

Filed: April 15, 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.

IPR2024-00676
U.S. Patent No. 8,677,450

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 8,677,450**

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES.....	v
EXHIBIT LIST	vi
CLAIM LISTING	vii
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 450 PATENT	4
A. Effective Filing Date	4
B. Person of Ordinary Skill in the Art	4
C. Overview of the 450 Patent	4
VI. CLAIM CONSTRUCTION	7
VII. PRINCIPAL PRIOR ART	7
A. Summary of Krantz	7
B. Summary of Herrmann.....	10
C. The Combination of Krantz and Herrmann	14
VIII. THE CHALLENGED CLAIMS ARE UNPATENTABLE	19
A. Ground 1: The Challenged Claims are Obvious Based on Krantz in view of Herrmann.....	19
1. Claim 1	19
i. [1.0] A method for applying a security policy to network devices... ..	19

ii.	[1.1] performing an authentication of a device connected to an access point;.....	28
iii.	[1.2] scanning the device to collect information regarding the device;	33
iv.	[1.3] applying a security policy, the security policy including one or more requirements pertaining to the authentication and the information, the application of the security policy taking place in response to a gatekeeper, and	38
a.	applying a security policy . . . the information	38
b.	applying a security policy ... a gatekeeper	40
v.	[1.4] configuring the access point in response to a result of applying the security policy.....	47
2.	[2.0] further comprising facilitating updates to software on the device in response to applying the security policy, using the gatekeeper.	56
3.	[3.0] wherein configuring the access point includes setting an access control list on the access point.	59
4.	[4.0] wherein configuring the access point includes assigning a VLAN.....	63
5.	[7.0] wherein the authentication includes using an EAP protocol.	65
6.	[8.0] wherein the authentication includes using a RADIUS protocol.	65
7.	[9.0] wherein one of the requirements pertains to a status of an application on the device.	67
8.	[10.0] wherein one of the requirements pertains to a status of an operating system exon [sic] the device.....	68
9.	[14.0] wherein the scanning is performed using an agent on the device.	69
10.	Claim 16.....	72

i.	[16.0] A method of providing access over a communication network, the method comprising:	72
ii.	[16.1] receiving at an access point a request for access to a less restricted network, the request coming from an access device;	75
iii.	[16.2] applying a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device;	80
a.	applying a security policy... in response to the request.....	80
b.	application of the security policy including performing an audit of the access device	83
iv.	[16.3] providing information to the access device to improve compliance of the access device to the security policy, in response to the audit;	87
v.	[16.4] granting access to the less-restricted network based on satisfaction of the security policy by the updated access device;	88
vi.	[16.5] authenticating a user of the access device, wherein granting access is further based on the authentication.....	90
11.	Claim 22	91
12.	[23.0] wherein performing the audit includes using an agent on the access device to collect information regarding the access device.....	95
13.	[25.0] wherein performing the audit includes receiving operating system information from the access device.....	98
14.	[27.0] wherein the information includes a software update of software on the access device.	99
IX.	THE BOARD SHOULD NOT EXERCISE ITS DISCRETION AND DENY INSTITUTION	102
A.	The Board Should Not Deny Institution Under 35 U.S.C. § 325(d).....	102

B.	The Board Should Not Deny Institution Under 35 U.S.C. § 314(a).....	102
1.	No Evidence Regarding a Stay	102
2.	Parallel Proceeding Trial Date	103
3.	Parallel Proceeding Investment.....	103
4.	Overlapping Issues with the Parallel Proceeding.....	104
5.	Overlapping Parties.....	104
6.	Strength of Petition and Other Considerations	104
X.	CONCLUSION.....	105

TABLE OF AUTHORITIES

	Page(s)
 Cases	
<i>Amazon Web Services et al. v. Zentian Ltd.</i> , IPR2023-01194, Paper 10 (Jan. 10, 2024).....	76
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 15 (May 13, 2020).....	75
<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)	77
<i>Vivid Techs., Inc. v. Am. Sci. & Eng.'g. Inc.</i> , 200 F.3d 795 (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)	75
35 U.S.C. § 325(d)	75
 Other Authorities	
37 C.F.R. § 42.100(b)	7
https://www.uscourts.gov/statistics-reports/federal-court- management-statistics-december-2023	76

EXHIBIT LIST

No.	Exhibit Description
1401	U.S. Patent No. 8,677,450
1402	U.S. Patent No. 8,677,450 File History
1403	Declaration of Henry Houh, Ph.D
1404	CV of Henry Houh, Ph.D
1405	U.S. Patent Pub. No. 2004/0111520 to Krantz et al
1406	U.S. Patent Pub. No. 2004/0107360 to Herrmann et al
1407	IEEE Std 802.1Q-1998 – IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
1408	U.S. Patent No. 6,430,621 to Srikanth et al.
1409	U.S. Patent No. 6,032,194 to Gai et al.
1410	Cisco IOS 12.0 Switching Services (1999)
1411	Microsoft Computer Dictionary 5 th Edition (2002)
1412	Webster’s New World Computer Dictionary (2001)
1413	[Reserved]
1414	[Reserved]
1415	[Reserved]
1416	RFC 2716 – PPP EAP TLS Authentication Protocol
1417	Wireless security with 802.1x and PEAP (2003)
1418	[Reserved]
1419	[Reserved]
1420	[Reserved]

CLAIM LISTING

Claim No.	Claims
[1.0]	A method for applying a security policy to network devices, the method comprising
[1.1]	performing an authentication of a device connected to an access point;
[1.2]	scanning the device to collect information regarding the device;
[1.3]	applying a security policy, the security policy including one or more requirements pertaining to the authentication and the information, the application of the security policy taking place in response to a gatekeeper, and
[1.4]	configuring the access point in response to a result of applying the security policy.
[2]	The method of claim 1, further comprising facilitating updates to software on the device in response to applying the security policy, using the gatekeeper.
[3]	The method of claim 1, wherein configuring the access point includes setting an access control list on the access point.
[4]	The method of claim 1, wherein configuring the access point includes assigning a VLAN.
[7]	The method of claim 1, wherein the authentication includes using an EAP protocol.
[8]	The method of claim 1, wherein the authentication includes using a RADIUS protocol.
[9]	The method of claim 1, wherein one of the requirements pertains to a status of an application on the device.
[10]	The method of claim 1, wherein one of the requirements pertains to a status of an operating system on [sic] the device.
[14]	The method of claim 1, wherein the scanning is performed using an agent on the device.

[16.0]	A method of providing access over a communication network, the method comprising:
[16.1]	receiving at an access point a request for access to a less restricted network, the request coming from an access device;
[16.2]	applying a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device;
[16.3]	providing information to the access device to improve compliance of the access device to the security policy, in response to the audit;
[16.4]	granting access to the less-restricted network based on satisfaction of the security policy by the updated access device; and
[16.5]	authenticating a user of the access device, wherein granting access is further based on the authentication.
[22.0]	A method of providing access over a communication network, the method comprising:
[22.1]	receiving at an access point a request for access via a less-restricted network, the request coming from an access device;
[22.2]	applying a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device;
[22.3]	providing information to the access device to improve compliance of the access device to the security policy, in response to the audit; and
[22.4]	granting access to the less-restricted network based on satisfaction of the security policy by the updated access device, the granting of access includes configuring the access point to allow the access.
[23]	The method of claim 22, wherein performing the audit includes using an agent on the access device to collect information regarding the access device.
[25]	The method of claim 22, wherein performing the audit includes receiving operating system information from the access device.
[27]	The method of claim 22, wherein the information includes a software update of software on the access device.

I. INTRODUCTION

Petitioner Cisco Systems, Inc. and Fortinet, Inc. submits this Petition for *Inter Partes* Review of claims 1-4, 7-10, 14, 16, 22-23, 25, and 27 (“Challenged Claims”) of U.S. Patent No. 8,677,450 (“450 Patent” (Ex.1401)), assigned to Patent Owner, InfoExpress Inc. Petitioner respectfully submits that the Challenged Claims of the 450 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 450 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 450 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 450 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 450 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 450 Patent.

B. Identification of Challenged Claims

Ground 1: Claims 1-4, 7-10, 14, 16, 22-23, 25, and 27 are unpatentable as obvious under 35 U.S.C. § 103 based on Krantz (Ex.1405) in view of Herrmann (Ex.1406).

V. THE 450 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 450 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.1403, ¶¶20-22.

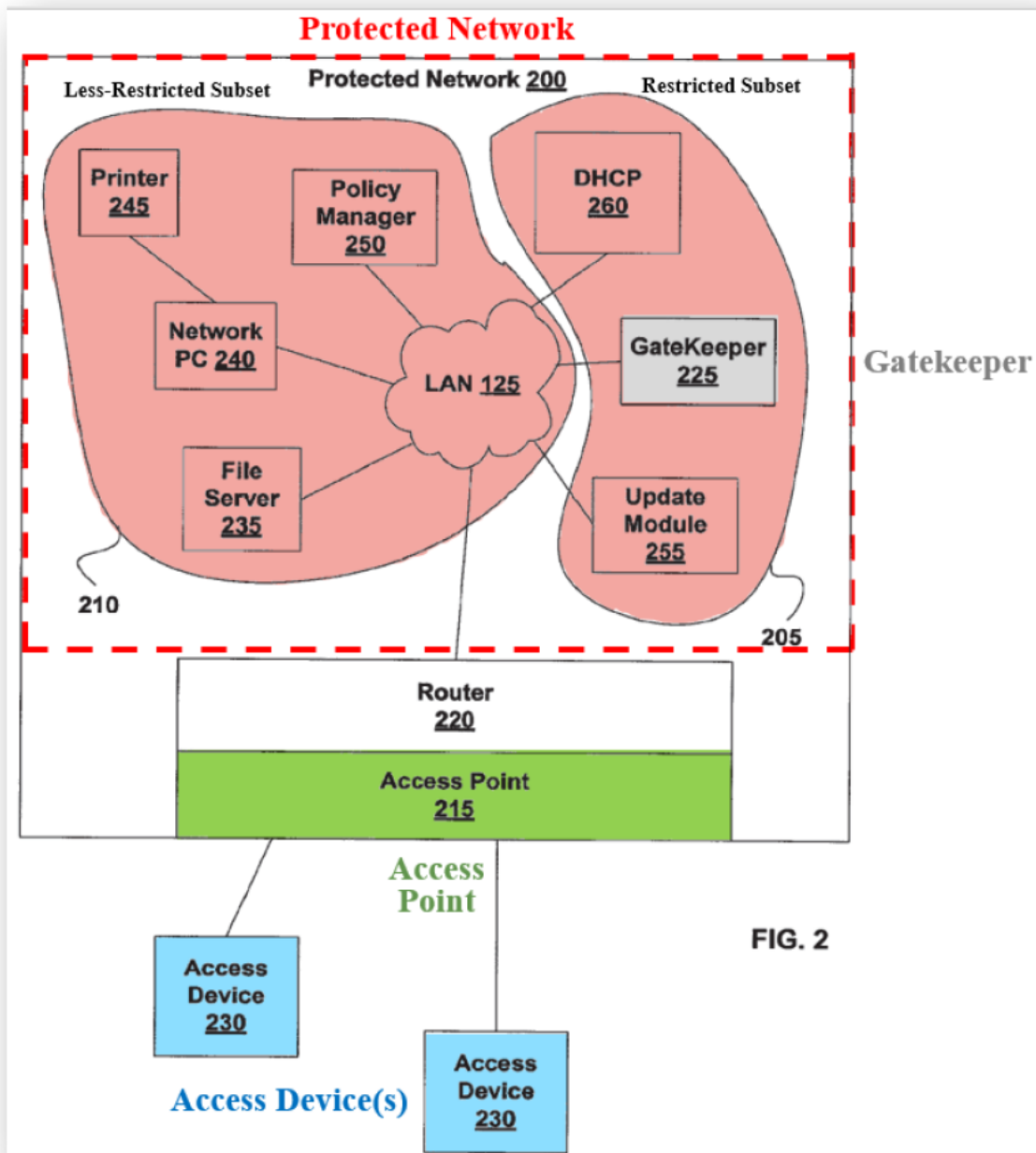
C. Overview of the 450 Patent

The 450 Patent describes “a protected network physically or logically divided into a restricted subset and one or more less-restricted subsets.” Ex.1401, 2:56-58. Access to less-restricted networks from a device “are first passed to the restricted subset.” Ex.1401, 2:59-60. Elements of the “restricted subset”—such as a “gatekeeper”—“apply security policies” to the device requesting access. Ex.1401, 2:59-60. If requesting device satisfies the “security policies,” access is granted “to

a less-restricted subset of the protected network.” Ex.1401, 2:60-64. Moreover, “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.1401, 2:62-64. Furthermore: “[i]n some embodiments, Authenticate User Step [] is considered part of the security policy audit.” Ex.1401, 12:9-11. Additionally, the security policy may include “scanning Access Device 230 for malicious code.” Ex.1401, 6:63-65. Such “active probing, scanning, and/or collection” may occur. Ex.1401, 12:7-9.

The 450 Patent explains, both “the passing of access requests to the restricted subset” and the subsequent granting of such requests is “accomplished by configuring and reconfiguring a communication port of an access point.” Ex.1401, 2:64-67.

Figure 2 depicts embodiments of the 450 Patent:



Ex.1401, Fig. 2 (annotated); Ex.1403, ¶34.

“Protected Network 200,” is “either physically or logically divided into a Restricted Subset 205 and a Less-Restricted Subset 210.” Ex.1401, 5:59-61. Access

to Protected Network 200 is “under the control of a GateKeeper 225,” which “enforce[s] a security policy against one or more Access Device 230 requesting access.” Ex.1401, 5:64-67.

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 450 Patent, the Board need not expressly construe the claim terms. *Vivid Techs., Inc. v. Am. Sci. & Eng. 'g. Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

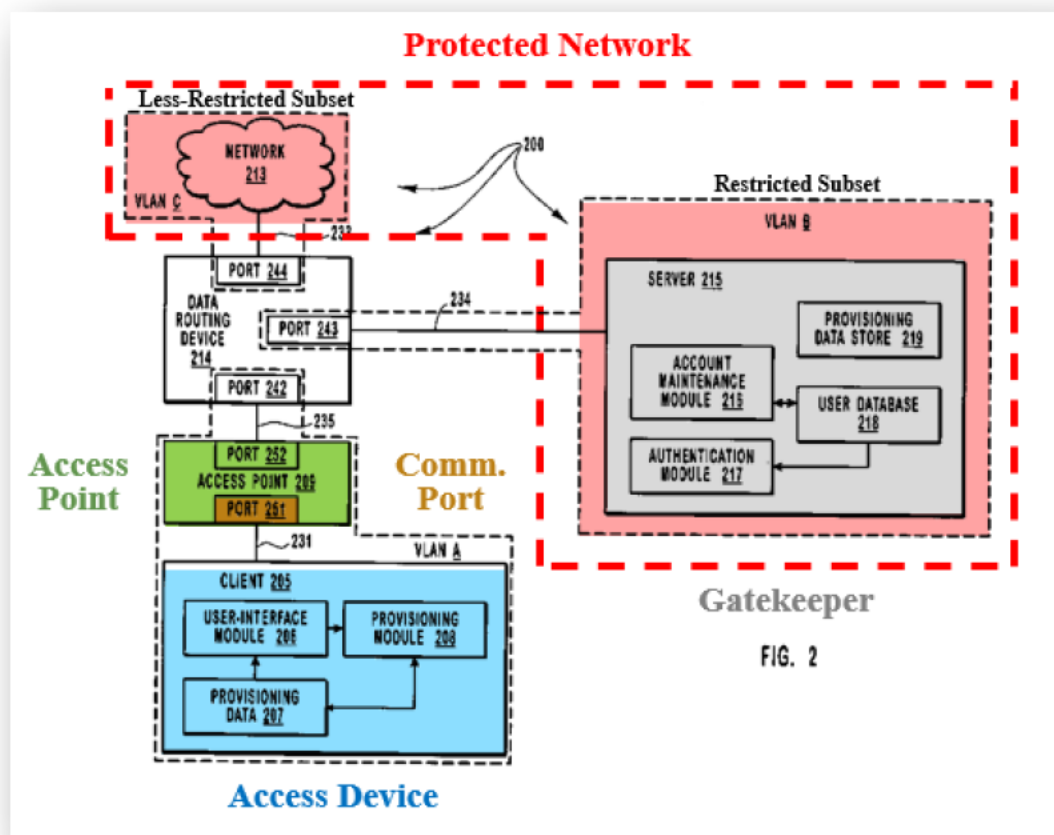
VII. PRINCIPAL PRIOR ART

A. Summary of Krantz

U.S. Patent Pub. No. 2004/0111520 to Krantz et al. (Ex.1405) was filed on December 6, 2002, and published on June 10, 2004. Krantz is prior art to the 450 Patent at least under pre-AIA 35 U.S.C. § 102(e).

Krantz is directed to facilitating controlled access to protected networks and in particular, “increasing the level of automation when provisioning and configuring a computer system to access a network.” Ex.1405, [0015].

Krantz teaches a system in which a device attempts to access a protected network. Ex.1405, [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.1405, [0016], [0068]-[0071], [0099], [0104], [0107]-[0109]. An embodiment of this network architecture is depicted below:



Ex.1405, Fig. 2 (annotated).¹ Ex.1403, ¶43.

Krantz utilizes Virtual Local Area Network (“VLAN”) techniques. Ex.1405, [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... 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.1405, [0060]. Access Point 209 utilizes ports which can be configured for data transfer. Ex.1405, [0062].

Krantz teaches a client requesting access to the network can send credentials to a server to authenticate itself. Ex.1405, [0016]. Based on credentials supplied, server “may authorize the client for at least partial access” or access to the entire

¹ Patentee uses different words to describe claimed features, e.g., a “Protected Network” and “Access Device” in some instances (e.g., Ex.1401, Fig. 2) versus “Network/Computer Network/communication network” and “Network Device/Device” in others (see, e.g., Ex.1401, claim 1). Similarly, those terms are used interchangeably herein.

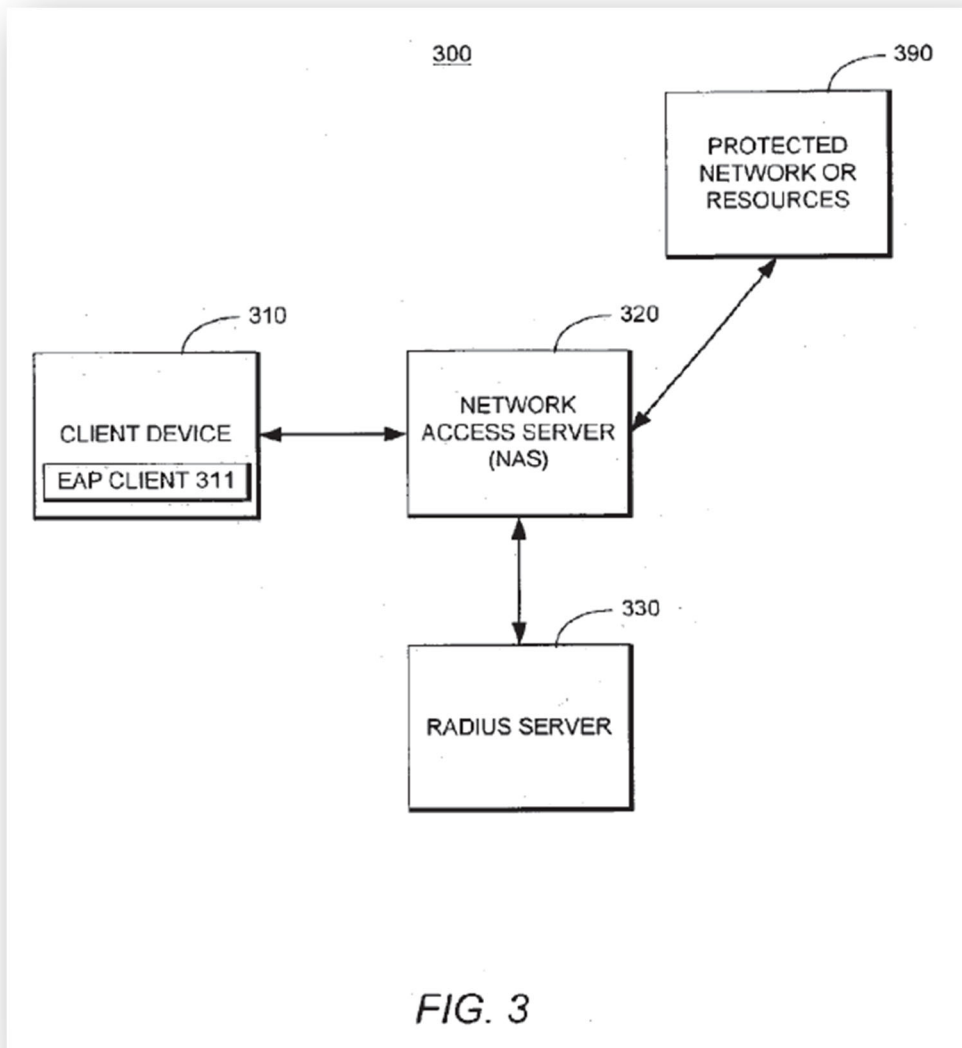
network. Ex.1405, [0016], [0104], [0107]-[0109]. Authentication may be made by server 215. Ex.1405, [0068]-[0071], [0099]. The server is also responsible for ensuring the client device adheres to certain configuration settings—including the established encryption protocol—for gaining access to the network authorized to be accessed. Ex.1405 [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 art to the 450 Patent at least under pre-AIA 35 U.S.C. § 102(e). Ex.1406.

Herrmann describes enforcing security policies when providing access to a network. Herrmann explains that if a device connected to a network is infected with a virus or worm, it may infect other machines on the network, and thus, ensuring such devices are running current anti-virus programs is particularly important. Ex.1406, [0012]. Thus, Herrmann proposes collecting 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.1406, [Abstract], [0063]. The basic architecture of the system includes a client access device, network access server, and

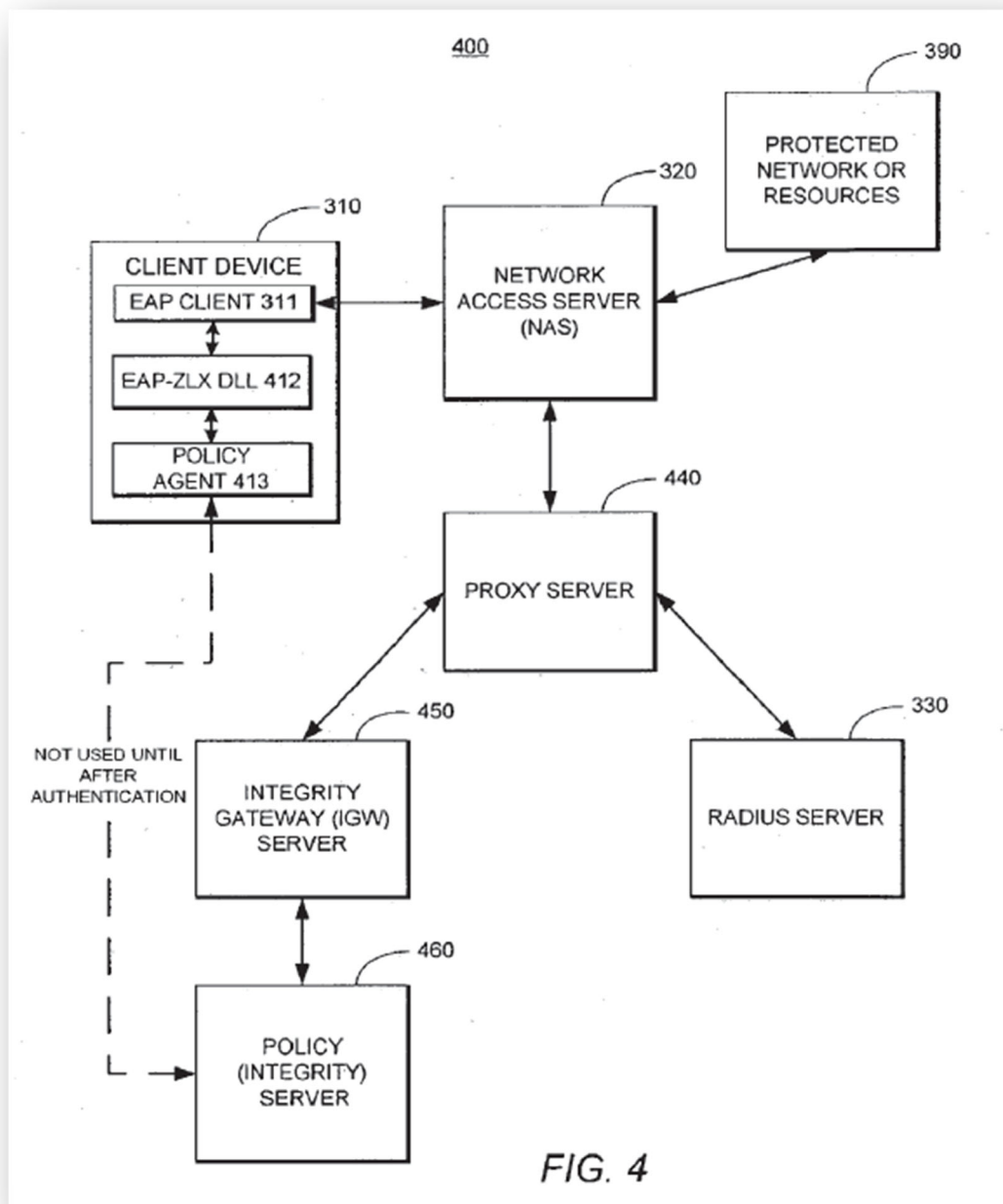
protected network and/or resources shown below in Figure 3 of Herrmann. Ex.1406, [0018], [0053], [0063].



Ex.1406, Fig. 3.

In Figure 4, “a client device 310 connects to the NAS 320 to access the protected network or resources 390.” Ex.1406, [0062]-[0063]. However, the system

includes an additional “policy (integrity) server 460” ... which “ensures that all users accessing a particular system or network comply with specified security policies, including access rights and cooperative anti-virus enforcement” and can deny network access for access devices that are not in compliance. Ex.1406, [0062], [0067].



Ex.1406, 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.1406, [0064]. This allows “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.1406, [0067].

C. The Combination of Krantz and Herrmann

It would have been obvious to include Herrmann’s techniques related to enforcing security policies (e.g., antivirus software status) and obtaining system data in the system of Krantz. Krantz already discloses that “access point 209 may block [] protocols ... from being transferred **until client 205 is authenticated (and authorized).**”² Ex.1405, [0072]. Furthermore, “[w]hen credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) **and compare the credentials to entries in [user database].**” Ex.1405, [0076]; Ex.1403, ¶51.

A POSITA would recognize that checking for anti-virus software would simply be an additional item for authentication module 217 (of server 215) to check in the already disclosed Krantz authentication process. Like Krantz, Herrmann discloses a “policy server 460 [which] may enforce a variety of different types of security policies or rules.” Ex.1406, [0068]. One rule would be “a policy requiring

² Emphasis added in bold throughout unless otherwise indicated.

that a **specific virus protection program** is operational on each client device... connected to a network.” Ex.1406, [0068]; Ex.1406, [0012]. Ex.1403, ¶52.

Krantz’s authentication module, which compares credentials of a user against a database (e.g., user-identifier/password), as modified by Herrmann, would also check for approved antivirus programs. Information regarding approved antivirus software and connected devices could be stored in the User Database or an additional Database could be added. Ex.1403, ¶53.

The 450 Patent itself confirms a POSITA would recognize the need for the authentication module of Krantz to check for approved antivirus programs. In the 450 Patent background, it discusses a **prior art** GateKeeper 110 (Ex.1401, 2:34-36) and 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.1401, 2:27-30; Ex.1403, ¶55.

Both Krantz and Herrmann are analogous art to the 450 Patent for at least two reasons. *First*, Krantz and Herrmann are both directed toward the same field of endeavor of the 450 Patent—network security. Ex.1401, 1:26-27; Ex.1405, Abstract Ex.1406, Abstract; Ex.1403, ¶56.

Second, Krantz and Herrmann are reasonably pertinent to a problem described in the 450 Patent: reliance “on mere user authentication” and “assur[ing] that **an**

access device used by the authenticated user meets network security policies” such as current anti-virus software. Ex.1401, 1:49-51, 1:60-63. Ex.1403, ¶57.

Krantz discloses a security policy beyond user authentication. For instance, “client 205 and server 215 exchange EAP-messages to pass **certificates, keys, and supported cipher suites**... other credential information may also be exchanged between client 205 and server 215.” Ex.1405, [0074]. Krantz discloses the security policy can include “a configuration sub-file to indicate whether or not **operating system credentials** should be used for authentication.” Ex.1405, [0099]; Ex.1403, ¶58.

Krantz states: “[i]n some embodiments, a server on a network can provide a client with limited access to the network. For example, a server... 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.1405, [0056]; Ex.1403, ¶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.1406, [0064]. “In response to [] 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 [an] up-to-date version of the applicable security policy.**” Ex.1406, [0067]. This policy server is notified by the client, containing policy agent 413, through periodic status messages (“IA_HEARTBEAT(s)”) to authenticate the device. Ex.1406, [0080], [0098]; Ex.1403, ¶60.

Herrmann discloses: “[n]ew viruses are frequently released... It becomes critical, therefore, to promptly update **anti-virus applications on all machines in a network**... before the network is infiltrated by a newly released virus.” Ex.1406, [0012]. Herrmann discloses: “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.1406, [0071]; Ex.1403, ¶61.

Herrmann discloses: “policy server 460 may enforce a variety of different types of security policies or rules... [e.g., requiring] devices connecting to a given network to be using particular security or anti-virus programs.” Ex.1406, [0068]; Ex.1403, ¶62.

It would have been obvious to combine Herrmann’s network access techniques (including checking its antivirus software) with the authentication and authorization system of Krantz. Both perform 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.1403, ¶63.

It would have been obvious to combine Herrmann with Krantz; a POSITA would have been motivated to do so based on the teachings of Krantz, e.g., Krantz relates to “configuring **computer systems** to appropriately communicate on a network, and more specifically, to automatically providing a **computer system** with appropriate information such that **the computer system can be provisioned** to communicate on a network.” Ex.1405, [0002]. Similarly, Herrmann explains that “[t]he present invention relates to ... policy enforcement on **computer systems** connected on one or more networks...” Ex.1406, [0003]; Ex.1403, ¶64.

A POSITA would have been motivated to apply Herrmann’s technique of checking connecting computer systems for antivirus software as it would provide added security and increase automation when connecting to a network. Ex.1406, [0068]; Security and automation are two stated goals of Krantz. E.g., Ex.1405, [0014], [0019]. A POSITA would have recognized that Herrmann’s policy server disclosure checking for compliance with an antivirus security policy, would be complimentary to Krantz, which seeks an automated process for network security. A POSITA would have had a reasonable expectation of success in implementing

these techniques into a combined Krantz/Herrmann system as it would involve minimal changes to the existing Krantz system. Ex.1403, ¶65.

VIII. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: The Challenged Claims are Obvious Based on Krantz in view of Herrmann

The Challenged Claim are taught or suggested by Krantz and Herrmann for the following reasons.

1. Claim 1

i. *[1.0] A method for applying a security policy to network devices...*

Krantz discloses a “*network*”³, and “*network devices*.” VLANs B and C constitute a protected network consistent with the “*network*” of the 450 Patent. The disclosed networks “can be implemented using any number of techniques [e.g.] ... **Virtual Local Area Networks (‘VLANs’)... Virtual Private Networks (‘VPNs’)**...” Ex.1405, [0017]. These are methods of creating a protected “*network*” as they facilitate access control capabilities described in Krantz. Ex.1405, [0017]

³ The patent specification/figures refer to a “protected network” throughout, but claims a “network” and/or “communication network.”

(“the server [] may authorize the client for [] partial access to the single network...”). Ex.1403, ¶¶66-67.

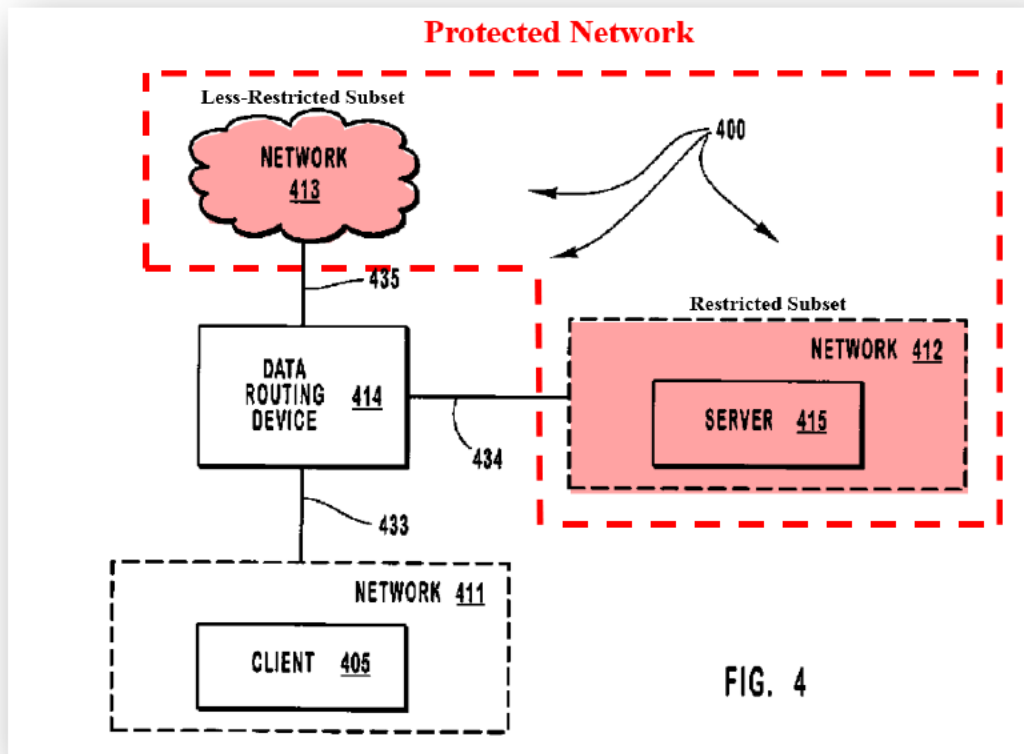
Krantz discloses “*network*” access control, e.g., “[a] server includes the **functionality to authorize clients to access a second network...**” Ex.1405, [0016]. “[C]lient sends credentials to [server] to authenticate with the server. Based on the credentials, the **server may authorize the client for at least partial access to the second network** and/or may deny access to the second network and **authorize the client for at least partial to access to the first network.**” Ex.1405, [0016]; Ex.1403, ¶68.

A POSITA would understand that combining the first/second networks into a logical “*network*” would be done physically or logically with Krantz focused on logical representations. Ex.1405, [0038]; Ex.1403, ¶69. Combining physical networks was a networking technique well-known to POSITAs. *E.g.*, Ex.1411, 223; Ex.1412, 317; Ex.1403, ¶70.

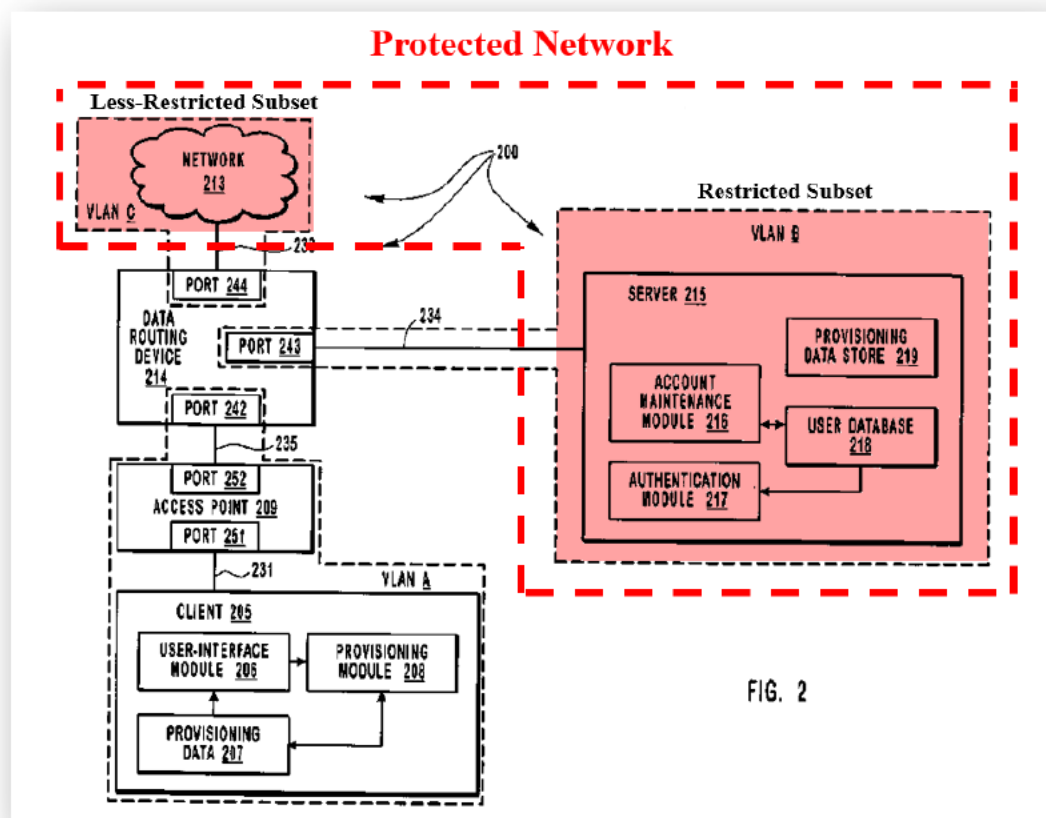
The 450 Patent’s “*network*” may be “**physically or logically divided** into a restricted subset and [] less-restricted subsets.” Ex.1401, 2:56-58. Such restricted and less-restricted subsets “are [typically] characterized by Virtual Local Area Networks (e.g., VLANs),” (Ex.1401, 3:3-8), and the protected “*network*” may

include “access restrictions” (“*access control*”). Ex.1401, 6:25-41; Ex.1403, ¶71.

The “*network*” of Krantz is below:



Ex.1405, Figure 4 (annotated).



Ex.1405, Figure 2 (annotated); Ex.1403, ¶72.

Krantz Figure 4 is “a network architecture 400 that can provide access to a first network while restricting access to a second network.” Ex.1405, [0030]. Krantz explains: “access to resources located in network 413 can be restricted [using] Virtual Local Networks (“VLANs”).” Ex.1405, [0052]; *see also* [0054] (access to resources on network 413 can be restricted using VPNs). Figure 2 implements the architecture of Figure 4 “using VLAN techniques,” which “can facilitate increasing the level of automation when provisioning a client.” Ex.1405, [0057]. Figure 2

provides specific techniques for Krantz's networking architecture. Ex.1405, Figures 2 and 4 and related descriptions. Thus, combined Networks 413 and 412 (also annotated as VLAN C and VLAN B) constitute a single logical “*network*.” Ex.1403, ¶73.

To the extent “*network*” is required to be a single network, Krantz explains that its techniques can be used “**within a single network.**” Ex.1405, [0017]; *see also* Ex.1405, [0055]; Ex.1403, ¶74; *see also* Ex.1405, [0016], [0071], [0074]-[0076] (“If an authenticated user of client **205** is authorized to access resources located on VLAN C...”); [0104], [0107]-[0109]; Ex.1403, ¶75.

Regarding network access, Krantz discloses several “*security polic[ies]*.” “Depending on the particular EAP type, server 215 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.” Ex.1405, [0074]; Ex.1403, ¶76.

Krantz discloses receiving data from clients (“*network device*”). For example, “a server has the functionality to authorize access” to a network/selected elements within a network after client (“*network device*”) sends credentials to the server. Ex.1405, [0016], [0071]. The “server (**based at least in part on received credentials**) [*‘applying a security policy’*] may authorize the client for at least partial

access to the single network [*‘to [the] network device[]’*].” Ex.1405, [0017]; *see also* [0074]-[0076], [0104], [0107]-[0109] (describing techniques for requesting access in a VLAN environment). Credentials from device/user in Krantz are used to control access to protected network resources (*“applying a security policy”*). Ex.1405, [0016], [0068]-[0071], [0099], [0104], [0107]-[0109]. A POSITA would understand this as *“applying a security policy to [a] network device[]”* because Krantz’s server is inspecting credentials (Ex.1405, [0016], [0071]) and authorizing access based on the inspection (Ex.1405, [0076], [0104], [0106]-[0109]), e.g., matching entries in a database (Ex.1405, [0076]); Ex.1403, ¶77.

Credentials “can include sending an Extensible Authentication Protocol (“EAP”) Response/Identity message from the client to the server...” Ex.1405, [0018]. Other audit data provided by Krantz’s “*network device*” may include, “user-identifier[s] and password[s].” Ex.1405, [0076]. Furthermore, “[a]fter an EAP type is selected . . . **computer systems can attempt to authenticate with one another** through... EAP messages... in accordance with the selected EAP type [e.g.], 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.1405, [0068]. EAP-TLS (e.g., Ex.1405, [0067]-[0074], [0100]) was a known

authentication protocol for authenticating client devices. Ex.1405, [0099] (describing EAP-MSChap V2); Ex.1403, ¶78.

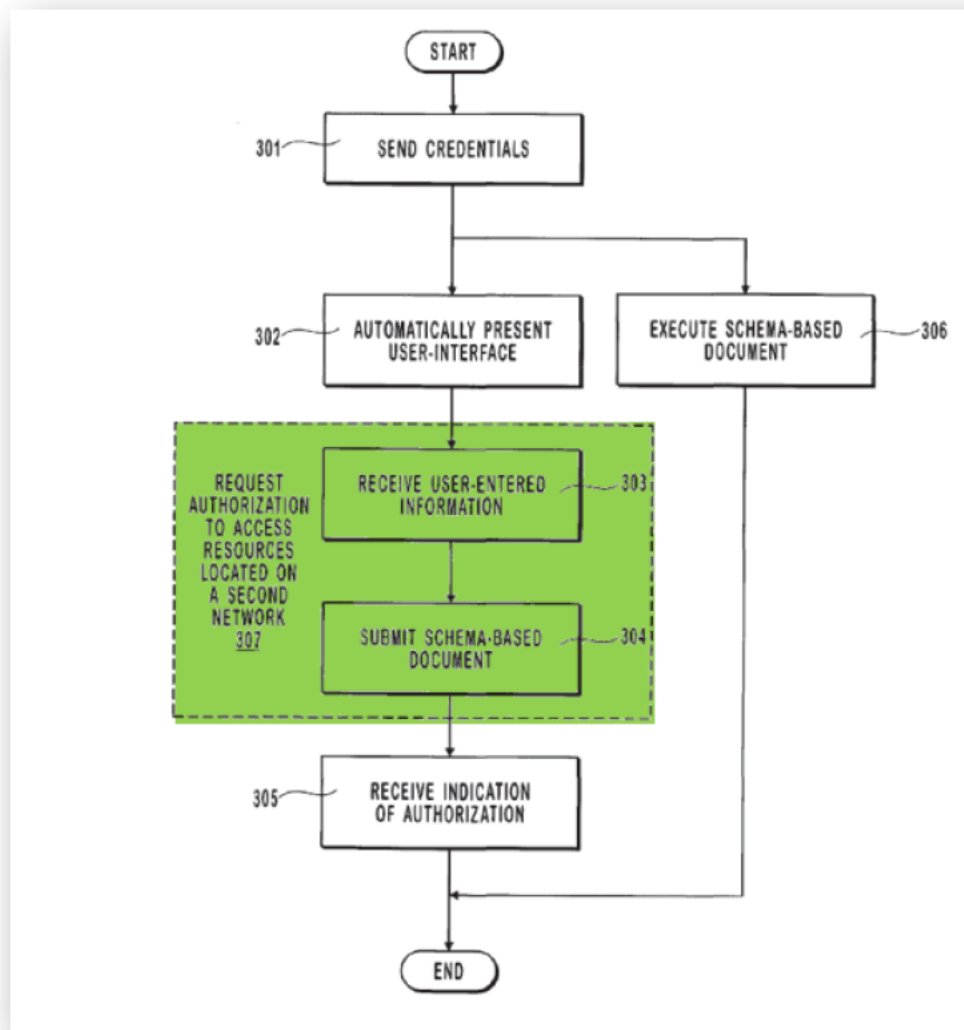
Krantz explains that the credentials are audited **at the server**:

[A]uthentication module 217 can receive the credentials [] and compare the credentials to entries in user⁴ database 218.

Ex.1405, [0076]; Ex.1403, ¶79.

Krantz Figure 3 “[illustrates] a method 300 for provisioning a computer system...” Ex.1405, [0070]. It “includes a functional, result-oriented step for **requesting authorization to access resources located on a second network (step 307).**” Ex.1405, [0104]. “**Step 307** may include any corresponding acts for accomplishing [] authorization to access resources located on the second network.” Ex.1405, [0104].

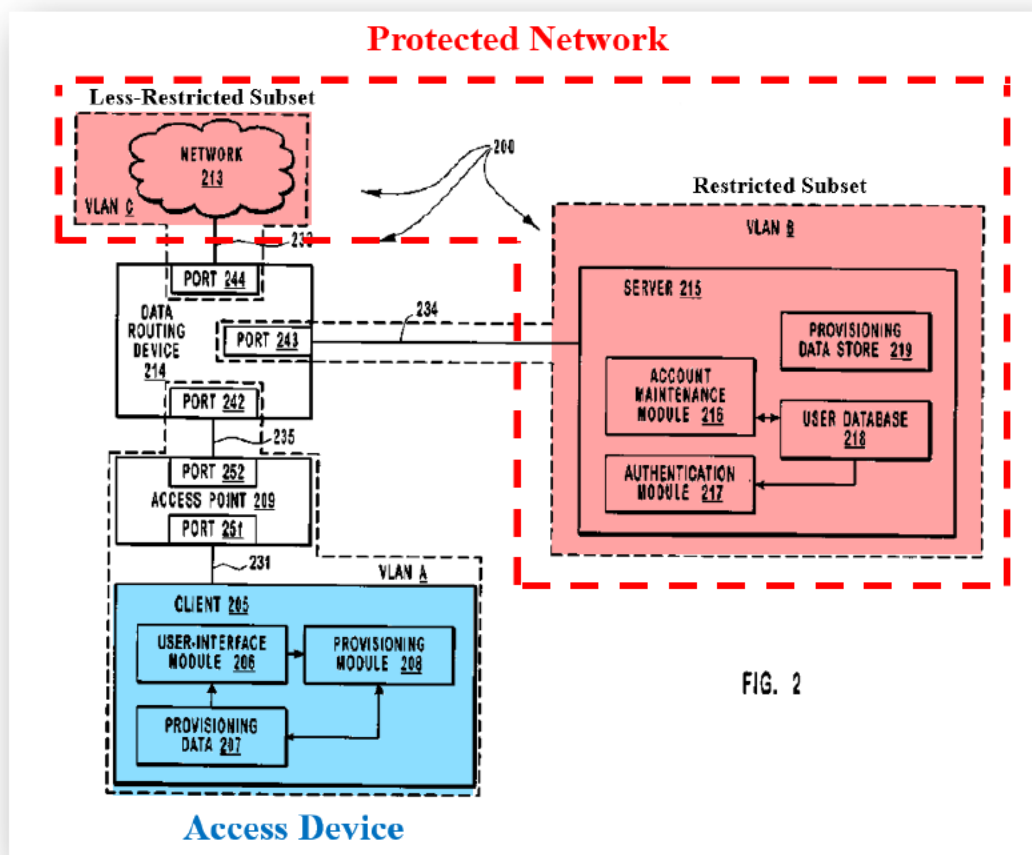
⁴ Authenticating a user can be part of the audit: “[i]n some embodiments, Authenticate User Step [] is considered part of the **security policy** audit.” Ex.1401, 12:9-11.



Ex.1405, Figure 3 (annotated); Ex.1403, ¶80.

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... etc.) from a user at client 205” (*i.e.*, “*applying a security policy*”). Ex.1405, [0104]; Ex.1403, ¶81.

The “*network device*” being audited in Krantz is blue:



Ex.1405, Figure 2 (annotated); Ex.1403, ¶82.

Herrmann additionally discloses this limitation. Herrmann discloses: “policy agent (or integrity agent) 413 to **retrieve information about the current security policy in operation on the client device 310** [“*a security policy*”].” Ex.1406, [0064]. This include “a policy requiring that a **specific virus protection program is operational on each client device** [“*applying a security policy to [a] network device[]*”] that is connected to a network.” Ex.1406, [0012]; Ex.1403, ¶83.

Herrmann explains: “In response to a message from the IGW server 450 (or a subsequent message from the policy agent 413 on the client device 310), **the policy server 460 evaluates whether [] client device 310 has a correct, up-to-date version of the applicable security policy** [*“applying a security policy to [a] network device[]”*].” Ex.1406, [0067]; Ex.1403, ¶¶84-85. A POSITA would have been motivated to combine Krantz and Herrmann for the reasons stated in §VII.C.

ii. ***[1.1] performing an authentication of a device connected to an access point;***

Krantz discloses: “[a] client sends credentials to the server to attempt to **authenticate with the server** [*‘authentication of a device’*].” Ex.1405, [0016]. For instance, “[s]ending 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** [i.e., the *‘device [is] connected to 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... **The access point** may also be configured to block communications from the client that use protocols other than EAP and 802.1X.” Ex.1405, [0018]; Ex.1403, ¶86.

Krantz discloses “perform[ing] an authentication.” Server 215 is in gray below (“gatekeeper” as discussed for [1.3]):

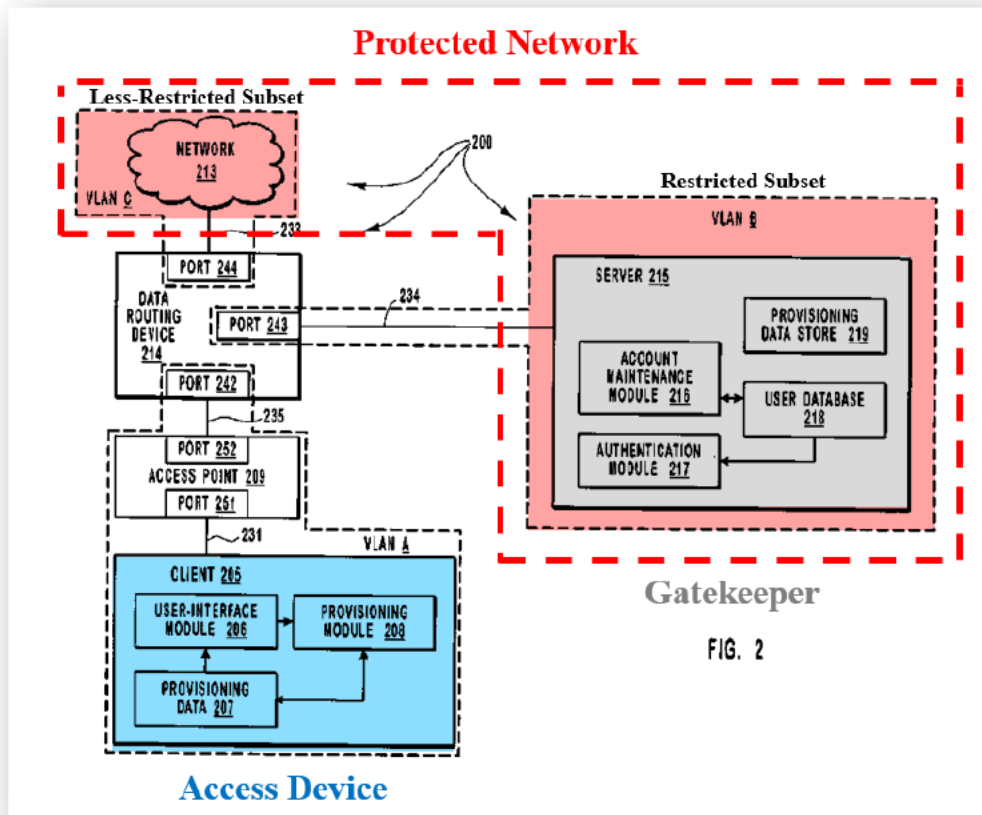


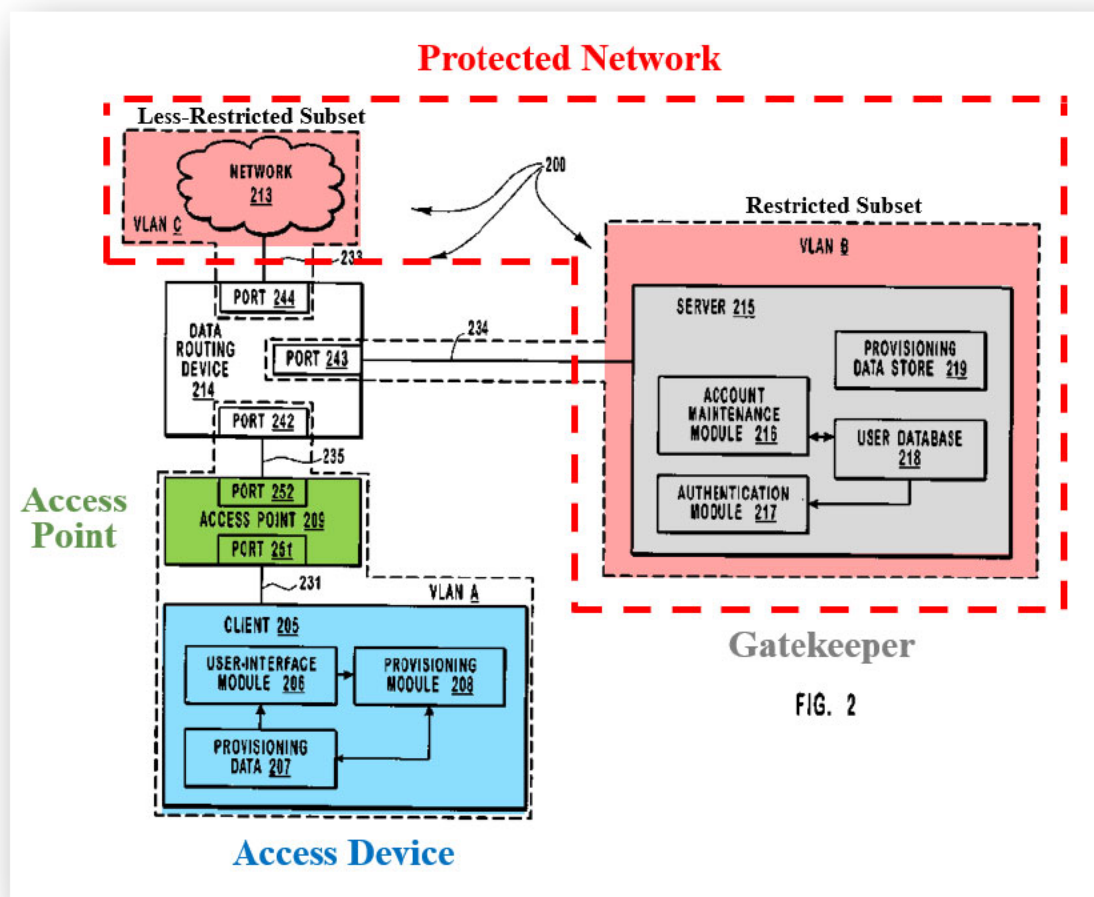
FIG. 2

Ex.1405, Figure 2 (annotated); Ex.1403, ¶87.

Krantz discloses: “performing an authentication” of network devices can occur multiple ways, e.g.: exchanging user-identifiers/passwords, **EAP-messages** to pass certificate keys, as well as cipher suites, etc. Ex.1405, [0073] (“**Server 215 can receive the EAPOL packet []** transferred to authentication module 217 for authentication. Alternately, **access point 209 and/or data routing device 214** may

[] encapsulate the **EAP-Response/Identity message within an EAP-RADIUS message** that is transferred onto VLAN B. Thus, if logical communication link 234 includes other RADIUS servers, **the EAP-Response/Identity message** can be transferred through these other servers to server 215.”); [0074] (“Depending on... **EAP type, server 215 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**. 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.”); *see also*, Ex.1405, [0058], [0067]-[0072], [0078], [0099]-[0101]; Ex.1403, ¶88.

The “*network device*” in Krantz is “*connected to an access point*”—annotated in green:



Ex.1405, Figure 2 (annotated); Ex.1403, ¶89.

Krantz explains: “[n]etwork architecture also includes access point 209. Access point 209 can be a wired or wireless access point that facilitates communication between client 205 [“device connected to an access point”] and data routing device 214... access point 209 is connected to client 205 by corresponding

logical communication link 231⁵ [direct connection between ‘*network device*’ and ‘*access point*’]... Access point 209 includes ports 251 and 252. Data can be transferred between [access point] 209 and client 205 through port 251.” Ex.1405, at [0063]; Ex.1403, ¶90.

Krantz discloses: “MSChap V2 Parameters [] can be included in a configuration sub-file to indicate **whether or not operating system credentials should be used for authentication**,” i.e., the method “*perform[s] an authentication*.” Ex.1405, [0099]; Ex.1403, ¶92. Krantz explains that both **EAP-TLS and EAP-MSCHAP V2** can be required from clients seeking access/authorization. Ex.1405, [0099]; Ex.1403, ¶93.

A POSITA would have understood the above techniques in Krantz can authenticate the device/user of client 205 (“*performing an authentication of a device*.”) before authorization is granted, e.g.:

EAP-TLS. TLS (SSL) is the encryption method... The computer first authenticates to the network... PEAP-MSCHAPv2 uses machine and user credentials for authentication... credentials, carried inside MSCHAPv2, are used for client-to-server authentication.

⁵ Ex.1403, ¶91 (discussing properties of link 231).

Ex.1417, 2; Ex.1403, ¶¶94-95.

iii. *[1.2] scanning the device to collect information regarding the device;*

The security policy may include “**scanning** Access Device 230 for malicious code.” “Scanning” means gathering/collecting relevant information from the device. Ex.1403, ¶¶96-97. Krantz discloses gathering information, e.g., “client 205 and server 215 **exchange EAP-messages** to pass certificates, keys, and supported cipher suites... other credential information may also be **exchanged**...” Ex.1405, [0074]; Ex.1403, ¶98.

The “*network device*” (in blue) includes “provisioning data” 207:

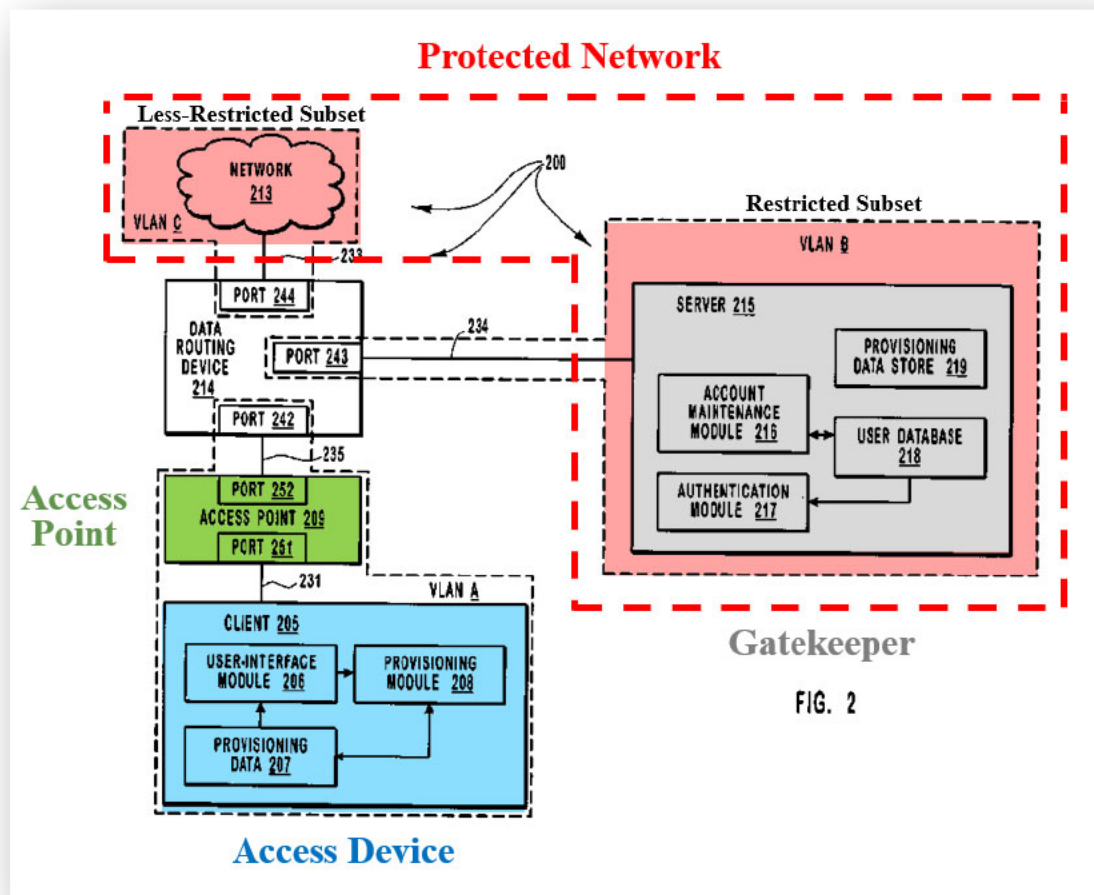


FIG. 2

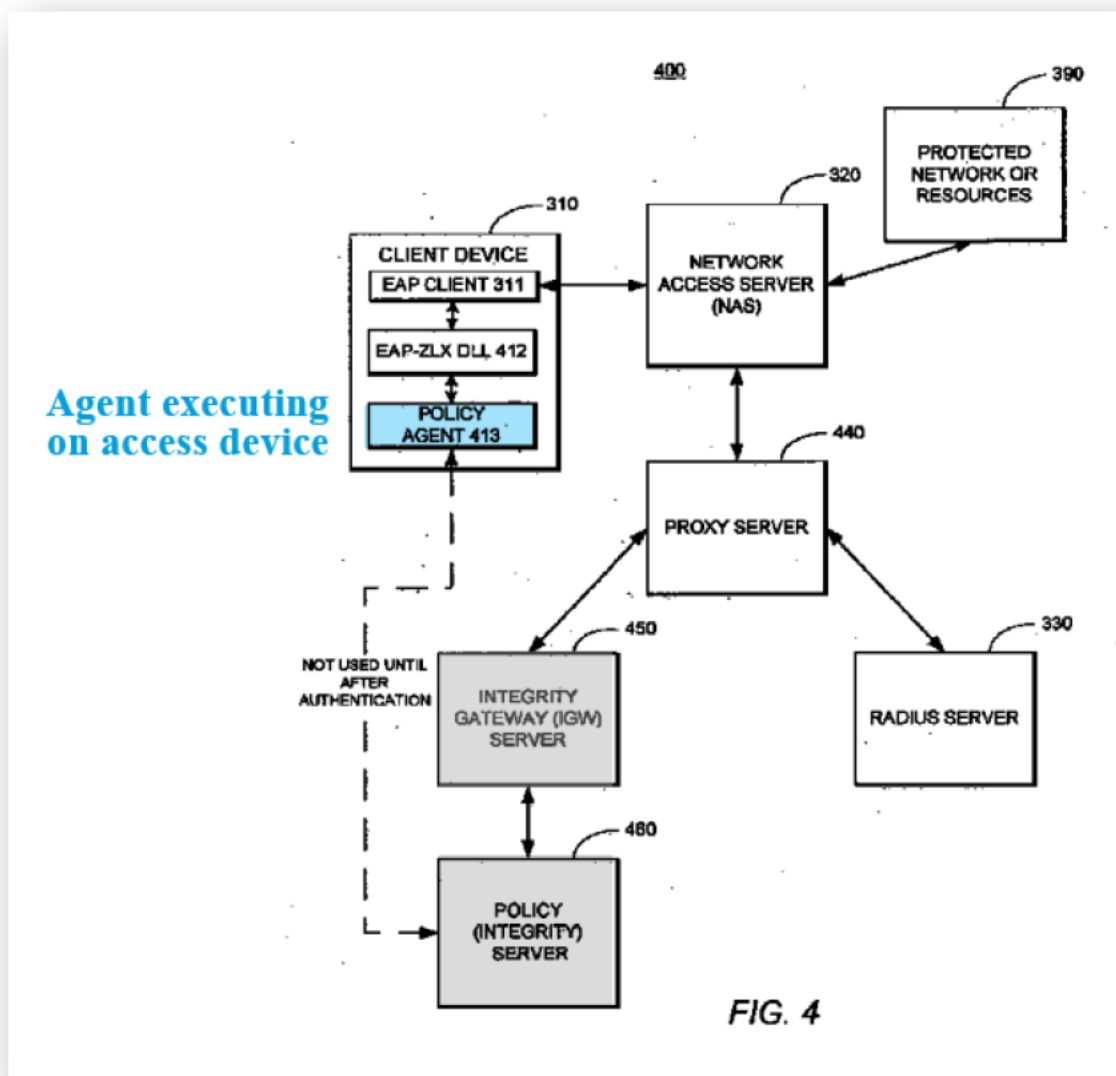
Ex.1405, Figure 2 (annotated); Ex.1403, ¶99.

Master documents and sub-files can be stored in provisioning data 207 (i.e., on the network device): **“Downloaded master documents and sub-files can be stored in provisioning data 207.”** Ex.1405, [0085]; *see also*, Ex.1405 [0090] (indicating “[r]eceived configuration sub-files can be stored in provisioning data 207 and processed by provisioning module 208 to configure client 205 for operation on a particular network.”); Ex.1403, ¶100.

This data/information determines network access, e.g., handshake protocols may be used between access device and gatekeeper (which can gather information about the device for network authentication). Ex.1405 [0099]; *see also*, Ex.1405, [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.1405, [0073] (EAP messages can be transferred via communication link 234). Thus, a POSITA would have recognized Krantz discloses “*scanning the device to collect information regarding the device*” because information is gathered from both the configuration sub-file and other device information is gathered, such as the operating system credentials of the device. Ex.1403, ¶101.

A POSITA would have understood “*scanning the device to collect information regarding the device*” (EAP-messages, operating system credentials, certificates, keys, and supported cipher suites, etc.) could be done by an agent on the device. Krantz does not state an agent is used, but it would have been obvious in view of Herrmann to do so, and a POSITA would have been motivated to combine Krantz and Herrmann for the reasons stated in §VII.C; Ex.1403, ¶102.

Herrmann discloses a “POLICY AGENT 413” (“*agent*”) (blue) on client device:



Ex.1406, Fig. 4 (annotated); Ex.1403, ¶103.

Herrmann discloses a “policy agent (or integrity agent) 413 to **retrieve information about the current security policy in operation on the client device 310** [“scanning the device to collect information regarding the device”].” Ex.1406, [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.1406, [0067]. A POSITA would understand that to “evaluate” the device, information regarding the device must be scanned (“*scanning the device to collect information regarding the device.*”). Policy server is notified by client, containing policy agent 413, through periodic status messages (“IA_HEARTBEAT(s)”) to authenticate the device. Ex.1406, [0080], [0098]. Herrmann’s disclosure of a policy agent retrieving information about network device and sending to a policy server is consistent with the 450 Patent’s disclosure of software agents configured to monitor local security and report results to a policy auditor. Ex.1401, 11:60-64; Ex.1403, ¶104.

A POSITA would have been motivated to add the security policy agent of Herrmann to the client device of Krantz. See, §VII.C. For example, two stated goals of Krantz involve automation and security. Ex.1405, [0014]; Ex.1405, [0019]. Thus, a POSITA would have recognized the policy agent of Herrmann would be complimentary to Krantz, as it would provide an automated means of network security. Ex.1403, ¶105.

Moreover, there would be a reasonable expectation of success in adding the policy agent of Herrmann to Krantz’s client device, as Herrmann describes policy

agent as a “client-side component” communicating with an “EAP-ZLX extension DLL [which] is an implementation of the EAP protocol [used] to provide support for security policy negotiation and enforcement.” Ex.1406, [0064]; *see also*, Ex.1406, [Fig. 4]. This is the same protocol utilized in Krantz. *See, e.g.*, Ex.1405, [0018] (“Sending... an [] (‘EAP’) Response/Identity message...”). This modification to Krantz could be a simple software modification to include a policy agent. Ex.1403, ¶¶106-108.

iv. ***[1.3] applying a security policy, the security policy including one or more requirements pertaining to the authentication and the information, the application of the security policy taking place in response to a gatekeeper, and***

a. ***applying a security policy . . . the information***

The Krantz gatekeeper may enforce/“*apply*” *security policies*, which can include “*one or more requirements pertaining to the authentication and the information.*” For instance, “[i]t may also be that **client 205 and server 215 exchange EAP-messages to pass certificates, keys, and supported cipher suites [‘information’]**. Depending on the EAP type, **other credential information may also be exchanged** between client 205 and server 215.” Ex.1405, [0074]; Ex.1403, ¶109.

Krantz discloses other examples—“[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** [security policy includes ... ‘*at least one requirement pertaining to the information*’] should be used **for authentication** [security policy includes ... ‘*at least one requirement pertaining to the authentication*’].” Ex.1405, [0099]; *see also*, exemplary XML configuration schema at [0091]; *see also*, Ex.1405 [0013], [0032], [0072], [0078] (other security policies include requiring user to download provisioning files); Ex.1403, ¶110.

Krantz discloses applying other security policies such as user-identifier and password. Ex.1405, [0076]; *see also* Ex.1405, [0074] (EAP used to authenticate, including through “certificates, keys, and supported cipher suites.”). Like Krantz, the 450 Patent describes requirements related to user identification/passwords and configuration requirements related to access devices (e.g., aspects of the operating system) (Ex.1401, 6:42-56), to authenticate an access device, or user, of the device. Ex.1401, 11:65-12:11; Ex.1403, ¶111.

The Krantz/Herrmann system would include “*one or more requirements pertaining to the authentication and the information*” (about the network device) such as requiring a particular antivirus software be installed on the device.

Herrmann discloses: “**It becomes critical... to promptly update anti-virus applications on all machines in a network...**” Ex.1406, [0012]; Ex.1403, ¶112. Thus, “a network administrator **may require all users accessing the network to implement a virus definition update (e.g., DAT file) []** targeted at a particular virus.” Ex.1406, [0071]. This may be implemented using security rules and **checking system data [network device “information”] to ascertain device compliance.** Ex.1406, [0068]. Ex.1403, ¶113.

A POSITA would have been motivated to combine Krantz with Herrmann (§VII.C) for reasons explained above, e.g., Krantz’s server 215 (“*gatekeeper*”) would check anti-virus software like Herrmann’s policy server. Ex.1406, [0012], [0068]. A POSITA would be motivated to add anti-virus requirements because Krantz focuses on network authentication/security. Ex.1405, [Abstract]; Ex.1403, ¶114.

b. *applying a security policy ... a gatekeeper*

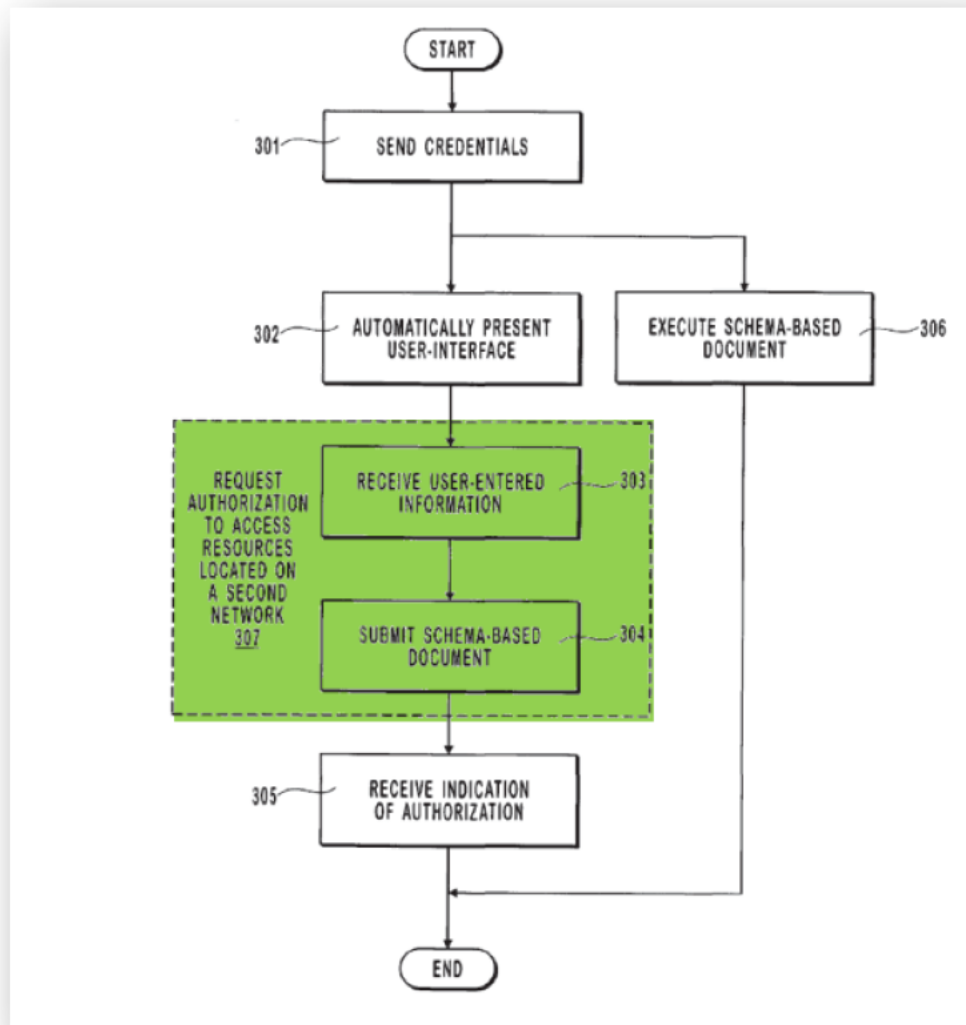
Krantz’s “*security polic[ies]*” can be “*appl[ied]*” and “*tak[e] place in response to a gatekeeper.*” Krantz discloses that “[d]epending on the particular EAP type, server 215 [*‘gatekeeper’*] can respond to the EAP-Response/Identity message in a variety of ways. Server 215 **may request that client 205 provide a password** [*‘security policy’*] that is associated with a user-identifier. A user of client 205 **can**

respond [*‘in response to a gatekeeper’*] by providing a password to server 215.” Ex.1405, [0074]; Ex.1403, ¶115.

Regarding Figure 2, Krantz discloses: “[w]hen credentials are sent to **server 215** [“*gatekeeper*”], **authentication module 217** can receive the credentials (e.g., user-identifier and password) **and compare the credentials to entries in [user database]. If credential information matches an entry in [user database], the identity of a user is authenticated** [“*applying of the security policy*”] ... If an authenticated user of client 205 is authorized to access resources located on VLAN C [] client 205 can then be authorized to access resources located on VLAN C.” Ex.1405, [0076]. Additionally, this “*security policy*” is applied in response to the client requesting access to resources on VLAN C. *See, e.g.*, Ex.1405, [0016-0018], [0071]-[0072], [0076], [0104]-[0109]; Ex.1403, ¶116.

Figure 3 of Krantz “[illustrates] method 300 for provisioning a computer system... described with respect to components depicted in network architecture 200.” Ex.1405, [0070]. Krantz discloses: “method 300 includes a functional, result-oriented step for **requesting authorization to access resources located on a second network (step 307).**” Ex.1405, [0104]. Krantz explains: “[s]tep 307 may include any corresponding acts for accomplishing the result of requesting authorization to access resources located on the second network.” Ex.1405, [0104]. Regarding

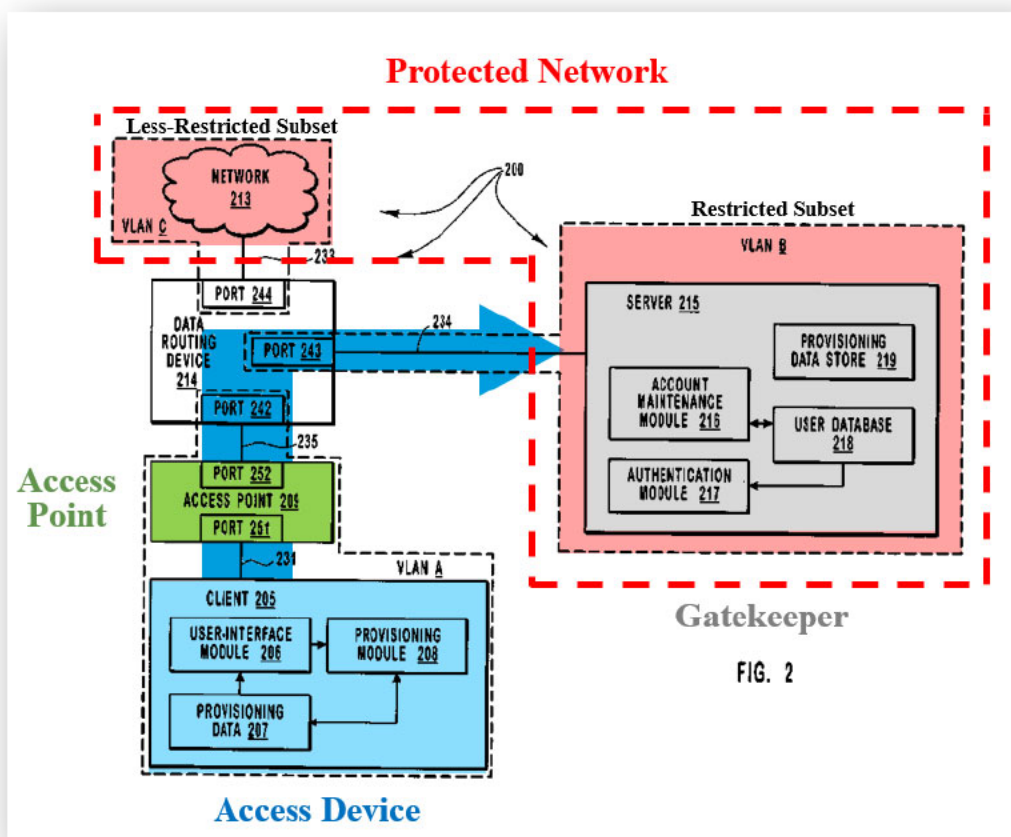
method 300, “[c]lient 205 can respond to [an] EAP-Response/Identity message that can include a User-Identifier.” Ex.1405, [0071].



Ex.1405, Figure 3 (annotated); Ex.1403, ¶117.

Krantz explains: step 307 “includes [the] corresponding act of receiving user-entered information (act 303). A **presented user-interface** can [] receive user-entered **information** [] from a user at client 205” and step 307 further includes “a

corresponding act of **submitting a schema-based document** (act 304). Ex.1405, [0104]. This can include a client **submitting** a first schema-based document that includes user-entered **information to a server**... [*‘in response to a gatekeeper’*].” Ex.1405, [0105]. The “*device*”—“Client 205”—sending “*information*” to the (“*gatekeeper*”) in Krantz is depicted in Figure 2:



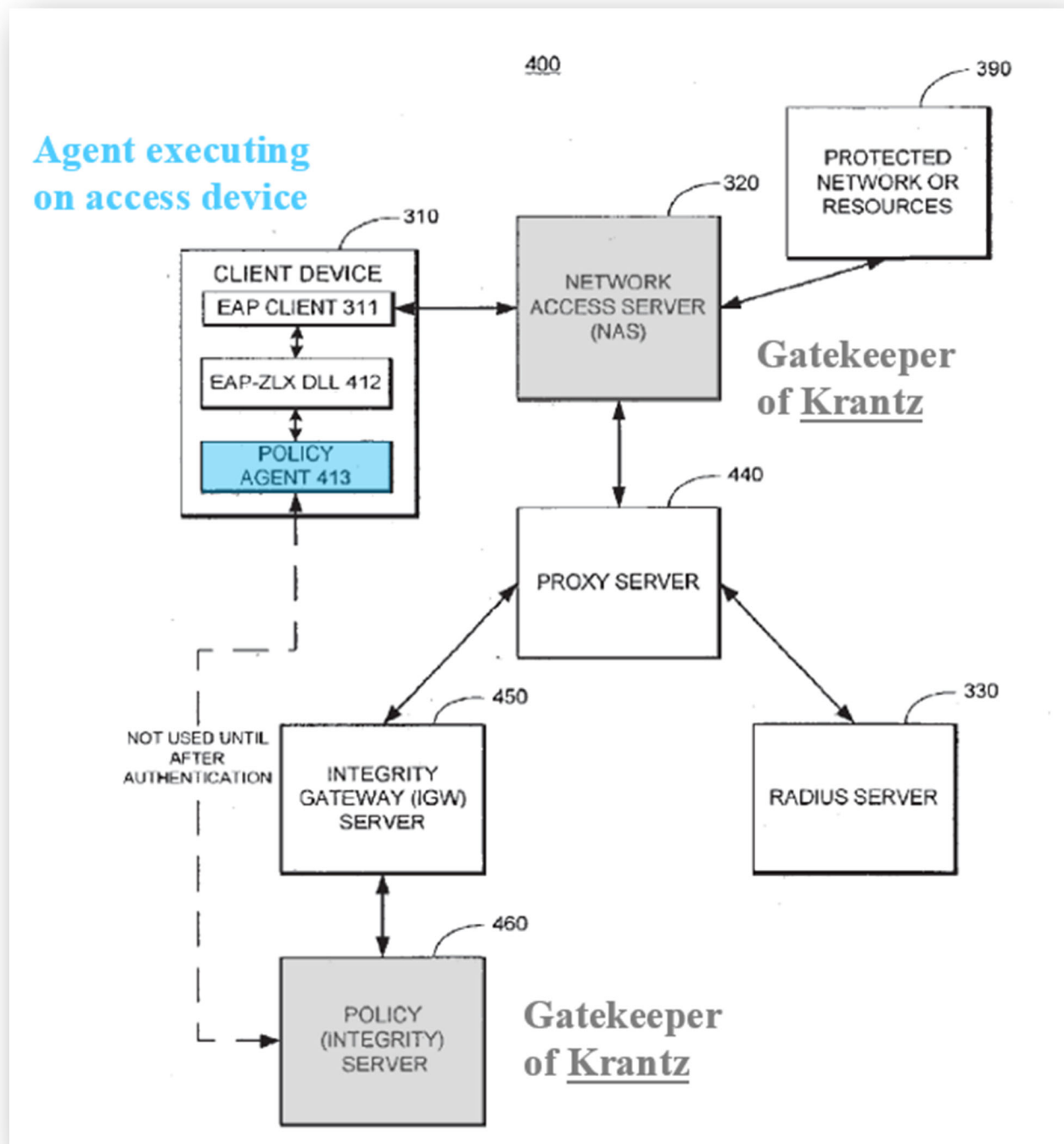
Ex.1405, Figure 2 (annotated); Ex.1403, ¶118.

It would have been obvious to implement “*the application of the security policy taking place in response to a gatekeeper*” as found in Herrmann, in the

gatekeeper of Krantz. Herrmann explains: “policy server 460... ensures that all users accessing a particular system or network comply with specified security policies [...]... 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] client device 310 has a correct, up-to-date version of the applicable security policy** [i.e., ‘*application of the security policy*’].” Ex.1406, [0067]. The “proxy server 440 and IGW server 450 operate to detect and route communications of interest to the policy server 460 to enable the policy server 460 to enforce policy requirements.” Ex.1406, [0073]. For instance, “proxy server 440 [may] issue[] a policy challenge to the client... and **[t]he client responds**” accordingly [“*taking place in response to a gatekeeper*”]. Ex.1406, [0077]; Ex.1403, ¶119.

Herrmann’s server components are like Krantz’s gatekeeper of Krantz. Herrmann explains: “a network access server (NAS) 320... acts as an access point (**i.e., gateway**) to a group of resources or collection of data (e.g., the protected network resources 390) and accepts requests for access to such resources from client machines.”). Ex.1406, [0053]; *see also*, Ex.1406, [0065] (describing “policy (integrity) server” as a “server-side component” and that it may “act on [] communications to **determine whether or not the client device 310 is in**

compliance with applicable security policies...” like the server 215 gatekeeper of Krantz. Moreover, Herrmann and Krantz discuss logical implementations of disclosed server techniques, thus policy (integrity) server 460 of Herrmann would easily integrate with Krantz:



Ex.1406, Fig. 4 (annotated); *see also*, Ex.1405, [0038], [0051] (describing logical communication links/logical representations of computer systems); Ex.1406, [0026] (describing invention as “a [standardized] logical structure for communication systems...”); Ex.1403, ¶¶120-121.

v. ***[1.4] configuring the access point in response to a result of applying the security policy.***

Krantz discloses: “*access point*” is a wireless access point that enables access to wired computer systems on VLAN B (e.g., server 215) and VLAN C (e.g., computer systems included in network 213).” Ex.1405, [0064]; Ex.1403, ¶¶122-123.

Mapping #1

First, Krantz explains: “if an authenticated user of client 205 is authorized to access resources located **on VLAN C**... client 205 can... access resources located on VLAN C.” Ex.1405, [0076]. As explained, Krantz discloses utilizing “*security polic[ies]*” including the use of user-identifiers and passwords. Ex.1405, [0076]. After applying these security policies, an authenticated client is configured to access resources (“*in response to a result of applying the security policy*”), i.e., the access point allows client to access resources on VLAN C. Ex.1405, [0076-0078]; Ex.1403, ¶124

The “*security policy*” is applied in response to client requesting access to resources on VLAN C. Ex.1405, [0016-0018], [0071]-[0072], [0076], [0104]-[0109]. Thus, after the requirements of the security policy are satisfied (i.e., “*in response to a result of applying the security policy,*”) the access point facilitates transfer of data between client 205 (the access “*device*”) and, ultimately VLAN C (“*configuring the access point*”). Ex.1405, [0063]-[0064]. As shown below, “*configuring the access point*” allows access to VLAN C.

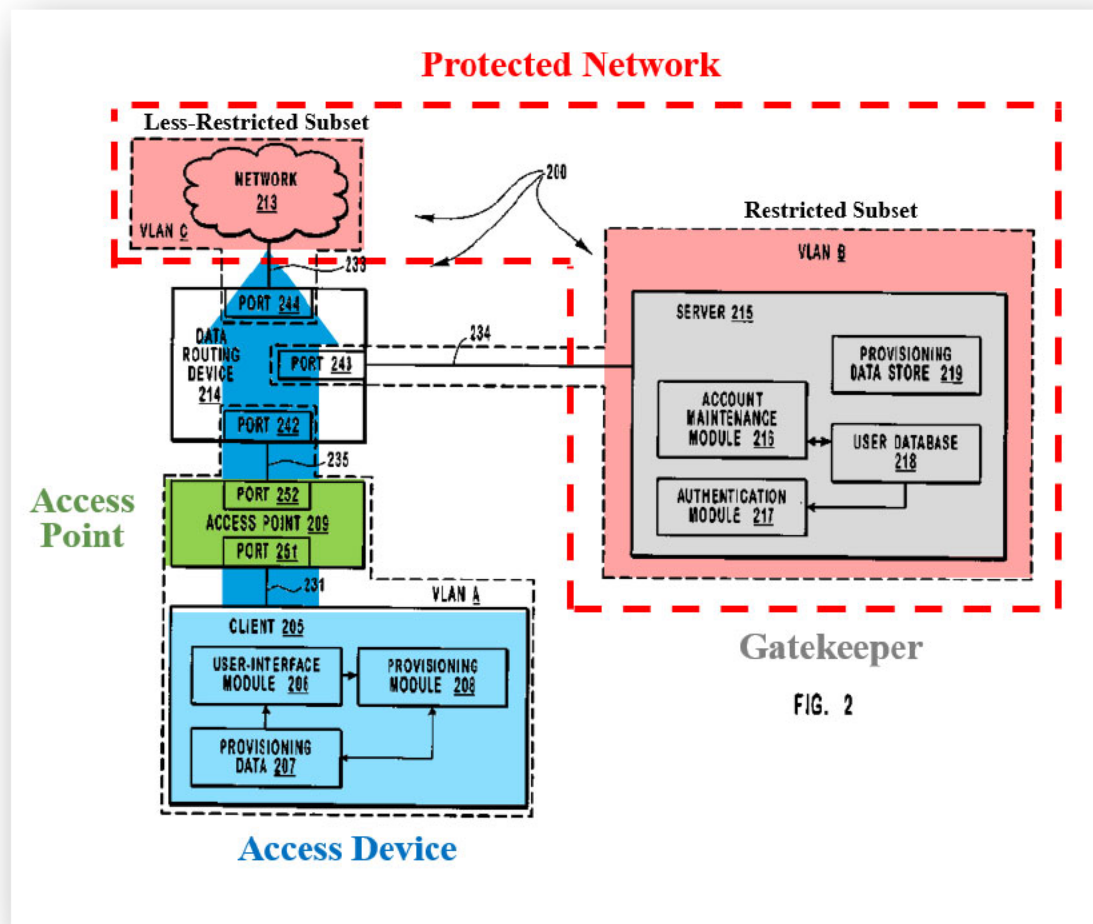


FIG. 2

Ex.1405, Figure 2 (annotated); Ex.1403, ¶125.

Mapping #2

Second, “[a]ccess point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 [] that are to be transferred to VLAN B and/or VLAN C.” Ex.1405, [0064]; *see also* Ex.1405, [0061]; *see also* Ex.1405, [0023]; Ex.1403, ¶126.

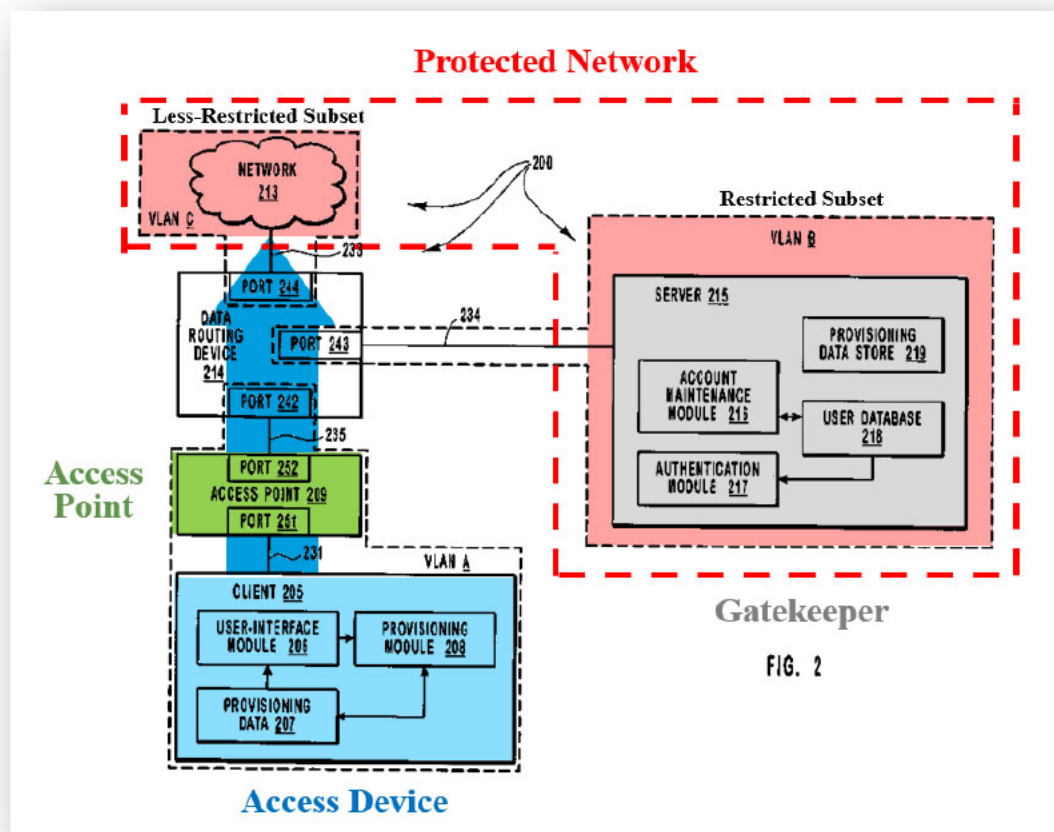
Krantz is thus explaining that when configured as a “VLAN aware device,” Krantz’s “*access point*” is “*configured*” because Access Point 209 (via Port 251) will insert VLAN Tag Headers into incoming data frames from a client **that may now access VLAN C**. Ex.1405, [0107]. Access Point 209/Port 251 is “*configure[ed]*” **because it previously** tagged incoming data from client 205 with headers enabling access to **VLAN B**. Ex.1403, ¶127.

Additionally, “[w]hen client 205 is authorized to access resources located on VLAN C, access point 209 may enable [] protocols [] 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 can send commands to access point 209 to cause access point 209 [] to insert appropriate Tag Headers.” Ex.1405, [0107]. Configuring input ports in VLAN aware devices to tag incoming data was a well-known technique to POSITAs by 2003. Ex.1407, 11 (Table 5-1); Ex.1408, 4:42-47; Ex.1409, 16:4-13; Ex.1410, p.210; Ex.1403, ¶128.

Moreover, Krantz explains: “data routing device 214 can [] separate computer systems into different VLANs. As depicted in FIG. 2, **data routing device 214 has been configured to separate network architecture 200 into VLANs A, B, and C**. Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.” Ex.1405, [0060]; *see*

also Ex.1405, [0064] (“**Access point 209 can be configured** as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to **VLAN B and/or VLAN C.**”). Accordingly, by configuring the flow of data in this manner, the “*gatekeeper*” (server 215) may apply security policies to authorize the access device access to data—such as the resources on VLAN C. Ex.1405, [0062]; Ex.1403, ¶129.

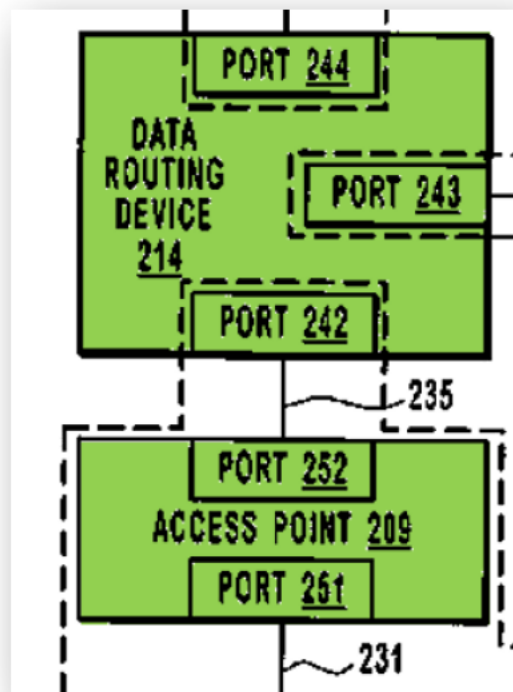
Several “*security polic[ies]*” can be applied, such as exchanging a user-identifier and password, EAP-messages to pass certificate keys, as well as cipher suites. Ex.1405, [0074], [0076]. Once applied, “the identity of a user is authenticated... **If an authenticated user of client 205 is authorized to access resources located on VLAN C [], client 205 can then be authorized to access resources located on VLAN C.**” Ex.1405, [0076]. Thus, a POSITA would understand “*access point*” is “*configured*” (Ex.1405, [0053]) when audit data demonstrates that access “*device*” is audited appropriately. The communication path for an authorized access “*device*” would flow through “communication port” 244 (of Data Routing Device):



Ex.1405, Fig 2 (annotated); Ex.1403, ¶130.

Mapping #3

To the extent asserted that Krantz does not expressly disclose “*configuring the access point...*” it would have been obvious to implement the Data Routing Device disclosure of Krantz within Access Point 209 itself. Access Point 209 is connected to Data Routing Device 214, and both include communication ports, e.g., 235 is a logical communication link connecting the two. Ex.1405, [0060].

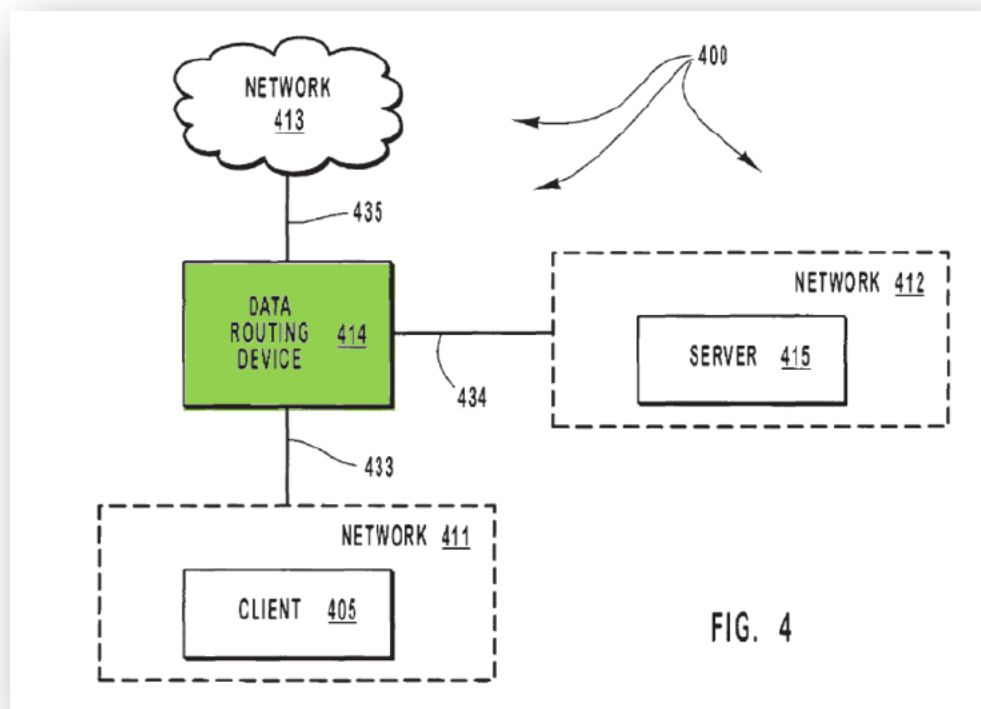


Ex.1405, Figure 2 (annotated). Krantz discloses: “data routing device 214 can be configured to separate computer systems into different VLANs [e.g.,] **VLANs A, B, and C**. Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.” Ex.1405, [0061]; Ex.1403, ¶¶131-133. For example, Krantz states that:

Data routing device 214 logically represents [] for example, a router and/or a switch, **that can determine how to transfer data between the ports included in data routing device 214...** 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)...

Ex.1405, [0059]; *see also*, e.g., Ex.1405, [0060]; *see also generally*, Ex.1405, [0064]. A configuration sending data to VLAN C (the “*network*” that has controlled access) would be pursuant to a security policy requiring authorization and authentication as described in Krantz. Ex.1403, ¶134.

A POSITA would have found it obvious that the functionality of “data routing device 214” could be implemented **at the access point itself** as data routing device is merely a “logical representation” of, e.g., a router and/or switch. Ex.1405, [0059]. Indeed, Krantz contemplates combining the functionality in a single physical/logical representation. Figure 4 demonstrates such functionality can be readily combined with the data routing device as the access point:



Ex.1405, Figure 4 (annotated); Ex.1403, ¶¶135-136.

In particular, Krantz explains that:

Data routing device 414 logically represents a computer system... **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.1405, [0051]; Ex.1403, ¶137.

Krantz discloses: “[d]ata routing device 214 **logically represents** a special-purpose computer system...” (Ex.1405, [0059]), thus a POSITA would understand that this “logical” architecture could be implemented in a single device (access

point). Krantz explains such a logical implementation would include functionality enabling a “data frame” to be “transferred in and out of data routing device 214 **at the same port.**” Ex.1405, [0059]. Krantz repeatedly describes “data routing” device and “access point” as having the same functionality. *Compare, e.g.,* Ex.1405, [0060] with [0064]; *see also* [0069], [0073] (describing the same functionality for both the data routing device and access point). Therefore, the functionality can occur at the combined access point/data routing device **or** the access point alone, having no impact on functionality of Krantz system. Using one technique or the other would merely have been a matter of design choice. Thus, it would have been obvious to combine the functionality of the Data Routing Device and Access Point of Krantz in the same device. Ex.1403, ¶¶138-139.

2. [2.0] further comprising facilitating updates to software on the device in response to applying the security policy, using the gatekeeper.

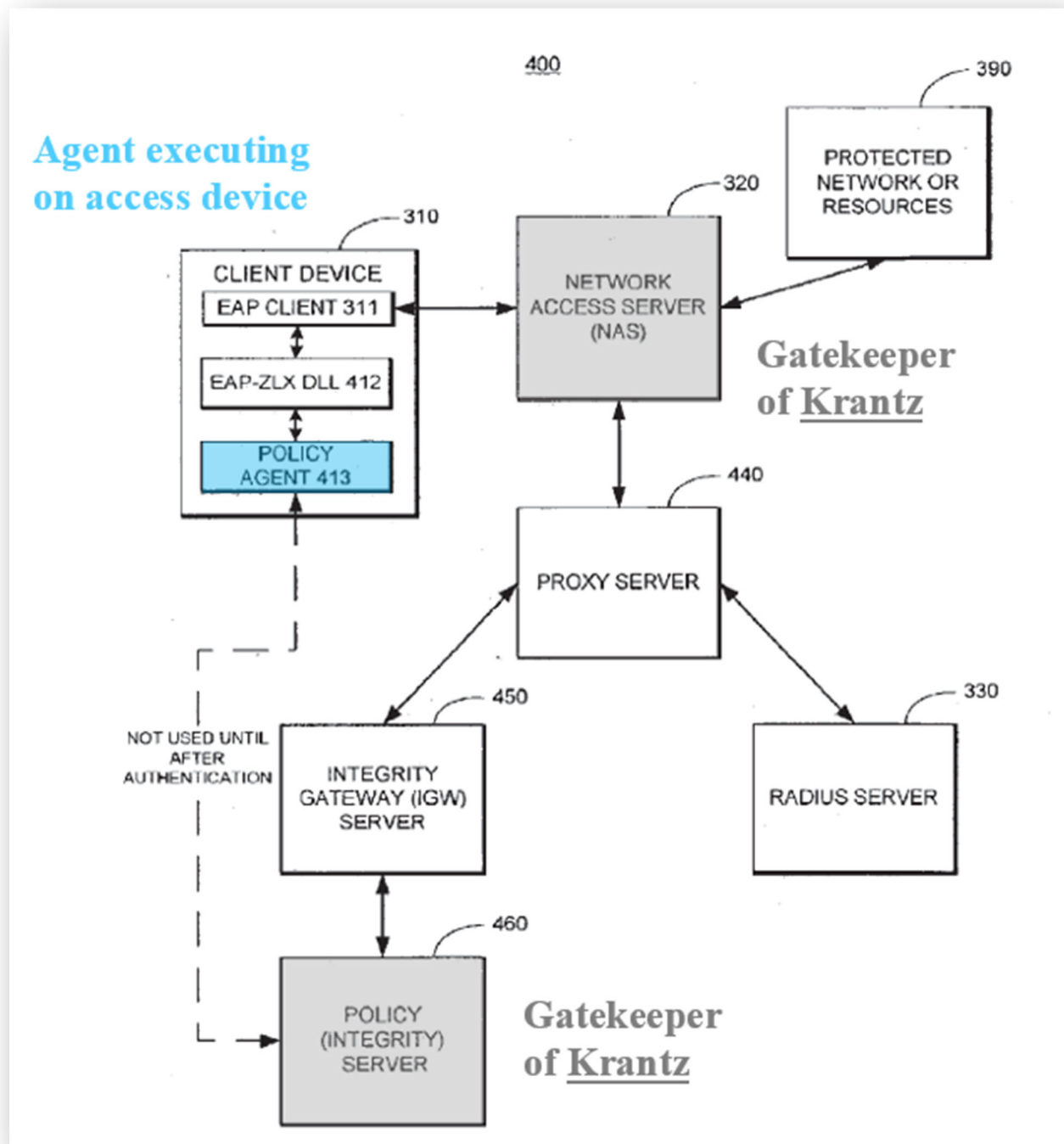
Krantz’s “gatekeeper is used” to “*facilitat[e] updates to software on the device in response to applying the security policy.*” Krantz identifies a problem in the prior art in which “*software incompatibilities must be worked out* by a user.” Ex.1405, [0013]; Ex.1403, ¶¶140-141.

Krantz discusses how connecting devices may require “provisioning files [] for gaining full access to network 413.” Ex.1405, [0056]; *see also*, Ex.1405, [0032],

[0078]. Dr. Houh confirms that provisioning files relate to network connectivity/security. *E.g.*, Ex.1409, [0079]; Ex.1403, ¶142.

Herrmann discloses: “[n]ew viruses are frequently released... It becomes critical [to] **promptly update anti-virus applications on all [network] machines...**” Ex.1406, [0012]; Ex.1403, ¶143. Thus, “network administrator **may require all users accessing the network to implement a virus definition update (e.g., DAT file)** [] targeted at a particular virus.” Ex.1406, [0071] (“*facilitating updates to software on the device in response to applying the security policy.*”). This may be implemented using security rules/checking system data of connecting devices to ascertain compliance. Ex.1406, [0068] (“**[policy server] may enforce [‘using the gatekeeper’]** a variety of different types of security policies or rules... [requiring] particular security or **anti-virus programs.**”); Ex.1403, ¶144.

Policy server 460 of Herrmann is like the gatekeeper of Krantz. Both Herrmann and Krantz discuss logical server implementations and, e.g., policy server 460 of Herrmann would easily integrate with Krantz:

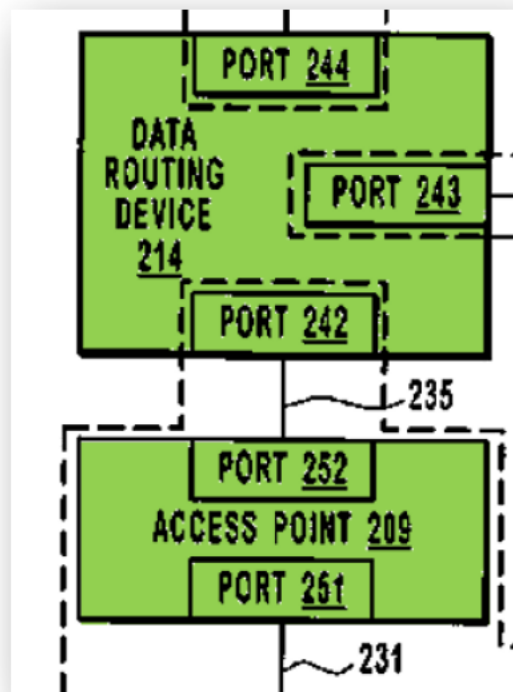


Ex.1406, Fig. 4 (annotated); *see also*, Ex.1405, [0038], [0051]; Ex.1406, [0026]; Ex.1403, ¶145.

A POSITA would have been motivated to include specific virus protection requirements because Krantz focuses on network authentication/security. §VII.C. They would have had a reasonable expectation of success because Krantz already discloses conditions for client access, e.g., “signup”/“renewal” conditions to authorize access. Ex.1405, [0019]. GateKeepers were known to control security policies (Ex.1401, 2:22-39), thus Krantz/Herrmann renders obvious this claim. Ex.1403, ¶¶146-147.

3. [3.0] wherein configuring the access point includes setting an access control list on the access point.

Krantz discloses: “access point 209 [‘*access point*’] is a wireless access point that enables access to wired computer systems on VLAN B (e.g., server 215) and VLAN C (e.g., computer systems included in network 213).” Ex.1405, [0064]; Ex.1403, ¶¶148-149. Krantz discloses: “*configuring the access point*” is involved in and “*includes setting an access control list*.” Data routing device 414 can be part of the Krantz access point. *See* §[1.4].



Ex.1405, Figure 2 (annotated); Ex.1403, ¶150.

Krantz explains: “access to resources located on network 413 can be restricted by [] Internet Protocol (“IP”) filtering. **Data routing device 414** [‘access point’], components in network 411, or components in logical communication link 433 can filter (‘IP’) address to **limit client 405’s access to resources with particular IP addresses**” (Ex.1405, [0053]), i.e., access point and data routing device can be “*configur[ed]*” based on what the client is authorized to access. Ex.1405, [0064] (“[a]ccess point 209 can be configured...”) Ex.1405, [0023] (“[A]ccess point may insert Tag Headers into client data to indicate to the **data routing device** [‘*configur[ed]* access point’] that client data is to be transferred to

the second network.”). Thus, when configured as a “VLAN aware device,” Krantz’s “*access point*” is “*configured*” 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**. Ex.1405, [0107]. Furthermore, Access Point 209/Port 251 is “*configur[ed]*” because it was previously tagging incoming data from client 205, as described above, with headers enabling access to VLAN B. Ex.1403, ¶151.

A POSITA would understand the configuring step could filter utilizing the database/list of clients disclosed in Krantz (*configuring the access point* also includes “*setting*” an *access control list*). Krantz explains: “[w]hen [client] is not authorized... IP addresses can be filtered such that client [can access] resources located on network 412 but [not] network 413. **When [client] is authorized** to access network 413, IP addresses can be filtered such that [client can access] resources [on] networks 412 and 413.” Ex.1405, [0053]. Thus, if client (“*access device*”) is on an authorized list (“*access control list*”) no filtering takes place (i.e., it is part of the “*access control list*” of permitted devices). Dr. Houh explains that limiting server access for specific clients through IP filtering is an “*access control list*” because it “control[s] access to specific devices.” Ex. 1401, 6:33-35; Ex.1403, ¶152.

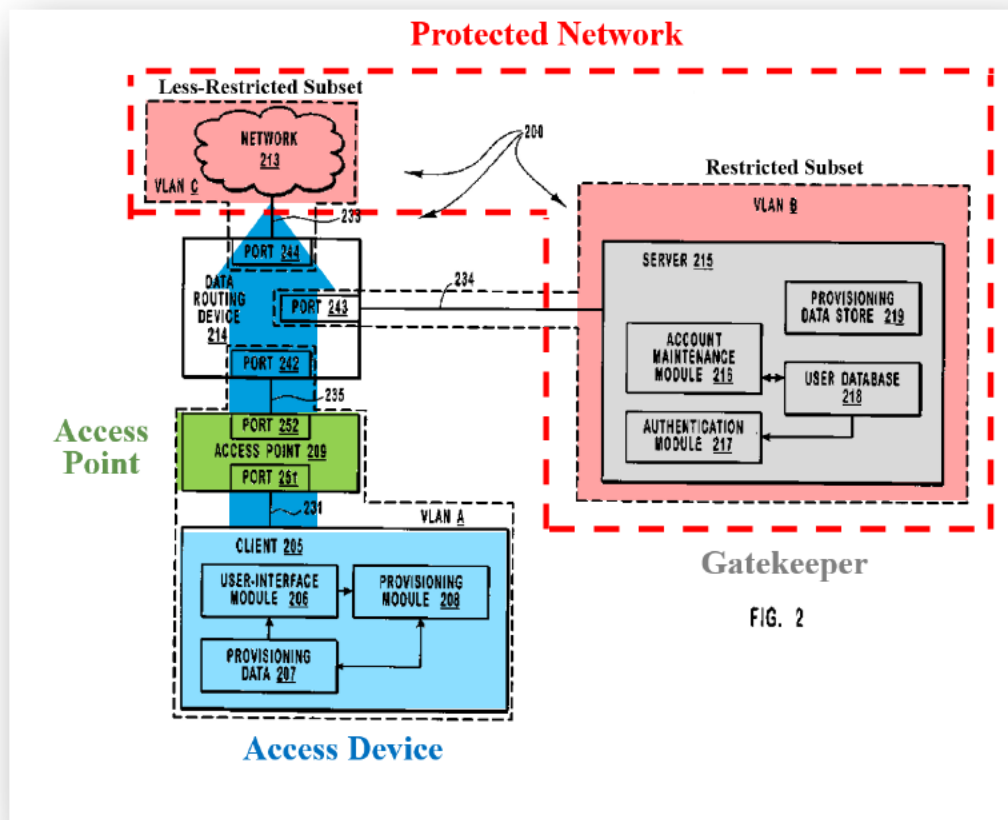
Because the access point/data routing device of Krantz controls access to specific devices it is “*setting an access control list on the access point.*” Krantz’s disclosure is consistent with the 450 Patent, which explains: “**access control lists within Router 220** are optionally used to independently control access to specific devices within Less-Restricted Subset 210.” Ex. 1401, 6:33-35. Similarly, **access point/data routing device** of Krantz independently controls access to specific devices (Ex. 1405, [0061]) because, e.g., Krantz discloses that “[a]ny of the ports included in data routing device 214 (e.g., ports 242, 243, and 244) **can be configured to transfer tagged data frames but drop untagged data frames.**” Ex. 1405, [0062]. Thus, Krantz discloses “*setting an access control list*” occurs “*on the access point.*” Ex.1403, ¶153. A POSITA would have also found it obvious to use an “*access control list*” in a VLAN embodiment to control client access. Ex.1405, [0052]; Ex.1403, ¶154.

Krantz describes additional “*access control list*” techniques, e.g. a database: “authentication module 217 can receive the credentials [] and compare the credentials to entries in [**user database**]. If credential information matches an entry in [user database], **the identity of a user is authenticated...**” Ex.1405, [0076]. A POSITA would recognize this is an “*access control list.*” Ex.1403, ¶155. Moreover, POSITAs would understand device information (e.g., IP addresses) could be stored

in a database like users/usernames because Krantz specifically discusses filtering IP addresses. Ex.1405, [0053]; Ex.1403, ¶¶156-157.

4. [4.0] wherein configuring the access point includes assigning a VLAN.

As discussed for claim [1.4], after “*requirements of the security policy are satisfied,*” the access point facilitates the transfer of data between client 205 (“the access device”) and, ultimately a VLAN, e.g., VLAN C. Ex.1405, [0063]-[0064]. As shown below, Krantz discloses “*configuring access point and assigning access to a VLAN,*” i.e., VLAN C.



Ex.1405, Figure 2 (annotated); Ex.1403, ¶¶158-159.

Krantz explains: “[a]ccess point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C.” Ex.1405, [0064]; *see also* Ex.1405, [0061], [0064]. Ex.1403, ¶¶160-161.

5. ***[7.0] wherein the authentication includes using an EAP protocol.***

Krantz discloses 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 [to] **be authenticated and possibly authorized to access resources located on VLAN C.**” Ex.1405, [0068]. The use of **EAP-TLS** (*e.g.*, Ex.1405, [0067]-[0074], [0100]) was known for authentication. Ex.1416, at 1, 2; *see also*, Ex.1405, [0099]; Ex.1403, ¶¶162-163.

Moreover, Krantz discloses that performing an “*authentication*” of the network device can include exchanging... **EAP-messages...**” Ex.1405, [0073], [0074] (“It may also be that **client 205 and server 215 exchange EAP-messages** to pass certificates, keys, and supported cipher suites...”); *see also*, Ex.1405, [0018], [0058], [0067]-[0072], [0078], [0099]-[0101]; Ex.1403, ¶¶164-165.

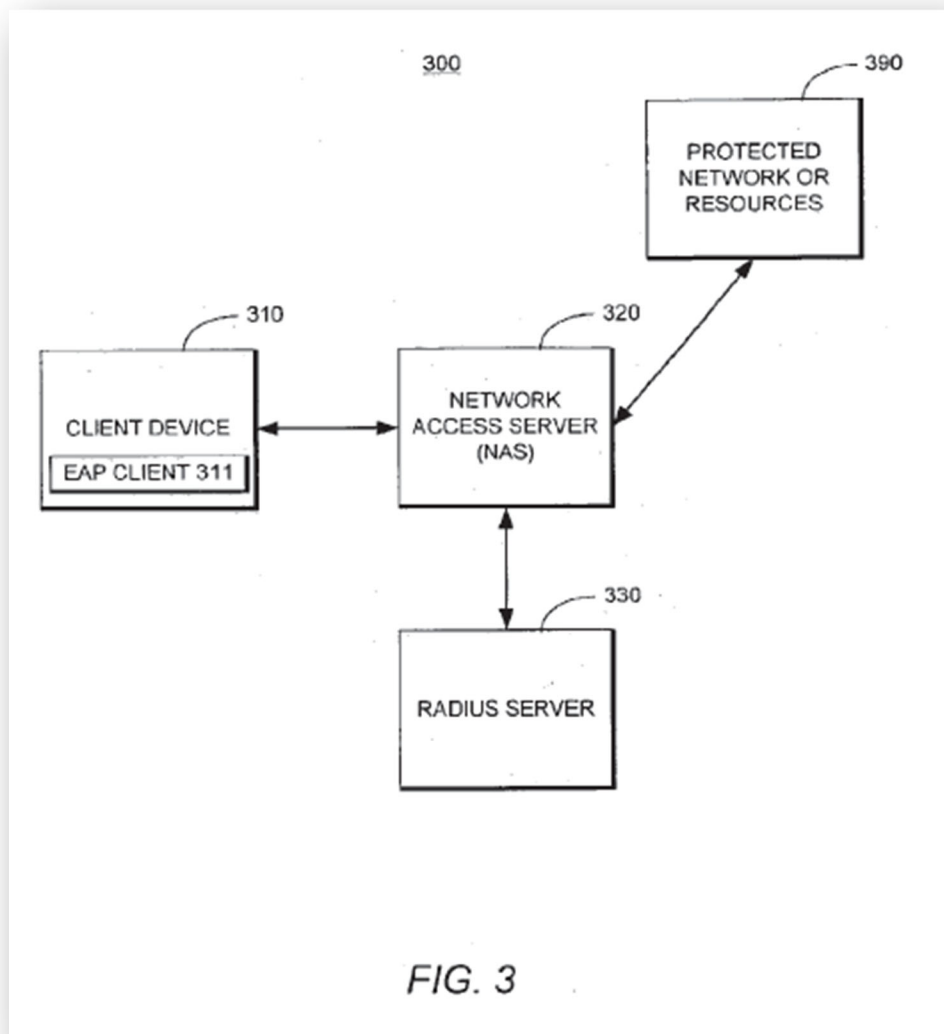
6. ***[8.0] wherein the authentication includes using a RADIUS protocol.***

“RADIUS” stands for “Remote Authentication User Dial-In Service.” Krantz specifically discloses this limitation:

A client sends credentials to the server **to attempt to authenticate with the server. The server can be a Remote Authentication Dial-In User Service (“RADIUS”) server** [...]

Ex.1405, [0016]; *see also* Ex.1405, [0058], (“[S]erver 215 . . . **may support the RADIUS attributes...**”), [0064], [0069], [0073], [0102]; Ex.1403, ¶¶166-167.

Similarly, Herrmann depicts a “network access server environment... [including] a RADIUS server providing authentication services.” Ex.1406, [0053]:



Ex.1406, Figure 3; Ex.1406, [0054], [0055], [0056]; Ex.1403, ¶¶168-169.

7. ***[9.0] wherein one of the requirements pertains to a status of an application on the device.***

Similar to [1.3], Krantz/Herrmann disclose applying a security policy including “*requirements*” pertaining to authentication/information. One requirement

pertains to “*a status of an application on the device.*” Herrmann, discloses: “policy server 460 may enforce [] different types of security policies or rules... [e.g.] requiring that **a specific virus protection program is operational on each client device** [*‘status of an application on the device’*] **that is connected to a network.**” Ex.1406, [0068], [0012]; Ex.1403, ¶¶170-171.

Herrmann discloses: “policy agent [] to retrieve information about the current security policy in operation on the [client device]. The information collected by the policy agent...” Ex.1406, [0064]. “In response... policy server 460 **evaluates whether or not the client device 310 has a correct, up-to-date version of the applicable security policy.**” Ex.1406, [0067]. Policy server is notified by client containing policy agent through “IA_HEARTBEAT(s)” messages to authenticate the device. Ex.1406, [0080], [0098]; Ex.1403, ¶172.

A POSITA would be motivated to modify Krantz to include evaluating additional data requiring a specific “*application on the device,*” (virus protection program), for the reasons discussed *supra*. §VII.C; Ex.1403, ¶¶173-174.

8. [10.0] wherein one of the requirements pertains to a status of an operating system exon [sic] the device.

As discussed for [1.3], Krantz and Herrmann disclose one or more “*requirements*” pertaining to authentication/information. Furthermore, Krantz

discloses that “client 205 and server 215 **exchange EAP-messages...**” Ex.1405, [0074]. A handshake protocol may be used between the device and gatekeeper with data including “*requirements pertain[ing] to a status of an operating system on the device,*” e.g.:

a **configuration sub-file** [is] used to authenticate... included in a configuration sub-file [are parameters regarding] whether [] **operating system credentials** should be used for authentication.

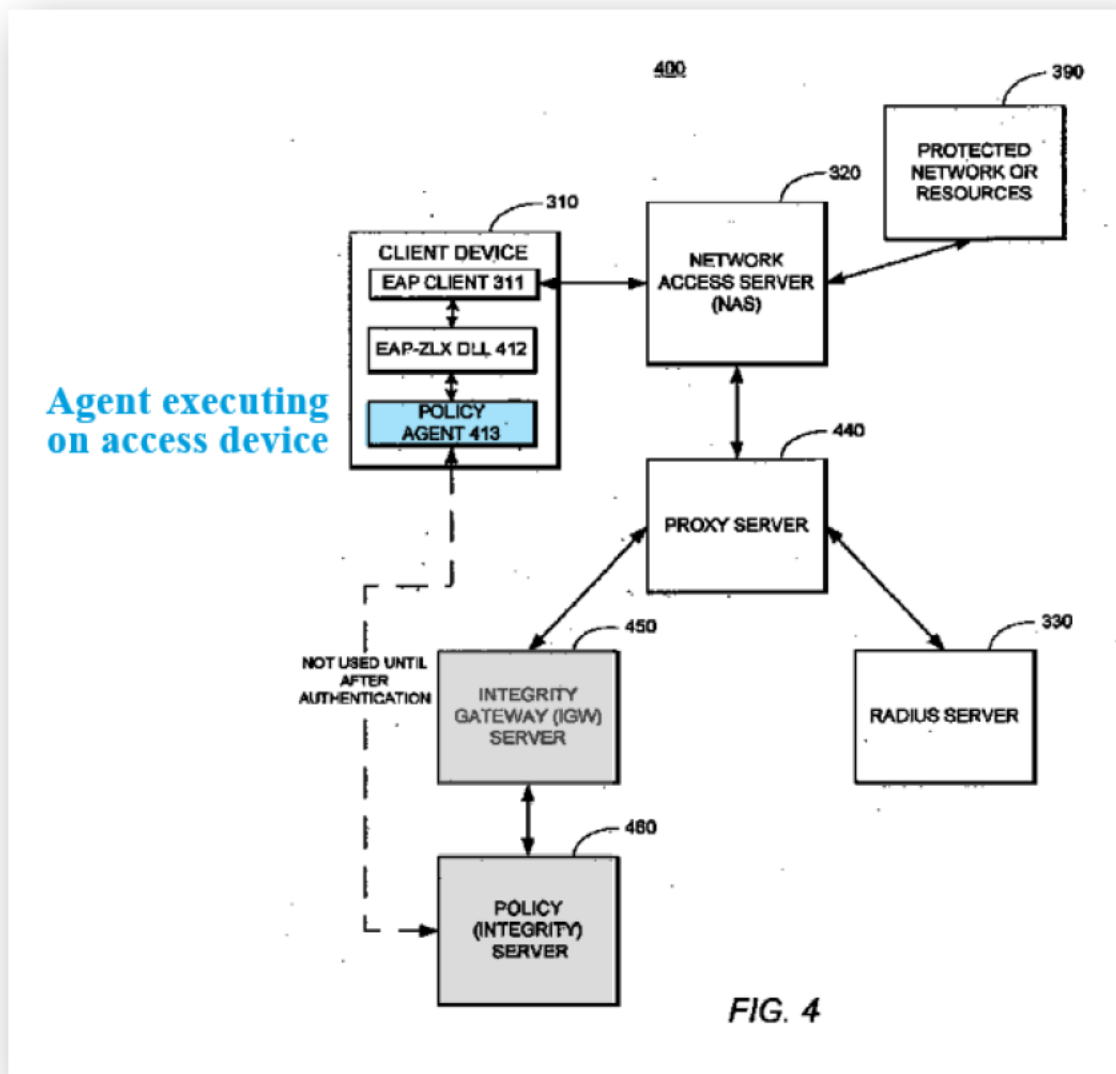
Ex.1405 [0099]; Ex.1403, ¶¶175-178.

9. [14.0] wherein the scanning is performed using an agent on the device.

As discussed *supra* for [1.2], Krantz in view of Herrmann discloses “*scanning the device to collect information regarding the device.*” Ex.1403, ¶179.

“Scanning” is used in its typical sense (gathering/collecting relevant information/data). Ex.1403, ¶180. As discussed for [1.2], Dr. Houh confirms that one way that “*scanning the device*” could be accomplished would be by utilizing an agent on the device and utilizing one would have been obvious in view of Herrmann. A POSITA would have been motivated to combine Krantz and Herrmann (§VII.C). Ex.1403, ¶181.

Herrmann discloses a “POLICY AGENT 413” (i.e., an “*agent*”) on the client access device:



Ex.1406 (Herrmann), Fig. 4 (annotated). Herrmann discloses: “policy agent... retrieve[s] information about the current security policy in operation on the client device 310 [‘scanning the device to collect information regarding the device’].” Ex.1406, [0064]. Herrmann explains: “In response to a message from the IGW server 450 (or [] policy agent 413 []), the policy server 460 evaluates [if] client

device 310 has a correct, up-to-date version of the applicable security policy.” Ex.1406, [0067]. A POSITA would have understood that to “evaluate” the device, device information must be scanned. The policy server is notified by client to authenticate access device. Ex.1406, [0080], [0098]. Herrmann’s disclosure of a policy agent retrieving information about the device and sending to a policy server is consistent with the 450 Patent’s disclosure that a software agent is configured to monitor local security and report results to a policy auditor. Ex.1401, 11:60-64. Moreover, “*the scanning is performed using an agent on the device*” as policy agent 413 is contained in client device 310. Ex.1403, ¶182.

A POSITA would have been motivated to add the security policy agent of Herrmann to the client device of Krantz. See §VII.C. A POSITA would have recognized that the policy agent of Herrmann would be complimentary to Krantz, as it would provide automated means of network security. Ex.1403, ¶183.

Moreover, there would be a reasonable expectation of success for adding Herrmann’s policy agent 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.1406, [0064], [Fig. 4]. This same protocol is utilized in Krantz. Ex.1405, [0018].

Additionally, this modification can be implemented as a simple software modification to include a policy agent. Ex.1403, ¶¶184-185.

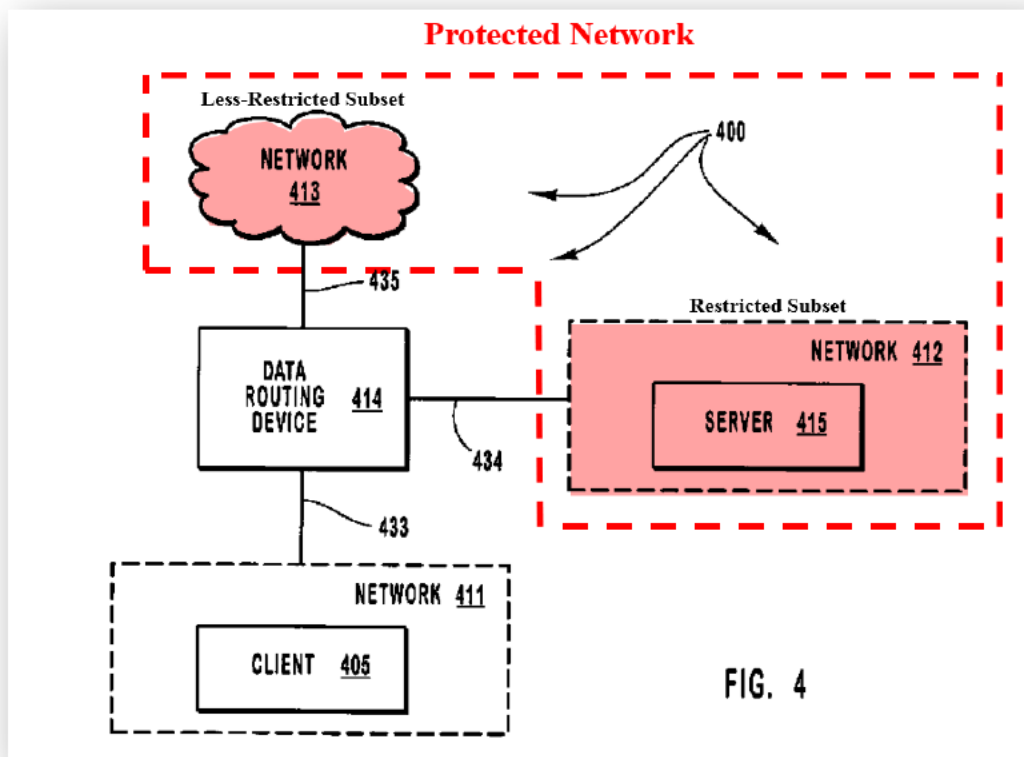
10. Claim 16

i. [16.0] *A method of providing access over a communication network, the method comprising:*

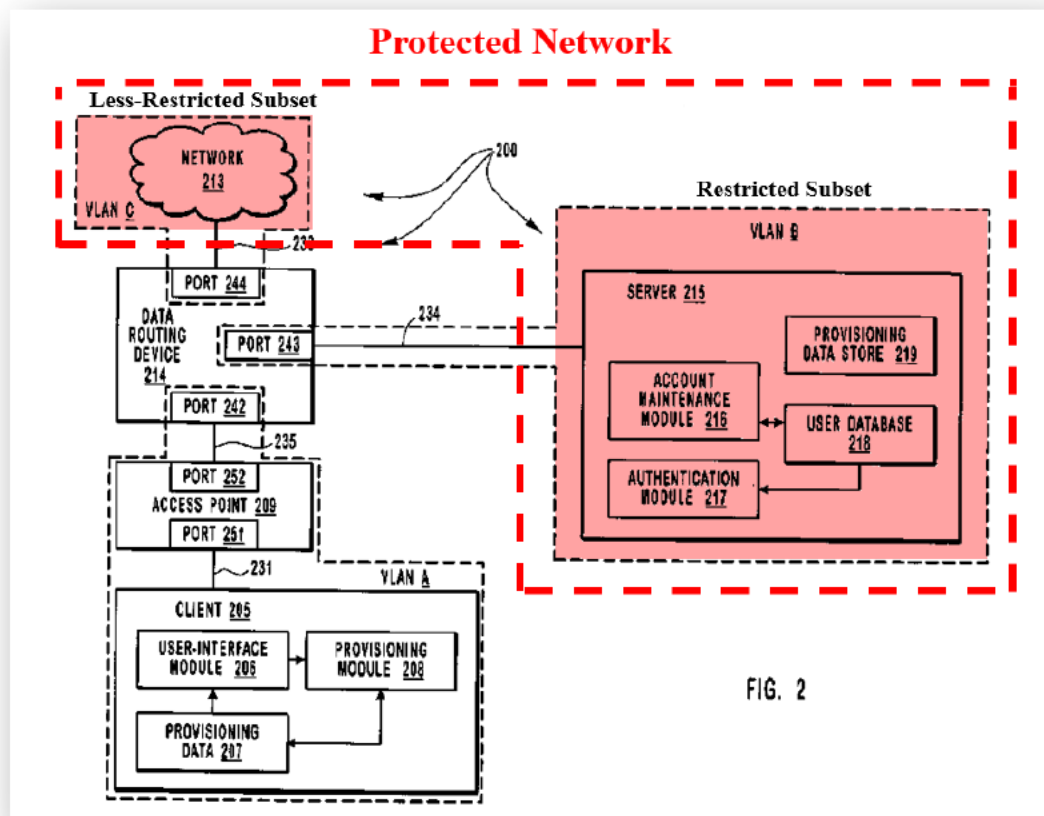
As discussed for claim [1.0], Krantz's network is consistent with the “network/communication network” of the 450 Patent, and Krantz's techniques can also be used “**within a single network.**” Ex.1405, [0017]; *see also*, Ex.1405, [0002]; Ex.1403, ¶186.

Krantz discloses: “[a] server includes the **functionality to authorize clients to access a second network ...**” Ex.1405, [0016] (“*providing access over a communication network.*”). “A client sends credentials to the server to attempt to authenticate with the server. Based on the credentials, the **server may authorize the client for at least partial access to the second network** and/or may deny access to the second network and **authorize the client for at least partial to access to the first network.**” Ex.1405, [0016]; Ex.1403, ¶187.

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



Ex.1405, Figure 4 (annotated).



Ex.1405, Figure 2 (annotated); Ex.1403, ¶188.

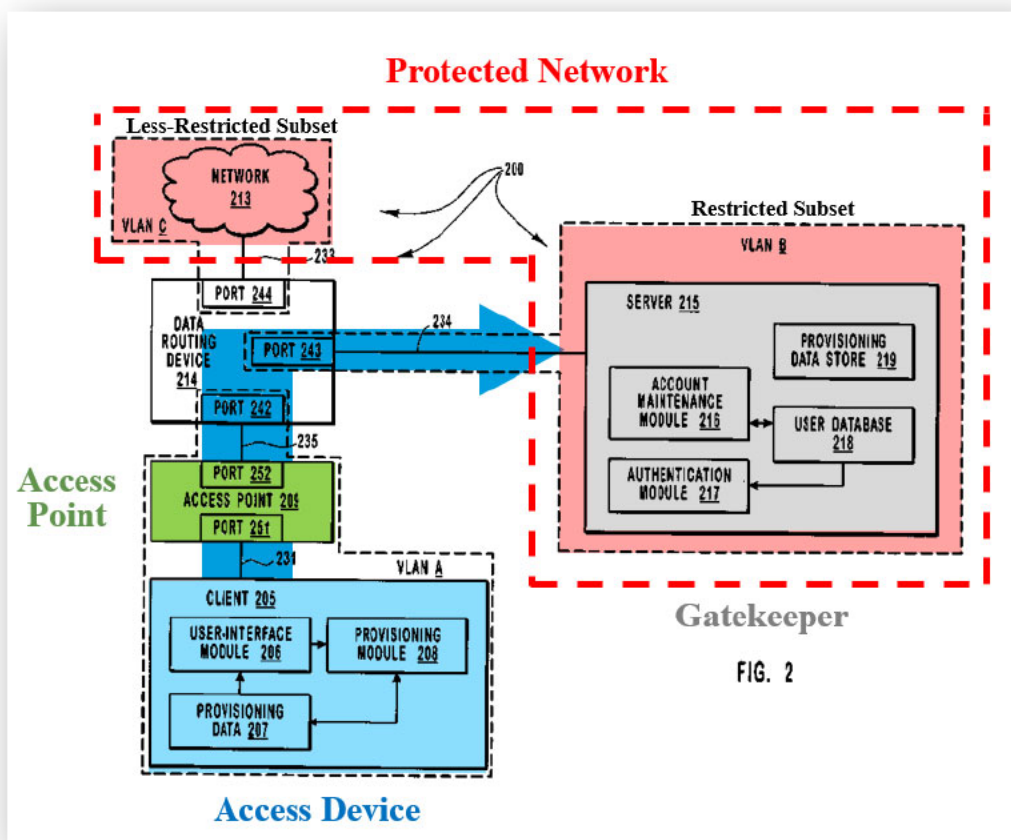
Krantz Figure 4 is “a network architecture 400 **that can provide access to a first network** while restricting access to a second network.” Ex.1405, [0030]. The disclosed system “**may authorize the client for at least partial access to the single network**” (“*providing access over a communication network*”). Ex.1405, [0016]. One example of authorizing/“*providing*” such “*access*” in Krantz is “by authorizing client access to selected computer systems or modules on the single network.” Ex.1405, [0017]; *see also* Ex.1405, [0016], [0071] [0074]-[0076] (“If credential

information matches... the identity of a user is authenticated... If an authenticated user of client 205 is authorized to access resources located on VLAN C... client 205 can then be authorized to access resources located on VLAN C.”); [0104], [0107]-[0109]; Ex.1403, ¶¶189-190.

ii. *[16.1] receiving at an access point a request for access to a less restricted network, the request coming from an access device;*

Krantz discloses client 205 (“access device”) “request[ing] access to a less restricted network.” Krantz discloses “a server has the functionality to authorize access” to a network/selected elements within a network after client 205 (“access device”) sends credentials to the server (“receiving a request.”). Ex.1405, [0016], [0071]. Krantz discloses: the “server (**based at least in part on received credentials**) may authorize the client for at least partial access to the single network.” Ex.1405, [0017]; *See also* [0068]-[0076], [0099], [0104], [0107]-[0109] (describing requesting access in a VLAN environment); Ex.1403, ¶¶191-192.

As seen below, any “access request” for access to less-restricted subset, i.e., VLAN C (“less restricted network”) from client (“access device”) sent to the server must be received at access point 209 (“receiving at an access point”).

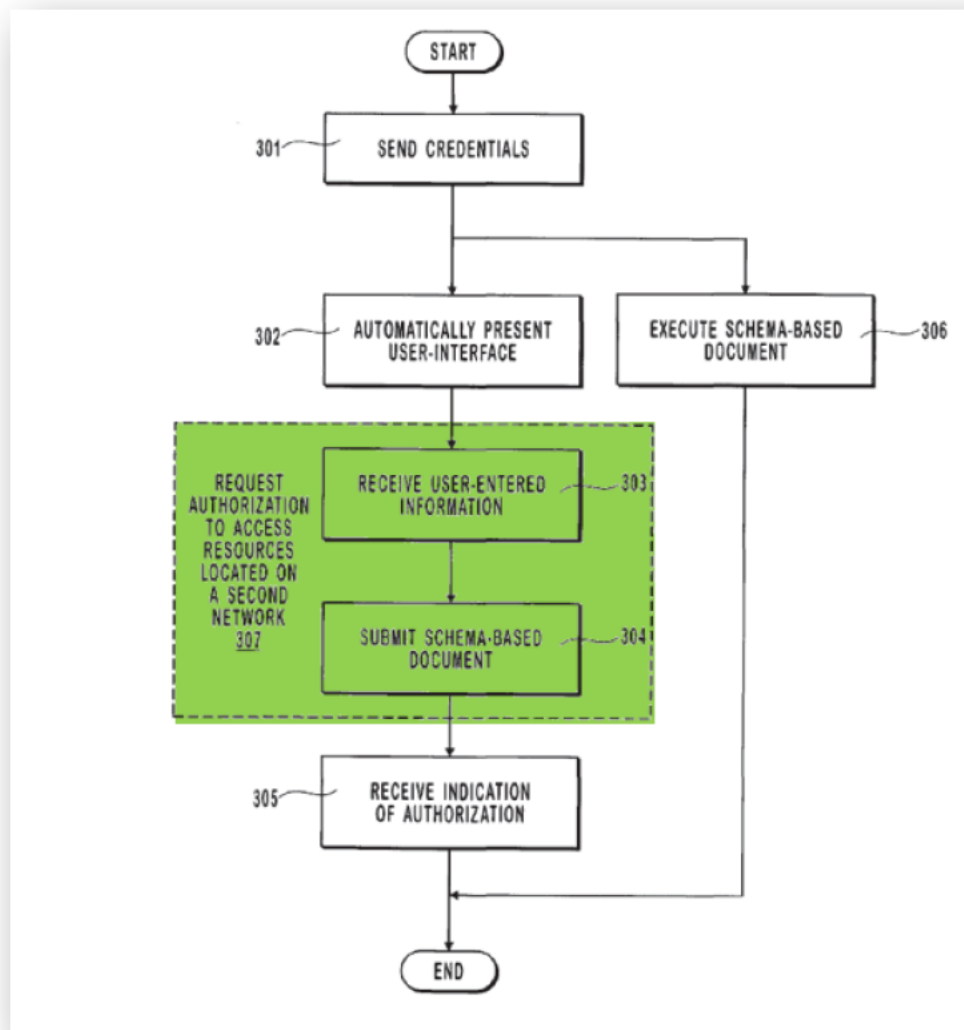


Ex.1405, Figure 2 (annotated); Ex.1403, ¶193.

The request/sending of credentials “can include sending an [‘EAP’] Response/Identity message from the client to the server. If the client is **attempting to connect to a network via an access point** [‘receiving at an access point’ the request for access], the EAP Response/Identity message may be encapsulated [and] transferred through the access point.” Ex.1405, [0018]; Ex.1403, ¶194.

Krantz Figure 3 “is a flow diagram illustrating a method 300 for provisioning a computer system,” and “method 300 [is] described with respect to components

depicted in network architecture 200.” Ex.1405, [0070]. Moreover, “method 300 includes a functional, result-oriented step for **requesting authorization** (*i.e.*, “*receiving a request*”) **to access resources located on a second network (step 307)**” (“*to a less restricted network*”). Ex.1405, [0104]; *see also* Ex.1405, [0071] (describing the client sending credentials to server to authenticate). Additionally, “[s]tep 307 may include any corresponding acts for accomplishing the result of requesting authorization to access resources located on the second network.” Ex.1405, [0104].



Ex.1405, Figure 3 (annotated); Ex.1403, ¶195.

The combination of VLAN C/VLAN B constitute a “*network*.” Krantz discloses that “[b]ased on [client] credentials, “the server **may authorize the client for at least partial access to the second network [VLAN C] and/or may deny access to the second network** and authorize the client for at least partial to access to the first network” (“*a request for access to a less restricted network.*”) Ex.1405,

[0016]; *see also* Ex.1405, [0017] (explaining that “the server [] may authorize the client for **at least partial access to the single network** [e.g.] by authorizing client access to selected computer systems or modules on the single network.”). Similarly, Krantz explains that its access methods “include[] a functional, result-oriented step **for requesting authorization to access resources located on a second network.**” Ex.1405, [0104]; Ex.1403, ¶196.

In Krantz, “second network”—VLAN C—is a “*less restricted network*” because it provides “full access to [its] resources” to authorized users, *see* Ex.1405, [0019]—precisely as the “*less-restricted subset of a protected network*” (i.e., the “*less restricted network*”) is described in the 450 Patent. For example, the 450 Patent explains that “[t]he less-restricted subset being **less restricted** relative to the restricted subset **in terms of what elements may be included in each subset**” (Ex.1401, 5:46-48), i.e., the “*less restricted network*” of the 450 Patent provides greater access to elements/resources than “*restricted subset.*”⁶ Ex.1403, ¶¶197-198.

⁶ In Krantz, the “*restricted subset*” is the first network, i.e., VLAN B.

- iii. *[16.2] applying a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device;*
 - a. *applying a security policy... in response to the request*

As discussed for [16.1] access device makes a “*request*.” The 450 Patent states: “gatekeeper⁷ is configured to enforce a security policy... before granting access to a less-restricted [network] subset.” Ex.1401, Abstract; Ex.1403, ¶200.

Krantz similarly discloses: “client **attempts** to become authorized to access resources located on a second network... [and] sends credentials to an access point [] coupled to a server [] that can authorize access to the second network.” Ex.1405,

⁷ Applicant admits this Gatekeeper is prior art. Ex.1401, 2:34-36.

[0031]; Fig. 2 (below).

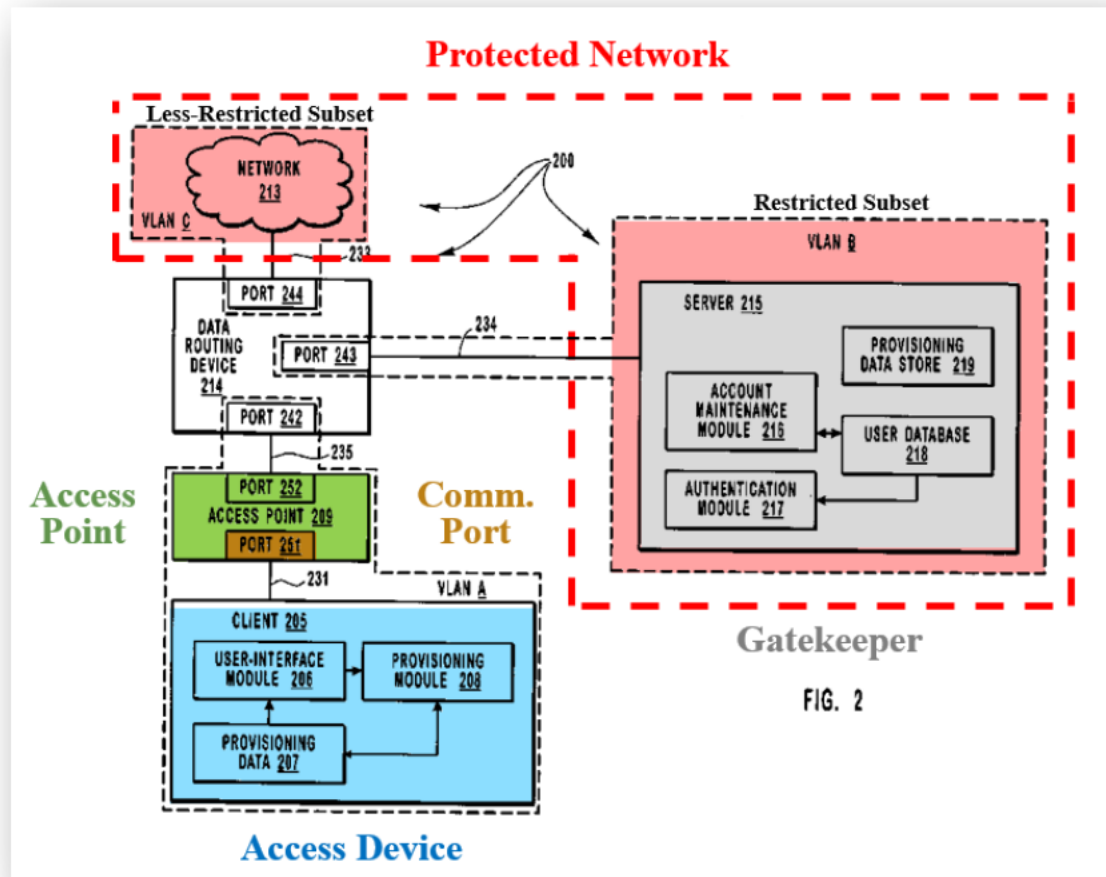


FIG. 2

Ex.1405, Fig. 2 (annotated); Ex.1403, ¶201.

For the “Gatekeeper” (server 215), Krantz discloses “*applying a security policy.*” The 450 Patent explains: “security policies may include [] user identification [], [] configuration of Access Device 230, application requirements [] on Access Device 230, or the like.” Ex.1401, 6:44-49; Ex.1403, ¶202.

Krantz discloses several examples of “*applying a security policy to the access device in response to the request.*” Krantz explains network access may be controlled by “configuration settings,” e.g., “supported types of encryption” or “supported types of authentication,” including EAP. Ex.1405, [0066]-[0067]. Krantz explains: “[a]fter an EAP type is selected . . . computer systems **can attempt to authenticate with one another** through the transfer of EAP messages. . . . 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 **[to] be authenticated and possibly authorized to access resources located on VLAN C.**” Ex.1405, [0068]. EAP-TLS (*e.g.*, Ex.1405, [0067]-[0074], [0100]) was a known authentication protocol for authenticating client devices. Ex.1416, 1; *see also*, Ex.1416, 2 (“**EAP methods [] focussed [sic] on authenticating a client to a server.**”); Ex.1403, ¶203.

Krantz also discloses: “the MS Chap V2 Parameters [] can be included in a configuration sub-file to indicate whether **or not operating system credentials should be used for authentication.**” Ex.1405, [0099]; Ex.1403, ¶204. Krantz explains that EAP-TLS and EAP-MSCHAP V2 can both be required for client access/authorization. Ex.1405, [0099]. A POSITA would understand each of the above techniques in Krantz are used to authenticate client 205 (“*applying a security policy to the access device in response to the request.*”) before authorization is

granted. *E.g.*, Ex.1417, at 2 (“EAP-TLS. TLS (SSL)... The computer first authenticates to the network using a machine certificate...”); Ex.1403, ¶205.

b. ***application of the security policy including performing an audit of the access device***

Krantz discloses: “[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...**” Ex.1405, [0074]; Ex.1403, ¶¶206-207.

Furthermore, “[w]hen credentials are sent to **server 215, authentication module 217 can receive the credentials** (e.g., user-identifier and password) **and compare the credentials to entries in [user database]. If credential information matches an entry in [user database], the identity of a user is authenticated...** If an authenticated user of client 205 is authorized to access resources located on VLAN C [] client 205 can then be authorized to access resources located on VLAN C.” Ex.1405, [0076]. Krantz’s disclosures are consistent with the 450 Patent’s description of the “*audit*” which can identify the access device and/or a user of the device. Ex.1401, 12:9-11 (“**Authenticate User Step 440** is considered part of the **security policy audit**”); *see also*, Ex.1401, 11:40-47. Ex.1403, ¶208.

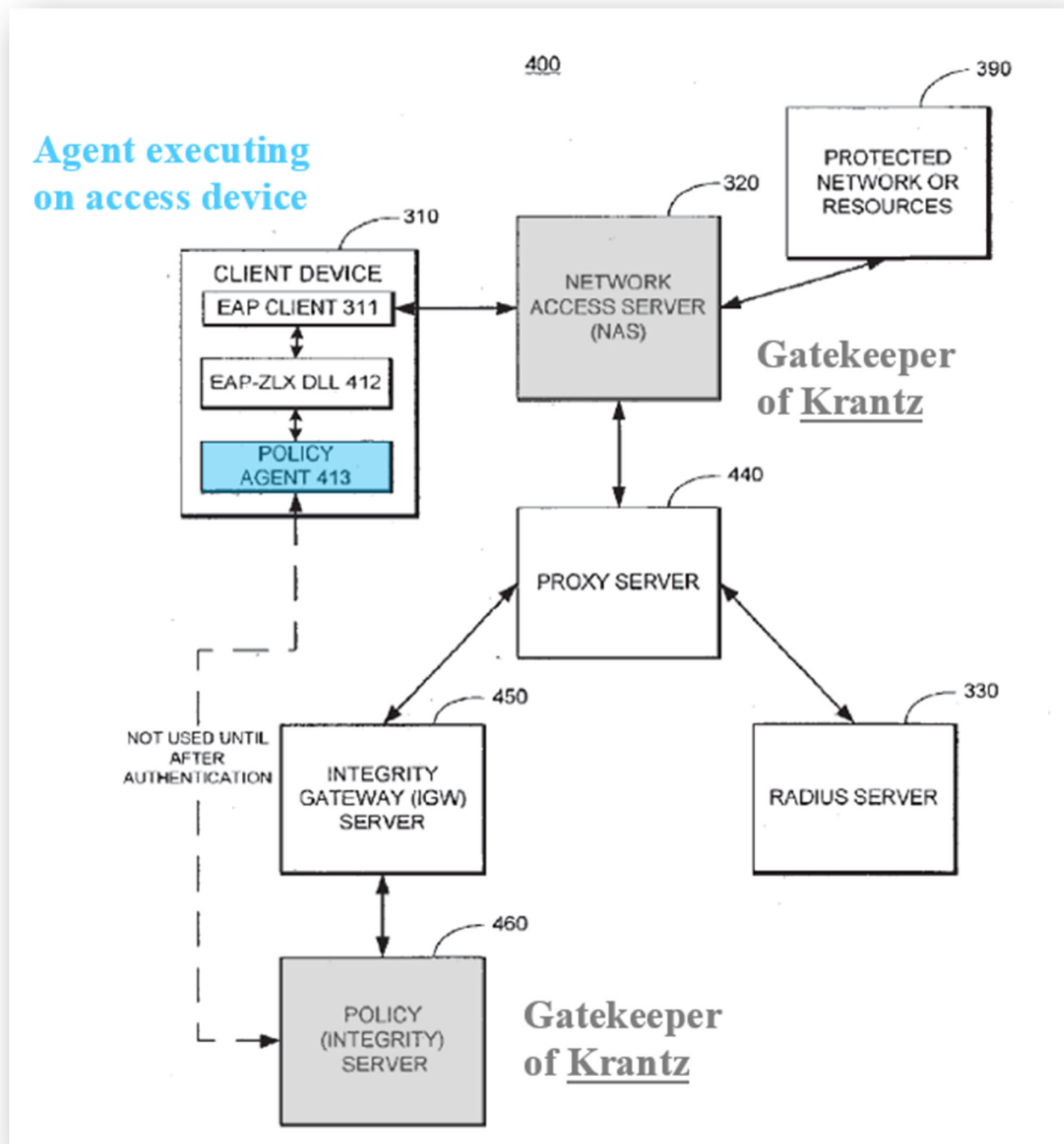
Krantz's gatekeeper may enforce *security policies*, including “*performing an audit of the access device*.” For instance, “[i]t may also be that **client 205 and server 215 exchange EAP-messages to pass certificates, keys, and supported cipher suites** [*“audit data of the access device”*]. Depending on the EAP type, **other credential information may also be exchanged** between client 205 and server 215.” Ex.1405, [0074]. Thus, audit data can be used to identify the access device consistent with the 450's teachings. Ex.1401, 11:40-47; Ex.1403, ¶209

The combined system of Krantz and Herrmann would include “*application of the security policy including performing an audit of the access device*,” e.g., requiring antivirus software as described in Herrmann. Ex.1406, [0012]; Ex.1403, ¶210.

Herrmann discloses: “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.1406, [0071]. This may be implemented using security rules and **checking system data** [*“audit data”*] **for connecting devices to ascertain compliance**. Ex.1406, [0068]; Ex.1403, ¶211.

It would have been obvious to implement Herrmann's features in Krantz's gatekeeper as Herrmann's server components are like the gatekeeper of Krantz, e.g., Herrmann explains: “network access server... acts as an access point (i.e., gateway)

to [] resources [] (e.g., the protected network resources 390) and accepts requests for access to such resources from client machines.”). Ex.1406, [0053]; Ex.1406, [0065] (describing “policy (integrity) server” as a “server-side component” that may “act on [] communications to determine whether or not the client device 310 is in compliance with applicable security policies...,” like the server 215 gatekeeper of Krantz. Furthermore, both Herrmann and Krantz discuss logical implementations of server techniques and thus the gatekeeper of Krantz would easily integrate with the policy agent of Herrmann:



Ex.1406, Fig. 4 (annotated); *see also*, Ex.1405, [0038], [0051] (describing the use of logical communication links and logical representations of computer systems); Ex.1406, [0026]; Ex.1403, ¶¶212-213.

iv. ***[16.3] providing information to the access device to improve compliance of the access device to the security policy, in response to the audit;***

As discussed *supra* for [16.2], the gatekeeper of Krantz may enforce “*security polic[ies]*,” which can include performing an “*audit*” of the access device. Additionally, Krantz explains, for example, that “[w]hen full access to resources located on the second network is not authorized [*in response to the audit*], 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** [*provid[e] information to the access device to improve compliance of the access device to the security policy.*’]. Ex.1405, [0032]; *see also* Ex.1405, [0056] (“Client 405 can be authorized to download provisioning files from these computer systems or modules, while being denied access to other resources located on network 413.”); Ex.1405, [0110] (“[M]ethod 300 also includes an act of executing a schema-based document (act 306)... For example, 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 [i.e., ‘*improve compliance of the access device to the security policy*’...”]; *see also*, Ex.1405, [0077] (discussing how client may be able to download “provisioning files (from VLAN B) to become authorized to access resources located on VLAN C.”), [0078], [0079]. Ex.1403, ¶¶214-217.

v. ***[16.4] granting access to the less-restricted network based on satisfaction of the security policy by the updated access device;***

As discussed for [16.3], in response to an audit, Krantz explains: “[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** [‘*provid[e] information ... to improve compliance of the access device*’ or ‘*update the access device*’ with the provisioning files]. Ex.1405, [0032]; *see also* Ex.1405, [0056] (“Client 405 can be authorized to **download provisioning files** [‘*update the access device*’] from these computer systems or modules, while being denied access to other resources located on network 413.”); Ex.1405, [0110] (“In parallel with acts 302 through 305, the method 300 also includes an act of executing a schema-based document (act 306). This can include **executing a third schema-based document** to configure a client for accessing the

second network [i.e.] **appropriately configure client 205 for accessing resources located on VLAN C.**"); Ex.1403, ¶¶218-219.

Based on this update of the “*access device*,” the system of Krantz can “*grant[] access to the less-restricted network based on satisfaction of the security policy by the updated access device*” as the provisioning process allows the access device to be granted access to VLAN C (the “*less-restricted network*”) as shown below. Ex.1405, [0110].

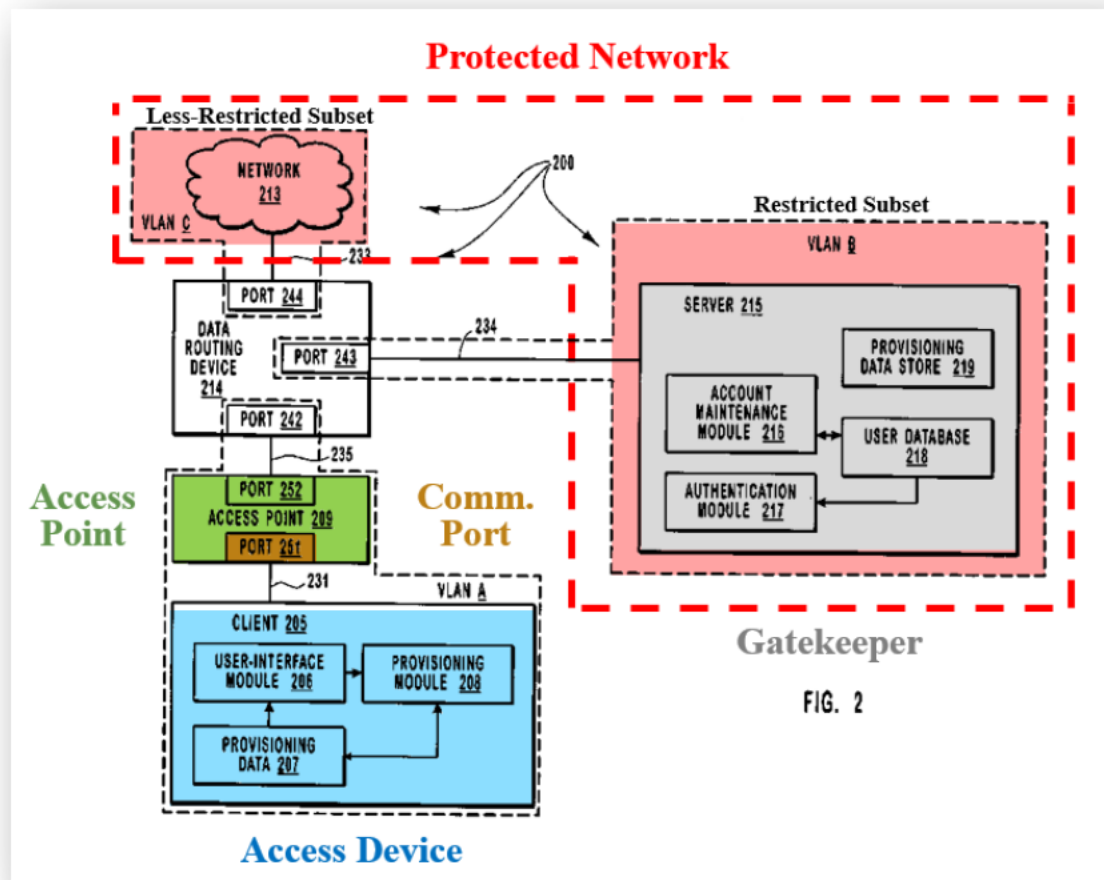


FIG. 2

Krantz, Fig. 2 (Ex.1405) (Annotated). Thus, Krantz can “appropriately configure client 205 **for accessing resources located on VLAN C** [*‘grant[] access to the less-restricted network’*].” Ex.1405, [0110]; *see also*, Ex.1405, [0101] (more information may be needed “to enable access to resources located on VLAN C.”), [0077] (client may be able to download “provisioning files (from VLAN B) **to become authorized to access resources located on VLAN C.**”), [0078] (“EAP-notification can include a [*‘URI’*] to a master document that contains information **for provisioning computer systems to access resources located on VLAN C.**”), [0079]. Thus, the “*update[] [to] the access device*” through, e.g., the provisioning techniques described above, allows it to be “*grant[ed] access to the less-restricted network*” (VLAN C) because it can now “*satisf[y] the security policy.*” Ex.1403, ¶¶220-221.

vi. ***[16.5] authenticating a user of the access device, wherein granting access is further based on the authentication.***

Like [1.3] and [16.4], Krantz discloses this limitation. For instance, Krantz discloses “*a user of the access device*” is authenticated: “[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**]. If credential information matches an entry in [**user database**], **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.1405, [0076]; *see also* Ex.1405, [0074] (EAP used to authenticate user); Ex.1403, ¶¶222-223.

Krantz explains that “[i]f an **authenticated user of client 205** [*“a user of the access device”*] is authorized to access resources located on VLAN C (**e.g., the user is up to date on payments** for their account), **client 205 can then be authorized to access resources located on VLAN C.**” Ex.1405, [0076]. Thus, the “*granting [of] access is further based on the authentication*” because the user must be authenticated, e.g. via the database to check that the user is up to date on payments in order to be granted access to the “*less-restricted network*” (VLAN C). Ex.1403, ¶¶224-225.

11. Claim 22

a. [22.0]

See [16.0]; Ex.1403, ¶226.

b. [22.1]

See [16.1]; Ex.1403, ¶227.

c. [22.2]

See [16.2]; Ex.1403, ¶228.

d. [22.3]

See [16.3]; Ex.1403, ¶229.

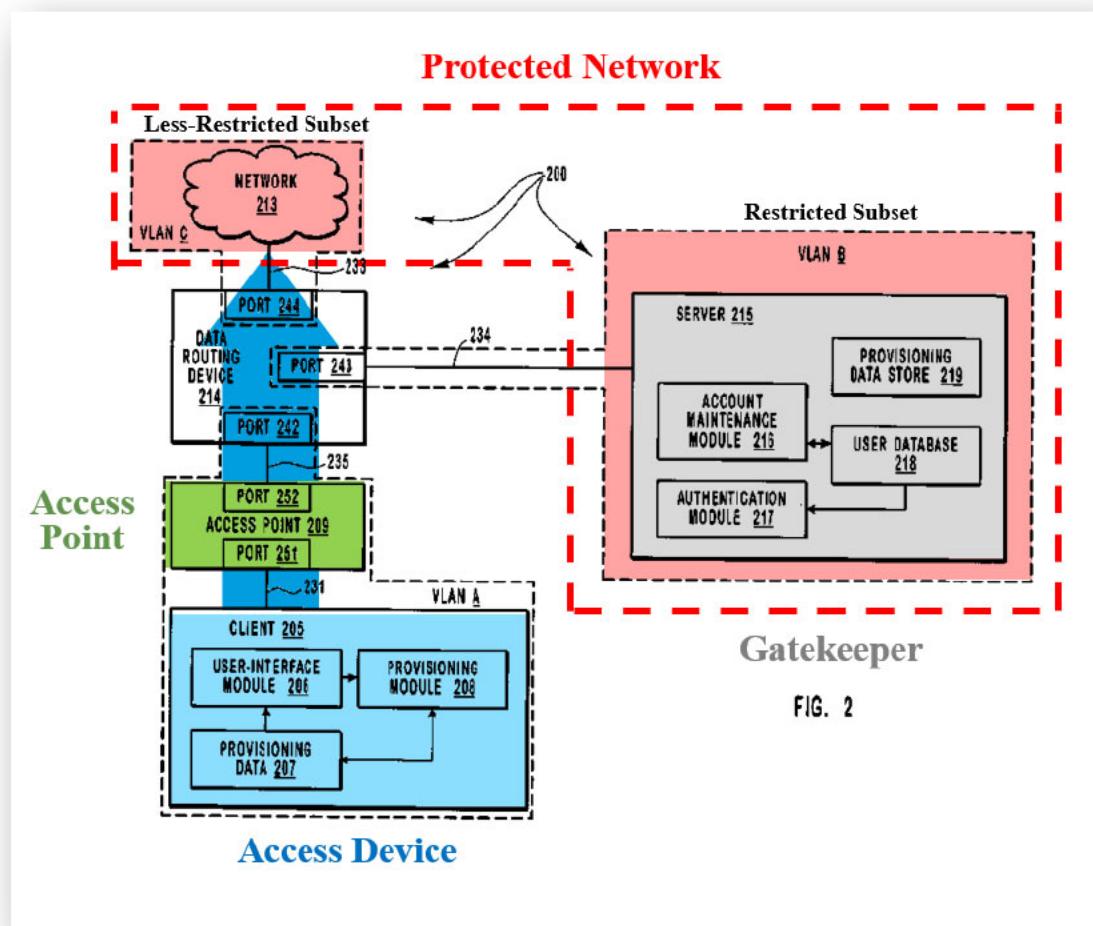
e. [22.4]

As discussed for [16.4], Krantz and Herrmann disclose “*granting access to the less-restricted network based on satisfaction of the security policy by the updated access device.*” Additionally, Krantz discloses the second half of this claim element, “*the granting of access includes configuring the access point to allow the access.*” As with [1.4], Krantz in view of Herrmann discloses “*configuring the access point in response to a result of applying the security policy.*”⁸ This configuration is what “*allow[s] the access*” to the less-restricted network. As explained for [1.4], Krantz discloses that “access point 209 (i.e., “*access point*”) is a wireless access point that enables access to wired computer systems on VLAN B (e.g., server 215) **and** VLAN C (e.g., computer systems included in network 213).” Ex.1405, [0064]; Ex.1403, ¶¶230-232.

Krantz states: “if an authenticated user of client 205 is authorized to access resources located **on VLAN C** [], client 205 can then be authorized to access

⁸ As for [1.4], it would have been obvious to implement the Data Routing Device disclosure of Krantz within the Access Point 209 itself.

resources located on VLAN C.” Ex.1405, [0076]. A “*security policy*” is applied in response to the client requesting access to resources on VLAN C. Ex.1405, [0016-0018], [0071]-[0072], [0076], [0104]-[0109]. Thus, after “requirements of the security policy are satisfied,” access point facilitates data transfer between client 205 (the access “*device*”) and, ultimately VLAN C. Ex.1405, [0063]-[0064]. As shown below, “*configuring the access point [is what] allow[s] the access*” to VLAN C (“*the less-restricted network*”).



Ex.1405, Figure 2 (annotated); Ex.1403, ¶233.

Additionally, Krantz explains: “[a]ccess point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 [] that are to be transferred to VLAN B and/or VLAN C.” Ex.1405, [0064]; *see also* Ex.1405, [0061], [0023]; Ex.1403, ¶234.

Thus, when configured as a “VLAN aware device,” Krantz’s “*access point*” is “*configured*” 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**. Ex.1405, [0107]. There is “*configuring [of] the access point to allow the access*” because it was previously tagging incoming data from client 205, as described above, with headers that enabled access to **VLAN B**. Ex.1403, ¶235.

Indeed, Krantz discloses “[w]hen client 205 is authorized to access resources located on **VLAN C**, access point 209 may enable any protocols that are currently blocked for port 251 and may insert Tag Headers indicating that data from client 205 is to be transferred to VLAN C. 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.1405, [0107]. As explained for [1.4], configuring input ports in VLAN aware devices to tag incoming data was well-known to POSITAs by 2003. Ex.1403, ¶¶236-237.

12. [23.0] wherein performing the audit includes using an agent on the access device to collect information regarding the access device.

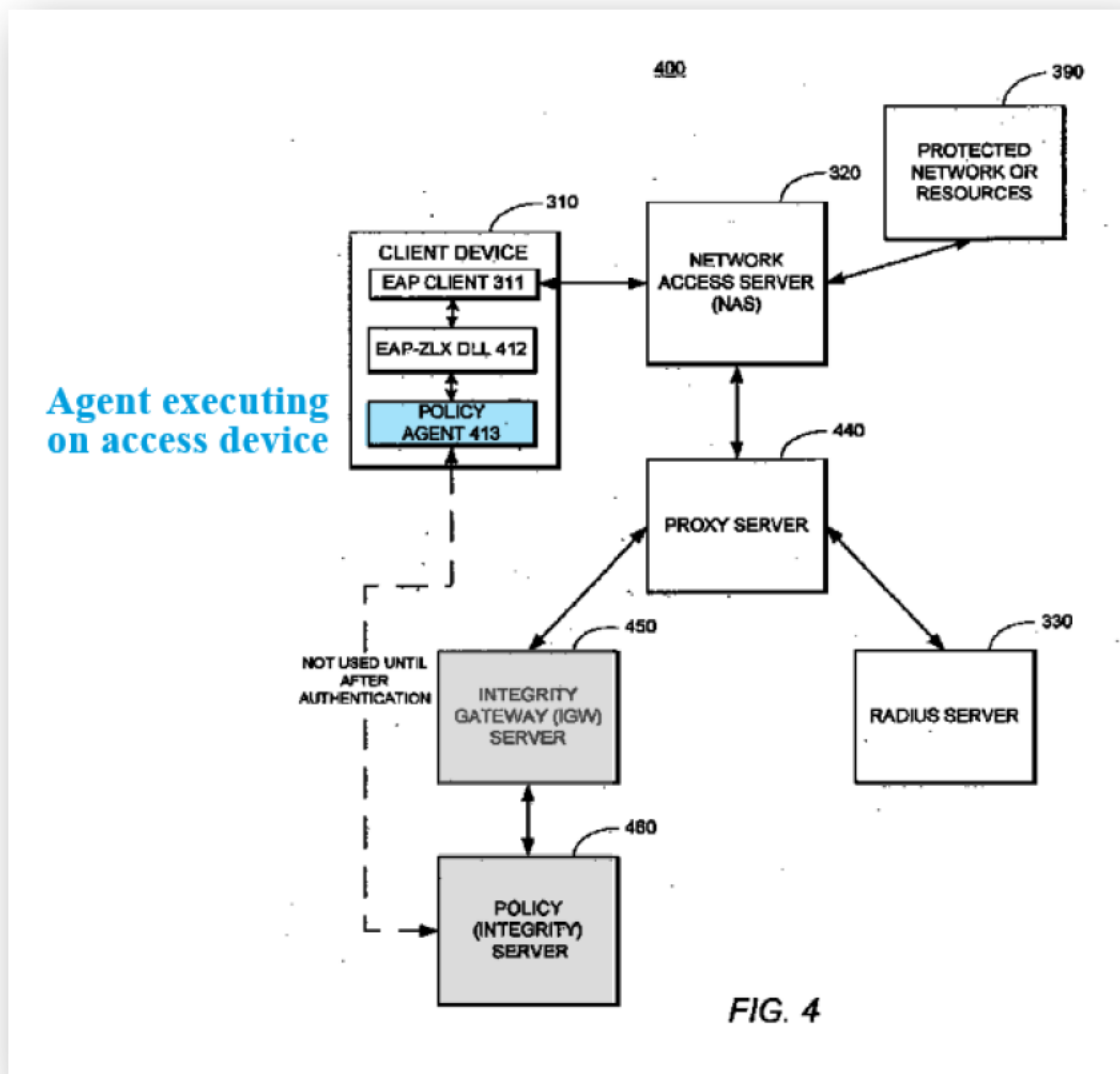
As with [22.2], Krantz in view of Herrmann discloses “*performing [an] audit of the access device.*” This audit “*includes using an agent on the access device to collect information regarding the access device.*” As for [1.2], Krantz in view of

Herrmann discloses “*scanning the device to collect information regarding the device.*” Ex.1403, ¶¶238-239.

As discussed for [1.2], “*scanning*” amounts to gathering relevant information. Ex.1401, 6:63-65, 12:7-9. As discussed for [14.0], Krantz in view of Herrmann discloses such scanning (or “*collect[ing] [of] information*”) is “*performed using an agent on the device.*” Ex.1403, ¶¶240-241.

Dr. Houh explains that one way that “*scanning/collecting information the device to collect information regarding the device*” (e.g., EAP-messages, operating system credentials...) could be accomplished, would be with an agent on the device. It would have been obvious in view of Herrmann to include one, and a POSITA would have been motivated to combine Krantz and Herrmann for the reasons stated in §VII.C. Ex.1403, ¶242.

Herrmann discloses “POLICY AGENT 413” (i.e., an “*agent*”) executing on the device interacting with a “POLICY (INTEGRITY) SERVER 460” and “INTEGRITY GATEWAY (IGW) SERVER 450” (in gray):



Ex.1406, Fig. 4 (annotated). Herrmann discloses: “policy agent [] retrieve[s] information about the current security policy in operation on the client device 310 [i.e., scanning the device to collect information regarding the device].”

Ex.1406, [0064]. Herrmann explains: “In response to [] 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.1406, [0067]. A POSITA would understand “evaluating” the device means device information must be scanned. Policy server is notified by the client, containing policy agent 413, to authenticate the access device. Ex.1406, [0080], [0098]. Herrmann’s disclosure of a policy agent retrieving information about the device and sending to a policy server is consistent with the 450 Patent. See claim [14]; Ex.1401, 11:60-64. Moreover, this is accomplished “*using an agent on the device*” as policy agent 413 is contained on client device 310. Ex.1403, ¶243.

A POSITA would have been motivated to add the security policy agent of Herrmann to the client device of Krantz for several reasons. §VII.C, *above*, two of the stated goals of Krantz involve automation and security. Ex.1403, ¶¶244-245.

13. [25.0] wherein performing the audit includes receiving operating system information from the access device.

As with [22.2], Krantz in view of Herrmann discloses “*performing [an] audit of the access device.*” Additionally, Krantz in view of Herrmann discloses that one aspect of the audit can include “*receiving operating system from the access device.*” Ex.1403, ¶¶246-247.

Krantz discloses that “client 205 and server 215 **exchange EAP-messages...**” Ex.1405, [0074]. A handshake protocol may be used between the device and the gatekeeper and some of the data may include “*receiving operating system from the access device.*” Ex.1405 [0099]:

a **configuration sub-file** to indicate a type of EAP [is] used to authenticate... [] Parameters [] **can be included in a configuration sub-file to indicate whether or not operating system credentials should be used for authentication.**

Ex.1403, ¶¶248-249.

14. [27.0] wherein the information includes a software update of software on the access device.

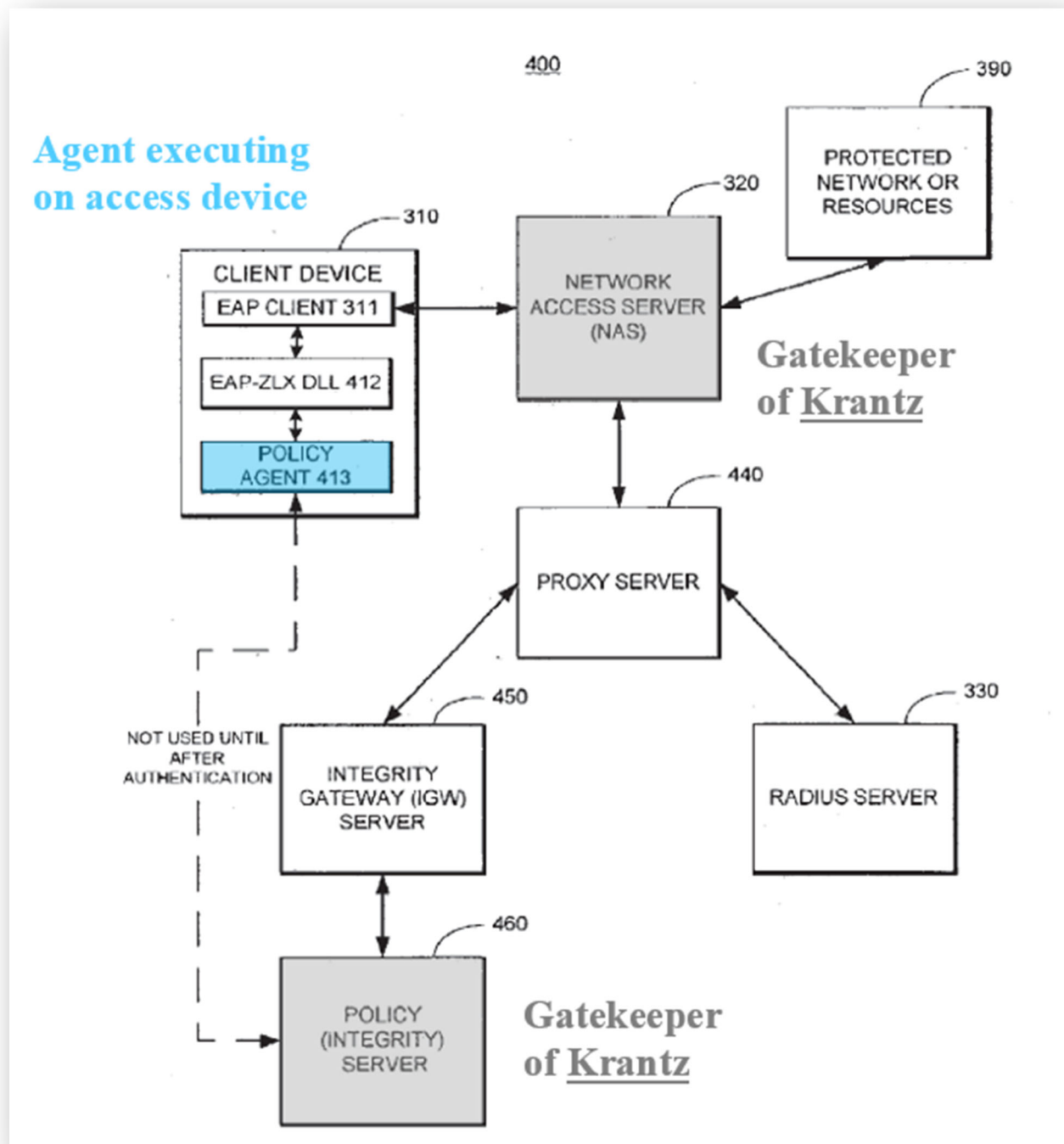
As explained for [22.3], information is provided to the access device to improve compliance of the device with the security policy. As explained for [2.0], Krantz in view of Herrmann discloses that such information can “*include a software update...*” Ex.1403, ¶¶250-251.

Krantz identifies that in prior art systems “***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.1405, [0013]. Krantz discusses how connecting devices may need “provisioning files [] for gaining full access to

network 413.” Ex.1405, [0056]; *see also*, Ex.1405, [0032], [0078] (discussing provisioning clients for gaining network access). A POSITA would have understood provisioning files relate to network connectivity/security, *see, e.g.*, Ex.1409, [0079]; Ex.1403, ¶252.

Herrmann discloses it is critical **“to promptly update anti-virus applications on all machines in a network...”** Ex.1406, [0012]. Thus, “a network administrator **may require all users accessing the network to implement a virus definition update (e.g., DAT file)** [] targeted at a particular virus.” Ex.1406, [0071] (i.e., “*the information includes a software update of software on the access device.*”). This may be implemented using security rules and checking system data for connecting devices to assure compliance. *See*, Ex.1406, [0068] (“**[P]olicy server 460 may enforce** a variety of different types of security policies or rules. [e.g.] requir[ing] client devices [use] particular security or anti-virus programs... a system administrator may [require] **a specific virus protection program is operational on each client device that is connected to a network.**”). Ex.1403, ¶253-254.

As discussed *supra*, policy server 460 of Herrmann is like the gatekeeper (server 215) of Krantz. Both Herrmann and Krantz discuss logical implementations of disclosed server techniques and thus the policy (integrity) server 460 of Herrmann would easily integrate with the system of Krantz as depicted below.



Ex.1406, Fig. 4 (annotated); *see also*, Ex.1405, [0038], [0051]; Ex.1406, [0026]; Ex.1403, ¶255.

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 (“*software update*”) for the reasons discussed for [2.0]. Ex.1403, ¶¶256-257.

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 450 Patent (or related patents), as neither Krantz nor Herrmann was cited or considered by the Examiner during prosecution of the 450 Patent. The references in this Petition were neither relied upon during prosecution nor are they cumulative of art relied upon during prosecution. Further, the 450 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 generally “does not weigh for or against discretionary denial” when neither party has requested a stay); *Amazon Web Services et al. v. Zentian Ltd.*, IPR2023-01194, Paper 10 at 11 (Jan. 10, 2024).

2. Parallel Proceeding Trial Date

Regarding factor 2, no trial date has been set. In addition, according to the most recent statistics⁹ 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 was filed and partially granted, and the investment by the parties has been relatively minimal. In addition, claim

⁹ <https://www.uscourts.gov/statistics-reports/federal-court-management-statistics-december-2023>

10 is not at issue in the related litigations¹⁰. *Samsung Bioepis Co. Ltd v. Regeneron Pharmaceuticals, Inc.*, IPR2023-00739, Paper 9 at 57 (Oct. 20, 2023) (“[B]ecause certain of the challenged claims, . . . are not expressly at issue in the district court litigation, *Fintiv* factor 3 favors institution.”).

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

¹⁰ Additionally, claims 1-4, 7-9, 11, and 14 were held patent ineligible.

strikingly similar disclosure to that of the 450 Patent, is directed at the same problem and proposes the same solutions as the 450 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 are unpatentable for the reasons demonstrated above.

Dated: April 15, 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 13,880 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 15, 2024

Respectfully Submitted,

/Scott M. Border/

Scott M. Border

Reg. No. 77,744

Winston & Strawn LLC

1901 L Street, N.W.

Washington, D.C. 20036

T: 202-282-5054

sborder@winston.com

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I hereby certify that on this 15th 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:

Rimon Law, P.C.
1655 W Fairview Ave, Suite 102
Boise, ID 83702

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 15, 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