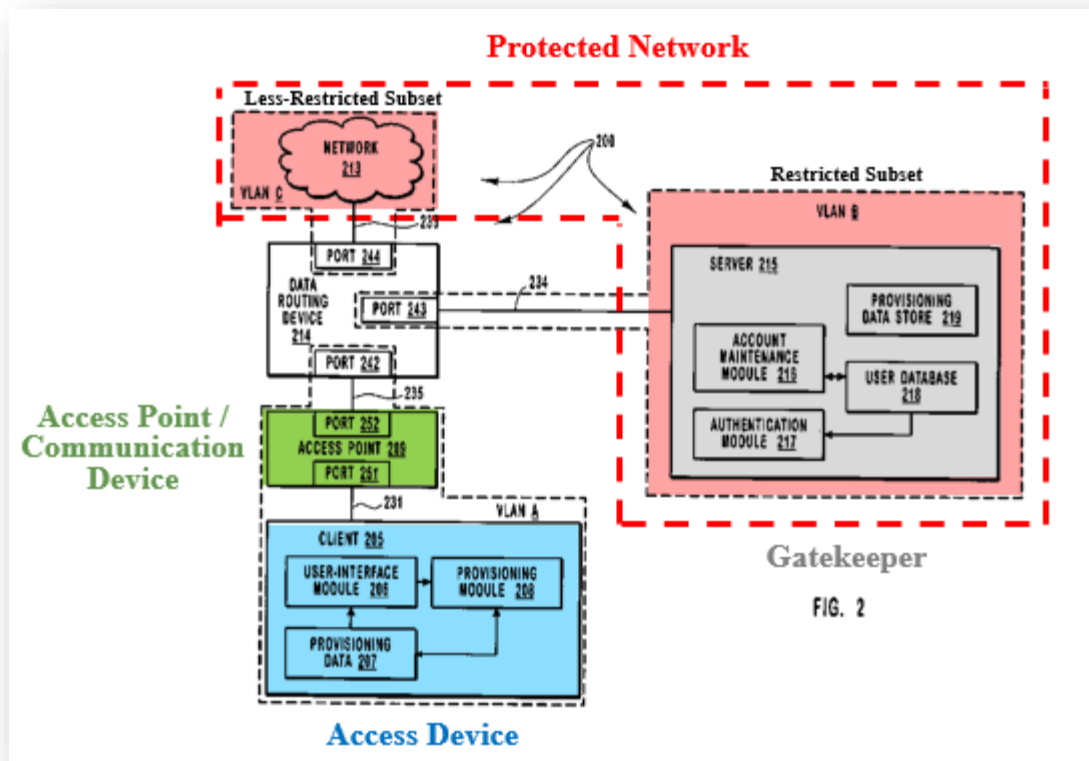
Indeed, with respect to the disclosures in Figure 2, Krantz expressly discloses that “Data routing device 214 **logically represents** a special-purpose computer system, such as, for example, a router and/or a switch, that can determine how to transfer data between the ports included in data routing device 214,” Ex.1505, [0059] so a POSITA would understand in view of that disclosure that such a “logical” architecture could readily be implemented in a single device such as an access point. 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.1505, [0059]. In fact, Krantz repeatedly describes the “data routing” device and “access point” device as having the same functionality. *Compare, e.g.,* Ex.1505, [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, it is clear that the functionality 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 described in Krantz. Using one technique or the other would merely have been a matter of design choice. Ex.1503, ¶136.

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.1503, ¶137.

**v. *[1.4] the restricted subset of the protected network
including the gatekeeper***

As explained above for claim [1.1], Krantz includes server 215 (“*gatekeeper*”) depicted below as part of VLAN B (“*the restricted subset of the protected network including the gatekeeper.*”) Ex.1503, ¶141.

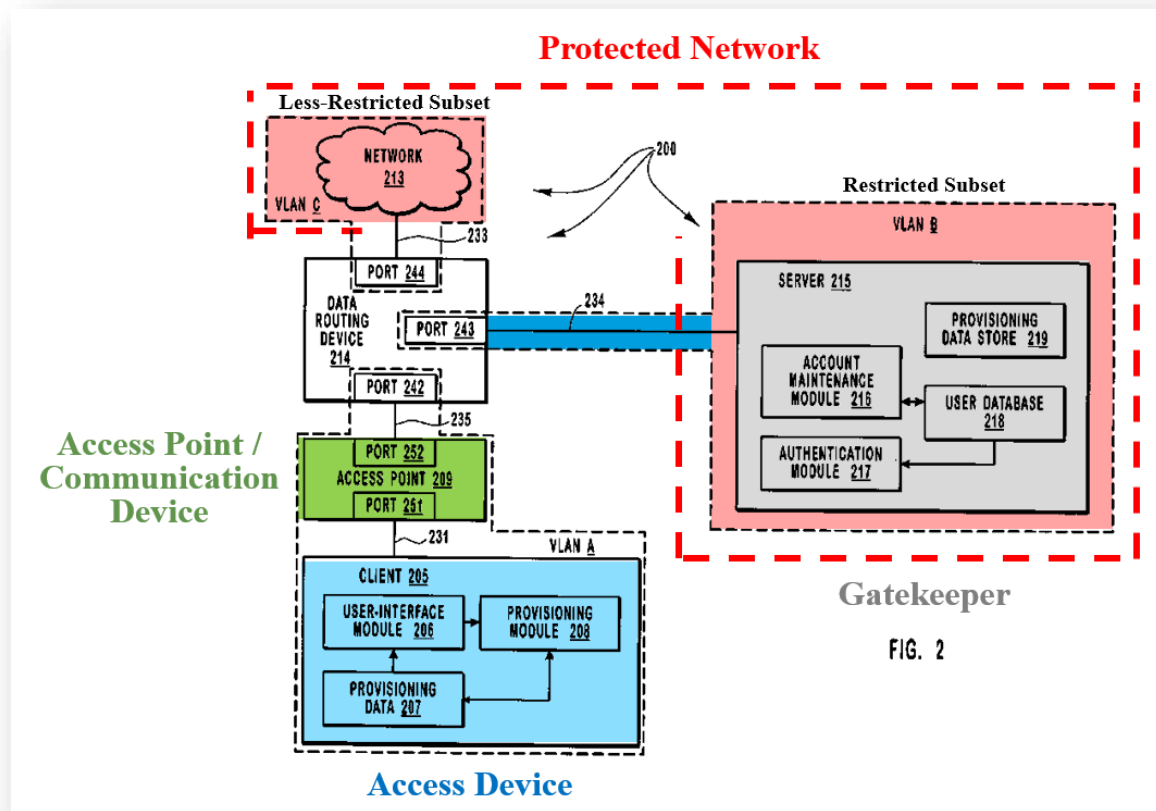


Ex.1505, Figure 2 (annotated). Ex.1503, ¶141.

2. Claim 2

First, the “*network gatekeeper*” of Krantz is “*communicatively coupled with a router [data routing device 214]*” via logical communication link 234 and 235.

Ex.1505, Fig. 2 (below), [0060]. Ex.1503, ¶¶144-145.



The 484 Patent explains that “access control lists within Router 220 are optionally used to independently **control access to specific devices** within Less-Restricted Subset 210.” Ex. 1501, 6:24-27. Ex.1503, ¶146.

Krantz discloses how a “router [is] configured to limit the access to only the restricted subset using an access control list.” As discussed above—see Claim [1.3] (Mapping #3)—Krantz explains that “access to resources located on network 413 can be restricted by the use of Internet Protocol (“IP”) filtering. **Data 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.1505, [0053]. In other words, the access point in conjunction with the data routing device can be “*configure[ed]*” based on what the client is authorized to access. Ex.1505, [0064]; *see also*, Ex.1505, [0023] (“[T]he access point may insert Tag Headers into client data to indicate to the **data routing device** [*‘a router configure[ed]’*] that client data is to be transferred to the second network.”). Ex.1503, ¶147-148.

A POSITA would understand that the “*reconfiguring*” step in claim [1.3] could utilize the database or list of clients to filter as disclosed in Krantz (“*a router configured to limit the access to only the restricted subset using an access control list*”). Krantz explains that “[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. **When client 405 is authorized to access network 413, IP addresses can be filtered** such that client 405 is exposed to IP addresses of resources located on both networks 412 and 413. Alternately, **when client 405 is authorized to access network 413 IP filtering may cease altogether.**” Ex.1505, [0053]. In other words, if the client or “*access device*” is on an authorized list (“*access control list*”) it is permitted access and no filtering takes place (i.e., it is part of the “*access control list*” of devices permitted to access resources). Dr. Houh explains that limiting access to server resources for specific clients through IP

filtering is a form of an “*access control list*” because that in essence “controls access to specific devices.” Ex. 1501, 6:24-27. Ex.1503, ¶149.

Moreover, a POSITA would have similarly found it obvious to use an “*access control list*” in a VLAN embodiment because such an embodiment has client access control considerations. Ex.1505, [0052]. Ex.1503, ¶150.

Krantz describes additional techniques where such an “*access control list*” is utilized. In Krantz, a database is utilized as follows: “[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** (i.e., server 215 believes that the user represented by the user-identifier is the user who entered the credential information).” See, Ex.1505, [0076]. Moreover, Dr. Houh confirms that device information (such as IP addresses) could just as easily be stored in a database as users/usernames as Krantz specifically discusses filtering IP addresses. Ex.1505, [0053]. Ex.1503, ¶151.

3. Claim 3 - *wherein the network gatekeeper is further configured to update the access device using an update module.*

Krantz explains that “the server can authorize limited access. . . such that the **client can download provisioning files** [from the “*the network gatekeeper*”] for gaining full access resources located on the second network. Ex.1505, [0032]; see

also Ex.1505, [0056] (“Client 405 can be authorized to download provisioning files from these computer systems or modules [*“is further configured to update the access device using an update module”*], while being denied access to other resources located on network 413.”). Ex.1503, ¶¶154-155.

Krantz also describes “**provisioning module 208** can execute an XML document, defined in accordance with an XML configuration schema, **to appropriately configure client 205 for accessing resources located on VLAN C** [*“update the access device.”*]. **Provisioning module 208** can retrieve previously downloaded XML documents, such as, for example, a configuration sub-file, from provisioning data 207,” Ex.1505, [0110], in concert with Provisioning Data Store 219 [*“network gatekeeper . . . using an update module”*]. Ex.1505, Figure 2, [0085]. Ex.1503, ¶156.

4. Claim 4 - *wherein the network gatekeeper is further configured to obtain system data from the access device.*

Krantz explains that EAP-TLS and EAP-MSCHAP V2 can both be required from a client seeking access and authorization from Server 215 [*“network gatekeeper”*]. Ex.1505, [0099]. And Krantz 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** [*“configured to obtain system data from the access device”*] **should be used for authentication.**” Ex.1505, [0099]. Ex.1503, ¶¶163-164.

5. **Claim 5 - wherein the network gatekeeper is further configured to use the system data to determine if the access device meets requirements of a security policy, and to issue commands responsive to this determination, the commands being configured to grant access to the less-restricted subset.**

See Claims 1 and 4, *above* (describing server 215 (“*network gatekeeper*”) using operating system credentials (“*system data*”) to authenticate a user pursuant to a security policy). Ex.1503, ¶164. Krantz also explains that “[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** [*“and to issue commands responsive to this determination”*] **to access point 209 to cause access point 209 to enable protocols and cause access point 209 to insert appropriate Tag Headers** [*“the commands being configured to grant access to the less-restricted subset.”*]. Ex.1503, ¶¶170-171; *see also* Ex.1503, ¶¶111-139.

6. **Claim 11 - wherein the at least one security policy is responsive to an identity of the access device.**

Krantz explains that “[c]lient 205 can respond to the EAP-Request/Identity message with an EAP-Response/Identity message **that can include a User-Identifier**. If a user of client 205 has an account with server 215 this User-Identifier may be a User-Identifier that was assigned to the user by server 215 [*“at least one*

security policy is responsive to an identity of the access device.”].” Ex.1505, [0071].
Ex.1503, ¶¶178-179.

7. Claim 12 - wherein the at least one security policy is selected by the policy auditor responsive to a part of the less-restricted subset of the protected network to which access is requested.

See Claim 3, above.

Krantz explains that “[w]hen full access to resources located on the **second network is not authorized** [*“responsive to a part of the less-restricted subset of the protected network to which access is requested”*], 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 resources located on the second network.** Ex.1505, [0032]; *see also* Ex.1505, Figure 2, [0056], [0085], [0110].
Ex.1505, ¶¶183-185.

Krantz is thus describing that its system is “*responsive to*” the needs for certain provisional files to be installed as part of a “*security policy [that] is selected by the policy auditor*” for access. Ex.1503, ¶186.

8. Claim 16 - wherein the communication device includes a wireless access point.

Krantz explains that “**Access point 209 can be a wired or wireless access point** that facilitates communication between client 205 and data routing device 214.” Ex.1505, [0059]; *see also* Ex.1505, [0064]. Ex.1503, ¶¶206-208.

9. **Claim 17 - *wherein the communication device includes a wireless access point configured to support an 802.1x standard.***

Krantz explains that “[o]ne protocol used for encapsulation is the **802.1x protocol, which may be referred to as EAP encapsulation over LANs (‘EAPOL’)**. Access point 209 and data routing device 214 **can be configured to support EAPOL.**” Ex.1505, [0069]; *see also* Ex.1505, [0072]. Ex.1503, ¶¶209-211.

10. **Claim 18 - *wherein the communication device includes a network switch* and Claim 19 - *wherein the communication device includes a router.***

The combination of Access Point 209 and Data Routing Device 214 (“*access point*”) described above, *see* Claim [1.3] (**Mapping #3**)—Krantz explains that “Data routing device 214 logically represents a special-purpose computer system, such as, for example, **a router and/or a switch.**” Ex.1505, [0059]. Ex.1503, ¶¶212-214, 215-217.

11. **Claim 23 - *wherein the network gatekeeper is further configured to authenticate 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** (i.e.,

server 215 believes that the user represented by the user-identifier is the user who entered the credential information).” Ex.1505, [0076]; *see also* Ex.1505, [0074] (describing using EAP to authenticate user, including through exchange of “certificates, keys, and supported cipher suites.”). Ex.1503, ¶¶218-220.

12. Claim 24 - *wherein the network gatekeeper is configured to update the access device if 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 resources located on the second network.**” [*“network gatekeeper is configured to update the access device if requirements of the security policy are not satisfied”*]. Ex.1505, [0032]; *see also* Ex.1505, [0056], [0110]. Ex.1503, ¶¶221-223.

13. Claim 25 - *wherein the communication device includes a remote access virtual private network.*

Krantz’s networks “can be implemented using any number of techniques, such as. . . **Virtual Private Networks (“VPNs”).**” Ex.1505, [0017]. Krantz does not expressly disclose that its “*access point*” could comprise a “*remote access virtual private network,*” but it would have been obvious to implement that functionality in view of Krantz itself. Ex.1503, ¶¶231-232.

Krantz recognizes the importance of security and access-control techniques, Ex.1505, [0055], and a VPN was a well-known technique for preventing unauthorized access. Ex.1512, 4; Ex.1513, 3. Dr. Houh therefore explains that 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.1505, [0017], [0032], [0038], [0054]. Ex.1503, ¶¶232-233.

B. Ground 2: Claims 1–6, 11–13, 15–19, and 23–25 are Obvious Based on Krantz and Herrmann

Krantz teaches or suggests each element of claims 1–5, 11, 12, 16-19 and 23-25. *See* §VIII.A. To the extent one asserts that Krantz does not teach or suggest certain of the claim elements described below, those elements would have been obvious based on the teachings of Krantz and Herrmann, and a POSITA would have been motivated to combine Krantz and Herrmann for the reasons demonstrated above in §VII.C, and for the additional reasons described below. Accordingly, Krantz/Herrmann render obvious every element of claims 1–6, 11–13, 15–19, 23–25 as demonstrated below.

1. Claim 1

i. [1.1]-[1.3]

To the extent one asserts that Krantz does not disclose “*at least one security policy including requirements that must be satisfied,*” Krantz/Herrmann describe a

security policy requiring antivirus software be installed on the network device, as in Herrmann. Herrmann specifically discloses that “[I]t becomes critical, therefore, **to promptly update anti-virus applications on all machines in a network.**” Ex.1506, [0012]. Ex.1503, ¶88.

Herrmann explains 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.1506, [0071]. This may be implemented using security rules and **checking system data for connecting devices to ascertain compliance.** Ex.1506, [0068]. Ex.1503, ¶89.

A POSITA would have been motivated to combine Krantz with Herrmann for the reasons described above. *See* §VII.C. A POSITA would recognize that checking for antivirus software based on a security policy would merely be an additional item for server 215 (“*gatekeeper*”) and its components (e.g., authentication module 217) to check in the authentication process already disclosed by Krantz. Like Krantz, Herrmann discloses that a “policy server 460 may enforce a variety of different types of security policies or rules,” Ex.1506, [0068], including “a policy requiring that a **specific virus protection program** is operational on each client device that is connected to a network.” Ex.1506, [0012]. Moreover, a POSITA would be motivated to modify the system of Krantz to include the additional “*security policy*” requiring a specific virus protection program (“*including requirements that must be*

satisfied”) because Krantz is specifically focused on network authentication and security. Ex.1505, [0019]. Ex.1503, ¶90.

2. **Claim 3 - wherein the network gatekeeper is further configured to update the access device using an update module.**

Krantz explains 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.1505, [0013]. Ex.1503, ¶157.

Krantz also discloses how a connecting device may be required to have “provisioning files [] for gaining full access to network 413.” Ex.1505, [0056]; *see also*, Ex.1505, [0032], [0078]. Dr. Houh confirms provisioning files generally relate to network connectivity and security. Ex.1509, [0079]. Ex.1503, ¶158.

Herrmann discloses that “[i]t 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.1506, [0012]. Ex.1503, ¶159.

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.1506, [0071] (“*wherein the network gatekeeper is further configured to update the access device using an update*

module”). This may be implemented using security rules and checking system data for connecting devices to ascertain compliance. Ex.1506, [0068]. Ex.1503, ¶160.

A POSITA would be motivated to modify Krantz to include the additional policy requiring a specific virus protection program be updated for the reasons demonstrated above. See VII.C & Claim [1]/[Ground 2]. 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.1505, [0019]. Requiring the client to update antivirus software would merely be an additional condition, which a POSITA would understand the importance of as confirmed by the 484 Patent itself. Moreover, because prior art GateKeepers were known to control security policies (Ex.1501, 2:26-42), a POSITA would find that the gatekeeper of Krantz with Herrmann’s teachings renders obvious that the “*gatekeeper is further configured to update the access device using an update module.*” Ex.1503, ¶161.

3. Claim 4 - wherein the network gatekeeper is further configured to obtain system data from the access device.

Dr. Houh explains that a POSITA would recognize that checking for anti-virus software as in Herrmann (“*wherein the network gatekeeper is further configured to obtain system data from the access device*”) would merely be an additional item for server 215 (“*gatekeeper*”) to check in the authentication process already disclosed by Krantz. See §VII.C & Claim 1, 3. Like Krantz, Herrmann discloses that a “policy

server 460 [which] may enforce a variety of different types of security policies or rules.” Ex.1506, [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.1506; *see also*, Ex.1506, [0012]. Ex.1503, ¶¶165-167.

Krantz’s authentication module, which 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 or an additional Database could be added. Ex.1505, Fig 2 (and corresponding description). 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.1505, [0019]. Ex.1503, ¶168.

4. Claim 5

See Claims 1 and 4, *above* (describing Krantz/Herrmann having gatekeeper audit the status of anti-virus software to authenticate a user per a security policy),

Ex.1503, ¶¶165-168, and Claim 5 (§VIII.A.5), *above* (describing how Krantz “*issue[s] commands.*”) Ex.1503, ¶¶171-173.

5. Claim 6 - *wherein the system data includes antivirus software version data.*

See Claim 4. Ex.1503, ¶175.

Herrmann explains: “a system administrator may establish a policy requiring that **a specific virus protection program** [(‘*version data*’)] is operational on each client device that is connected to a network.” Ex.1506, [0068]. Ex.1503, ¶176.

6. Claim 11 - *wherein the at least one security policy is responsive to an identity of the access device.*

Herrmann’s authentication process specifically “involves obtaining **identity** and authentication information **from the client device 310.**” Ex.1506, [0056]. Ex.1503, ¶180.

Dr. Houh explains that checking for client identity—in addition to checking for anti-virus software—would merely be an additional item for server 215 (“*gatekeeper*”) and its various components (e.g., authentication module 217) to check in the authentication process already disclosed by Krantz. Moreover, a POSITA would be motivated to additionally modify the system of Krantz to include the additional “*security policy*” that “*is responsive to an identity of the access device*” because Krantz is specifically focused on network authentication and security, including identity of clients/users. Ex.1505, [0019]. Ex.1503, ¶181.

7. **Claim 12 - *wherein the at least one security policy is selected by the policy auditor responsive to a part of the less-restricted subset of the protected network to which access is requested.***

Krantz identifies a prior art problem 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.1505, [0013]. Ex.1503, ¶187.

Krantz also specifically discusses how a connecting device may be required to have “provisioning files [] for gaining full access to network 413.” Ex.1505, [0056]; *see also*, Ex.1505, [0032], [0078]. 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.1506, [0071] (“*responsive to a part of the less-restricted subset of the protected network to which access is requested*”). This may be implemented using security rules and checking system data for connecting devices to ascertain compliance. *See* Ex.1506, [0068]. Ex.1503, ¶188-190.

A POSITA would be motivated to modify the system of Krantz to include the additional policy requiring a specific virus protection program be brought up to date as in Herrmann because Krantz for the reasons described above. *See* Claim 3, *above*. Ex.1503, ¶191.

8. Claim 13 - *wherein the audit is responsive to antivirus software executing on the access device.*

See Claims [1.1], [3], [5], [11] and [12] (describing Krantz/Herrmann requiring a specific antivirus program as part of a security policy). Ex.1503, ¶¶193-195.

9. Claim 15 - *wherein the policy auditor is configured to request data from an agent on the access device.*

Krantz discloses the gathering of “*requested data*” from the access device. For instance, “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.1505, [0074]. Ex.1503, ¶197.

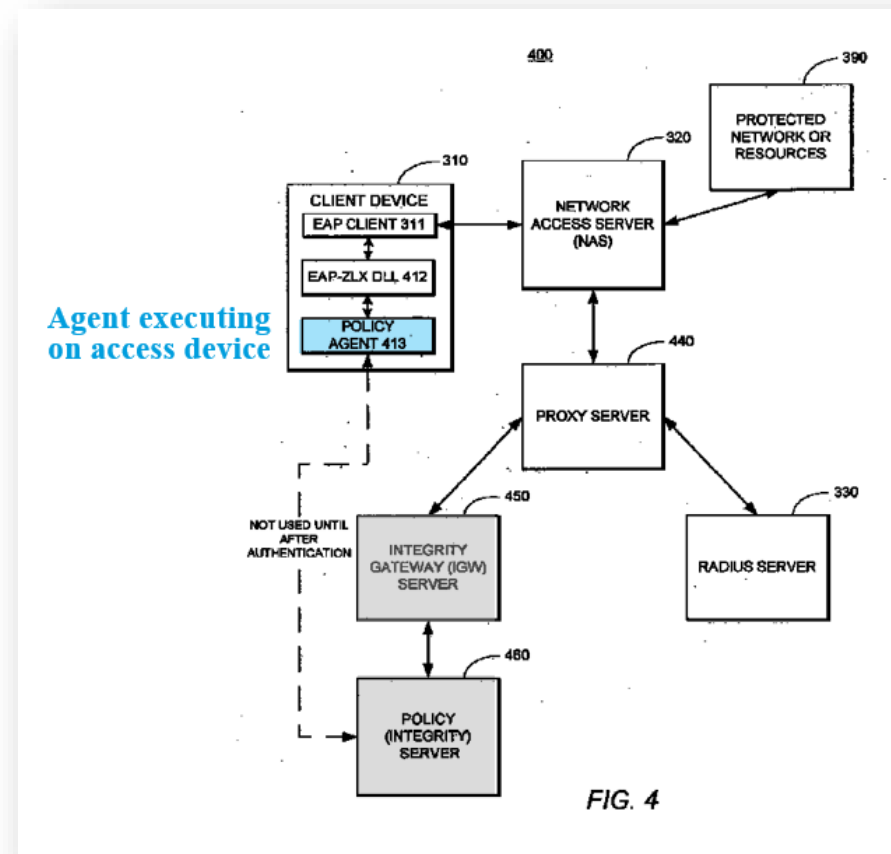
This data is utilized by the network to gather information about whether the device should be granted access to the network. With respect to the XML configuration schema disclosed in [0091] of Krantz, a handshake protocol may be used between the access device and the gatekeeper, which can gather information about the device for network authentication:

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. When EAP-MSChapV2 is indicated, [parameters] indicate whether or not **operating system credentials** should be used for authentication.

Ex.1505 [0099]; *see also* Ex.1505, [0013], [0032], [0072], [0078] (outlining other security policies that may be implemented such as requiring a user to download provisioning files for gaining access to resources); *see also* Ex.1505, [0073] (indicating that EAP messages can be transferred via communication link 234). Ex.1503, ¶198.

Krantz demonstrates a “*policy auditor is configured to request data from . . . the access device*” because via the handshake protocol it is gathering information from both the configuration sub-file as well as other information regarding the device, such as the operating system credentials for the purposes of implementing a security policy (and authentication). Ex.1503, ¶199.

Although Krantz does not state that “*an agent*” is used in requesting data from the access device, it would have been obvious in view of Herrmann. For example, Herrmann discloses a “POLICY AGENT 413” (“*agent*”) executing on the client access device interacting with a “POLICY (INTEGRITY) SERVER 460” and “INTEGRITY GATEWAY (IGW) SERVER 450” (shown in gray) below.



Ex.1506, Fig. 4 (annotated). Ex.1503, ¶¶200-201.

Herrmann discloses that “policy agent (or integrity agent) 413 [are used] to retrieve information about the current security policy in operation on the client device 310 [*“policy auditor is configured to request data from. . . the access device”*].” Ex.1506, [0064]. Herrmann explains: “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.1506, [0067]. Dr. Houh explains that to audit the device pursuant to a security policy, certain information regarding the device must

be requested. The policy server is notified by the client, containing policy agent 413, through periodic status messages called “IA_HEARTBEAT(s)” in order to authenticate the access device. Ex.1506, [0080], [0098]. Ex.1503, ¶202.

A POSITA would have been motivated to add the security policy agent of Herrmann to the client of Krantz for several reasons, including for the reasons already stated. *See* §VII.C, *above*. Two of the stated goals of Krantz involve automation and security. Ex.1505, [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.1503, ¶203.

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.1506, [0064]; *see also*, Ex.1506, [Fig. 4]. This is the same protocol utilized in Krantz. Ex.1505, [0018]. In addition, the modification to the teachings of Krantz can be implemented as a simple software modification to include a policy agent. Ex.1503, ¶204.

10. Claim 24 - *wherein the network gatekeeper is configured to update the access device if 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 resources located on the second network.**” [*“network gatekeeper is configured to update the access device if requirements of the security policy are not satisfied”*]. Ex.1505, [0032]; see also Ex.1505, [0056], [0110]; Ex.1503, ¶222.

Krantz therefore discloses that the *“network gatekeeper is configured to update the access device if requirements of the security policy are not satisfied.”* Ex.1503, ¶223.

To the extent one may assert Krantz does not disclose this claim element, Krantz/Herrmann disclose that the *“network gatekeeper is configured to update the access device if requirements of the security policy are not satisfied.”* Krantz explains 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.1505, [0013]. Ex.1503, ¶224.

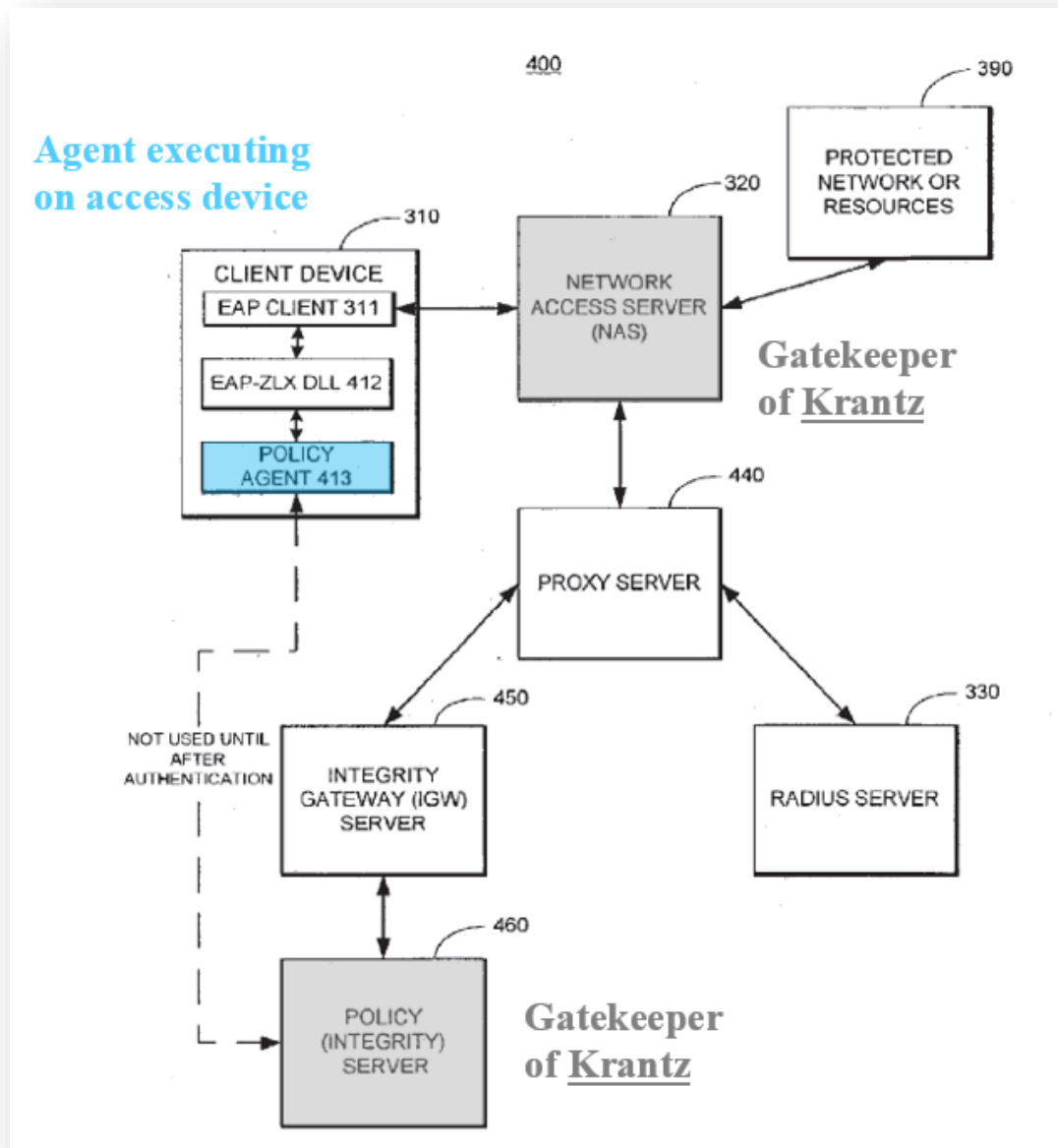
Krantz also specifically discusses how a connecting device may be required to have “provisioning files [] for gaining full access to network 413.” Ex.1505, [0056]; *see also* Ex.1505, [0032], [0078] (discussing provisioning clients for gaining access to the network). Dr. Houh confirms provisioning files generally relate to network connectivity and security. Ex.1509, [0079]. Ex.1503, ¶225.

Herrmann additionally discloses that “[i]t becomes critical, therefore, to promptly update anti-virus applications on all machines in a network in a timely fashion.” Ex.1506, [0012]. Ex.1503, ¶226.

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.1506, [0071]. This may be implemented using security rules and checking system data for connecting devices to ascertain compliance. Ex.1506, [0068] (“The policy server 460 may enforce [*‘network gatekeeper is configured’*] a variety of different types of security policies or rules. . . a system administrator may establish a **policy requiring that a specific virus protection program is operational** on each client device that is connected to a network [*“to update the access device if requirements of the security policy are not satisfied”*].”) Ex.1503, ¶227.

The policy server 460 of Herrmann is similar to the “*gatekeeper*” (server 215) of Krantz. Ex.1503, ¶¶201-204. Both Herrmann and Krantz discuss logical

implementations of the disclosed server techniques and thus the techniques of, e.g., the policy (integrity) server 460 of Herrmann would easily integrate with the system of Krantz as depicted below. Ex.1503, ¶228.



Ex.1506, Fig. 4 (annotated); *see also* Ex.1505, [0038], [0051] (describing the use of logical communication links and logical representations of computer systems); Ex.1506, [0026]. Ex.1503, ¶228.

A POSITA would be motivated to modify the system of Krantz to include the additional policy requiring a specific virus protection program be brought up to date because Krantz is specifically focused on network authentication and security. Ex.1505, [0019]. Ex.1503, ¶229.

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.1505, [0019]. Requiring the client to update antivirus software would merely be an additional condition, which a POSITA would understand the importance of as confirmed by the 484 Patent itself. Ex.1501, 2:14-22. Moreover, because prior art GateKeepers were known to control security policies (Ex.1501, 2:26-42), Dr. Houh confirms the disclosed gatekeeper of Krantz in combination with Herrmann renders obvious that it is the “*network gatekeeper [that] is configured to update the access device if requirements of the security policy are not satisfied.*” Ex.1503, ¶229.

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 challenges presented in this Petition are neither cumulative nor redundant to the prosecution of the 484 Patent (or related patents), as neither Krantz nor Herrmann was cited or considered by the Examiner during prosecution of the 484 Patent. The references in this Petition were neither relied upon during prosecution nor are they cumulative of art relied upon during prosecution. Further, the 484 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) (“*Fintiv II*”) (explaining that factor 1 “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)) (“As to factor 1, there is no evidence as to whether there will be a stay in the parallel case, so we regard this factor as neutral.”)

2. Parallel Proceeding Trial Date

Regarding factor 2, no trial date has been set. In addition, according to the most recent statistics⁷ 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 October 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 the early stages of discovery, a motion to dismiss has been filed and partially granted, and the investment by the parties has been relatively minimal. In addition, claim 6 is not at issue in the related litigations. *Samsung Bioepis Co. Ltd v. Regeneron Pharmaceuticals, Inc.*, IPR2023-00739, Paper 9 at 57 (Oct. 20, 2023).

⁷ <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**. Cisco and Fortinet 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* “says nothing about situations in which the petitioner is the same as, or is related to, the district court defendant.” *Fintiv*, IPR2020-00019, Paper 11 at 13-14.

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 484 Patent, is directed at the same problem and proposes the same solutions as the 484 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

The Challenged Claims of the 484 Patent are unpatentable for the reasons demonstrated above.

Dated: April 18, 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 13,964 words (as determined by the Microsoft Word word-processing system used to prepare the brief and including annotated figures), excluding the parts of the brief exempted by 37 C.F.R. § 42.24.

Dated: April 18, 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. § 42.6I, I hereby certify that on this 18th day of April, 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

Dated: April 18, 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