

Filed: March 26, 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.

IPR2024-00677
U.S. Patent No. 8,578,444

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 8,578,444**

TABLE OF CONTENTS

	Page
<u>TABLE OF AUTHORITIES</u>	iv
<u>EXHIBIT LIST</u>	v
<u>CLAIM LISTING</u>	vi
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 444 PATENT	3
A. Effective Filing Date	3
B. Person of Ordinary Skill in the Art	4
C. Overview of the 444 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. CLAIMS 1-7, 10, 12, 17, and 22 ARE UNPATENTABLE.....	20
A. Ground 1: Claims 1-7, 10, 12, 17, and 22 are Obvious Based on Krantz in view of Herrmann.....	20
1. Claim 1	20
i. [1.0] A method for auditing a device.....	20
ii. [1.1] performing an authentication.....	24
iii. [1.2] the device being connected.....	28

iv.	[1.3] sending a request...	31
v.	[1.4] receiving the audit data...	36
a.	“receiving the audit data at a gatekeeper configured to control access to a network”	38
b.	Receiving ... “from the agent, the audit data pertaining to the device and having been obtained by the agent,”	50
vi.	[1.5] applying a security policy...	54
2.	Claim 2	60
3.	Claim 3	70
4.	Claim 4	75
5.	Claim 5	77
6.	Claim 6	79
7.	Claim 7	80
8.	Claim 10	81
9.	Claim 12	83
10.	Claim 17	84
11.	Claim 22	86
i.	[22.0]	86
ii.	[22.1]	86
iii.	[22.2]	86
iv.	[22.3]	87
v.	[22.4]	87
vi.	[22.5]	87
vii.	[22.6]	87
viii.	[22.7]	87
ix.	[22.8]	87
IX.	THE BOARD SHOULD NOT EXERCISE ITS DISCRETION AND DENY INSTITUTION	88
A.	The Board Should Not Deny Institution Under 35 U.S.C. § 325(d)	88
B.	The Board Should Not Deny Institution Under 35 U.S.C. § 314(a)	89
1.	No Evidence Regarding a Stay	89

2.	Parallel Proceeding Trial Date	89
3.	Parallel Proceeding Investment.....	90
4.	Overlapping Issues with the Parallel Proceeding.....	90
5.	Overlapping Parties.....	90
6.	Strength of Petition and Other Considerations	91
X.	CONCLUSION.....	91

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
1201	U.S. Patent No. 8,578,444
1202	U.S. Patent No. 8,578,444 File History
1203	Declaration of Henry Houh, Ph.D
1204	CV of Henry Houh, Ph.D
1205	U.S. Patent Pub. No. 2004/0111520 to Krantz et al
1206	U.S. Patent Pub. No. 2004/0107360 to Herrmann et al
1207	IEEE Std 802.1Q-1998 – IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
1208	U.S. Patent No. 6,430,621 to Srikanth et al.
1209	U.S. Patent No. 6,032,194 to Gai et al.
1210	Cisco IOS 12.0 Switching Services (1999)
1211	Microsoft Computer Dictionary 5 th Edition (2002)
1212	Webster's New World Computer Dictionary (2001)
1213	[Reserved]
1214	[Reserved]
1215	[Reserved]
1216	[Reserved]
1217	Wireless security with 802.1x and PEAP (2003)

CLAIM LISTING

Claim No.	Claims
[1.0]	A method for auditing a device, the method comprising:
[1.1]	performing an authentication using an EAP protocol from the device,
[1.2]	the device being connected via a computer network to an access point configured to use an 802.1x protocol;
[1.3]	sending a request for audit data to an agent running on the device;
[1.4]	receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent,
[1.5]	applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper.
[2]	The method of claim 1, wherein applying the security policy includes configuring the access point.
[3]	The method of claim 2, wherein configuring the access point includes assigning an access control list.
[4]	The method of claim 2, wherein configuring the access point includes assigning a VLAN.
[5]	The method of claim 2, further comprising receiving, from the agent, updated audit data pertaining to the device after configuring the access point.
[6]	The method of claim 2, further comprising receiving, from the agent, updated audit data pertaining to the device while the device has access to a less-restricted subset of the network.
[7]	The method of claim 2, further comprising continuing to receive at the gatekeeper, from the agent, audit data pertaining to the device after the configuring of the access point.

[10]	The method of claim 1, wherein the request includes a request for audit data pertaining to an application.
[12]	The method of claim 1, wherein the received audit data includes information that concerns operating system of the device.
[17]	The method of claim 1, wherein the gatekeeper is configured to take part in bringing a software on the device up to date in response to applying the security policy.
[22.0]	A method for auditing a device, the method comprising:
[22.1]	performing an authentication using an EAP protocol from the device,
[22.2]	the device being connected to an access point configured to use an 802.1x protocol;
[22.3]	sending a request for audit data to an agent running on the device;
[22.4]	receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent;
[22.5]	applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper,
[22.6]	where applying the security policy includes configuring the access point;
[22.7]	receiving, from the agent, updated audit pertaining to the device while the device has access to a less-restricted subset of the network; and
[22.8]	re-auditing the device in accordance to the security policy using the received updated audit data.

I. INTRODUCTION

Petitioner Cisco Systems, Inc. and Fortinet, Inc. submits this Petition for *Inter Partes* Review of claims 1-7, 10, 12, 17, and 22 (the “Challenged Claims”) of U.S. Patent No. 8,578,444 (the “444 Patent” (Ex.1201)), assigned to Patent Owner, InfoExpress Inc. Petitioner respectfully submits that the Challenged Claims of the 444 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 444 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 444 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 444 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 444 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 444 Patent.

B. Identification of Challenged Claims

Ground 1: Claims 1-7, 10, 12, 17, and 22 are unpatentable as obvious under 35 U.S.C. § 103 based on Krantz (Ex.1205) in view of Herrmann (Ex.1206).

V. THE 444 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 444 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.1203, ¶21.

C. Overview of the 444 Patent

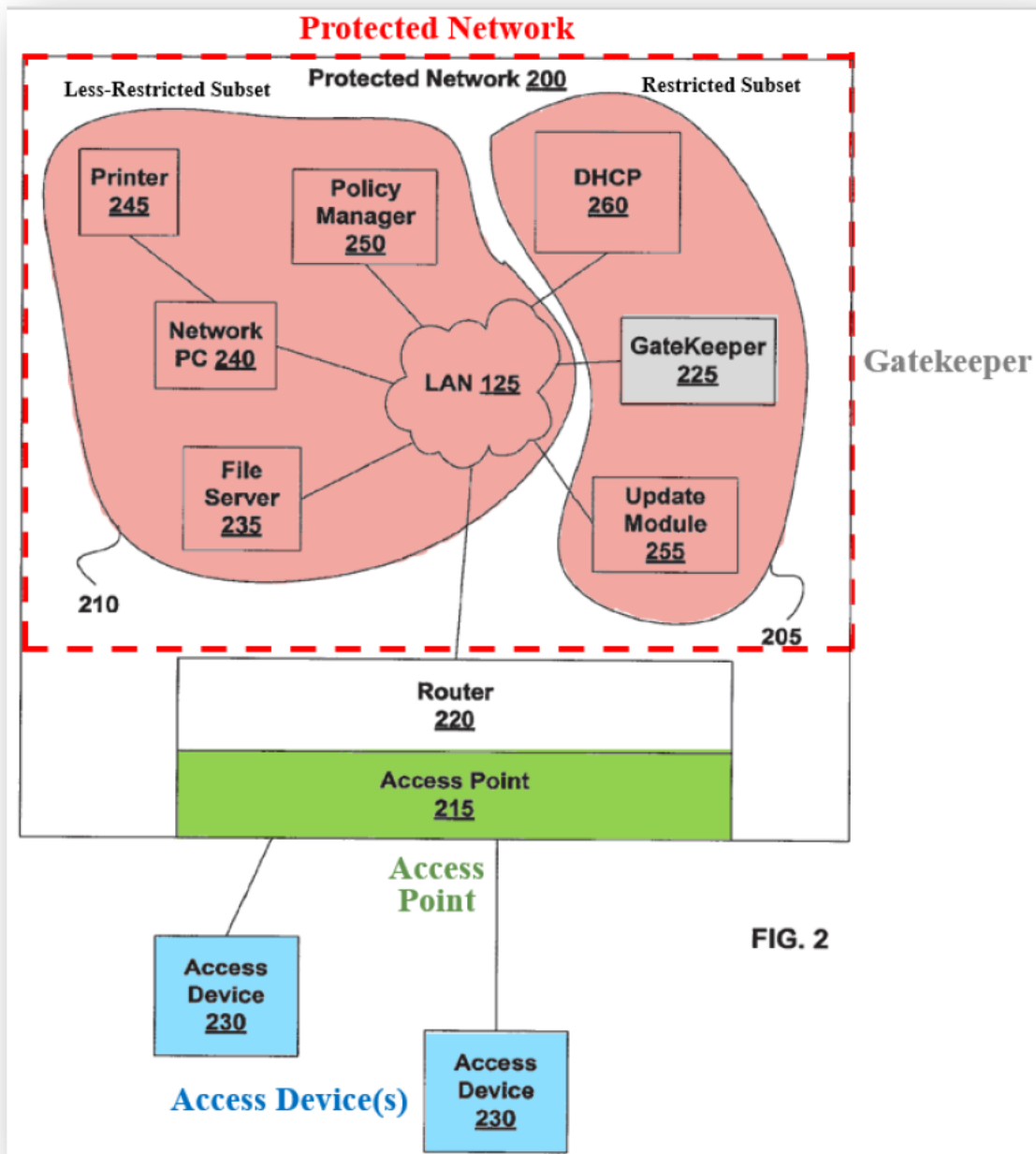
The 444 Patent describes “a protected network¹ physically or logically divided into a restricted subset and one or more less-restricted subsets.” Ex.1201, 2:56-58. Access to less-restricted networks from a device “are first passed to the restricted subset.” Ex.1201, 2:58-60. Elements of the “restricted subset”—such as a “gatekeeper”—“apply security policies” to the device requesting access. Ex.1201, 2:60-62. If the requesting device satisfies the “security policies,” access is then granted “to a less-restricted subset of the protected network.” Ex.1201, 2:60-64.

¹ Notably, the specification and figures refer to a “protected network” throughout, but the claim language merely claims a “network” or “computer network.”

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.1201, 4:4-8. The 444 Patent explains that “[i]n some embodiments, Authenticate User Step [] is considered part of the security policy audit.” Ex.1201, 12:9-11; Ex.1201, 11:42-55.

The 444 Patent further explains that both “the passing of access requests to the restricted subset” and the subsequent granting of such requests is “accomplished by configuring and reconfiguring a communication port of an access point.” Ex.1201, 2:64-67.

Figure 2 depicts embodiments of the invention described in the 444 Patent:



Ex.1201, Fig. 2 (annotated); Ex.1203, ¶34.

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

Ex.1201, 5:58-65. 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.1201, 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 444 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).

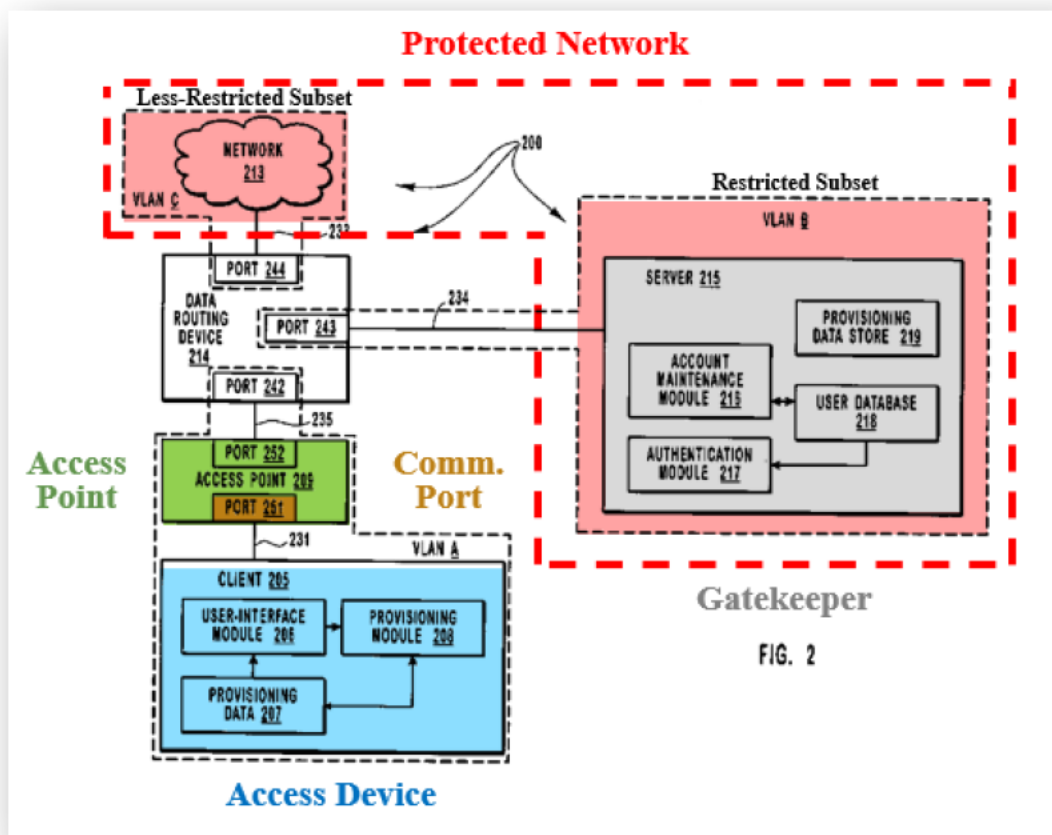
VII. PRINCIPAL PRIOR ART

A. Summary of Krantz

U.S. Patent Pub. No. 2004/0111520 to Krantz et al. (Ex.1205) was filed on December 6, 2002, and published on June 10, 2004. Krantz is prior art to the 444 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.1205, [0015].

Krantz teaches a system in which a device attempts to access a protected network. Ex.1205, [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.1205, [0016], [0068]-[0071], [0099], [0104], [0107]-[0109]. An embodiment of this network architecture is depicted below:



Ex.1205, Fig. 2 (annotated).²

Krantz utilizes Virtual Local Area Network (“VLAN”) techniques. Ex.1205, [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.1205, [0060]. Access Point 209 utilizes ports which can be configured for data transfer. Ex.1205, [0062].

Krantz teaches a client requesting access to the network can send credentials to a server to authenticate itself. Ex.1205, [0016]. Based upon the credentials

² Patentee uses different words to describe claimed features, e.g., referring to a “Protected Network” and “Access Device” in some instances (*see, e.g.*, Ex.1201, Fig. 2) while describing a “Network/Computer Network” and “Device” in others (*see, e.g.*, Ex.1201, claim 1). Similarly, those terms are used interchangeably herein.

supplied, the server “may authorize the client for at least partial access” or access to the entire network. Ex.1205, [0016], [0104], [0107]-[0109]. Authentication may be made by server 215. Ex.1205, [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.1205 [0110]-[0111].

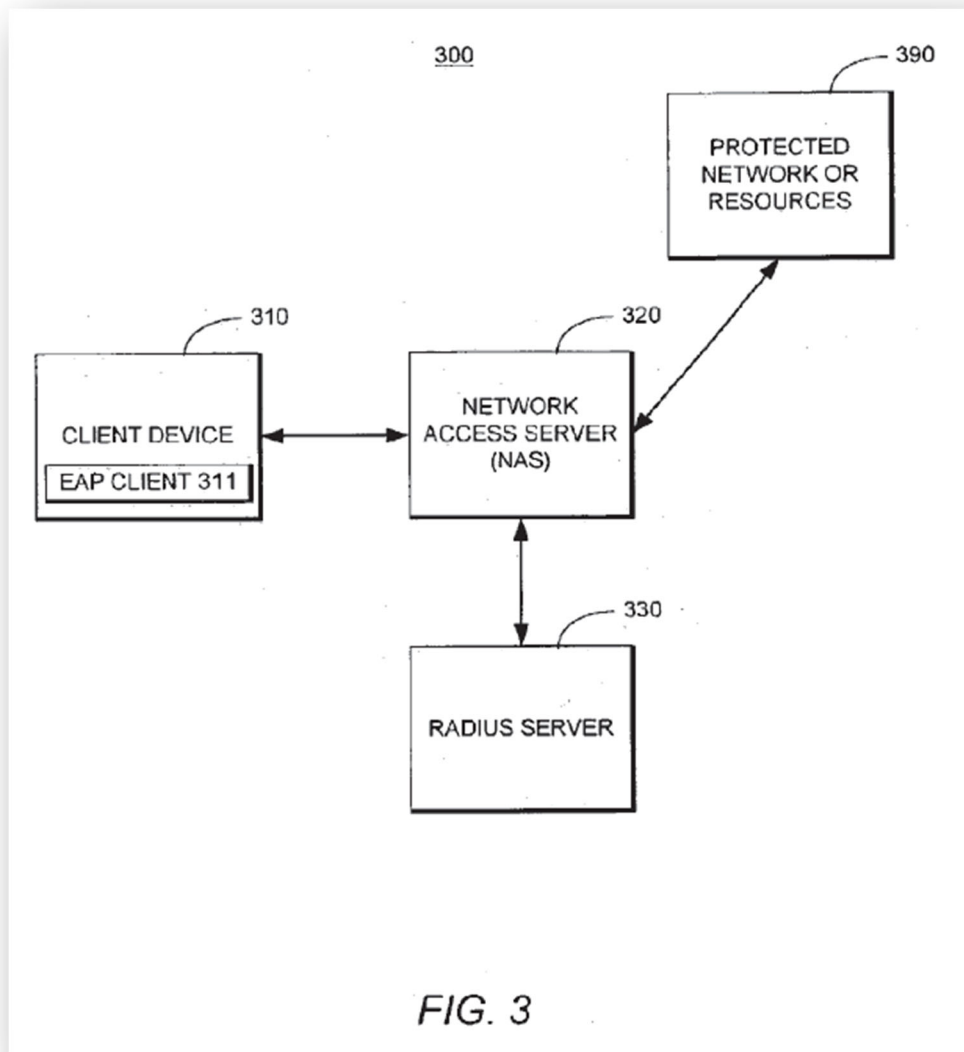
B. Summary of Herrmann

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 444 Patent at least under pre-AIA 35 U.S.C. § 102(e).

Herrmann describes enforcing security policies when providing access to a network. Herrmann explains that if a client device connected to a network is infected with a virus or worm, it may infect other machines on the same network, thus ensuring such devices are running current anti-virus programs is particularly important. Ex.1206 [0012].

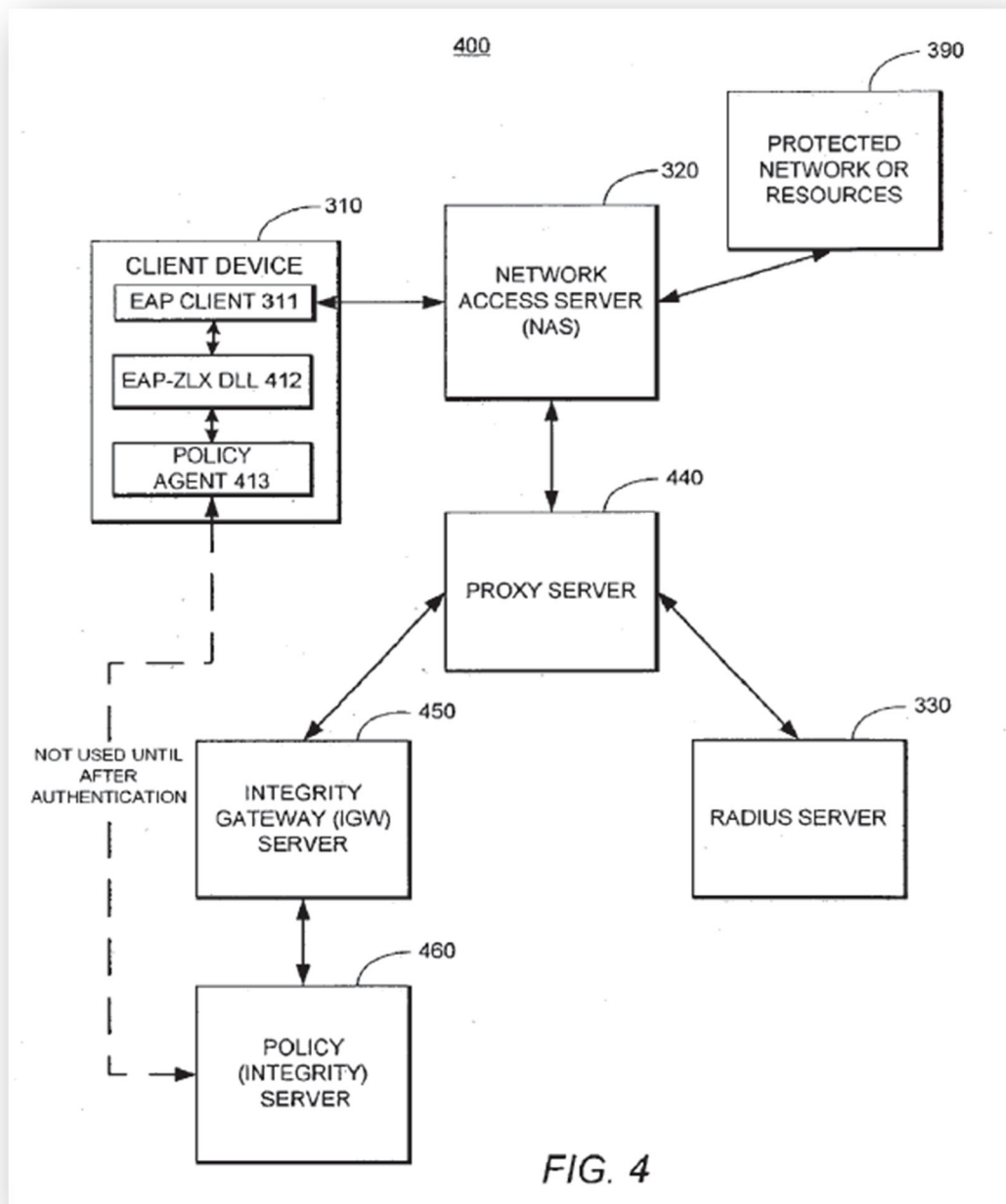
As a solution, Herrmann proposes collecting information from a client device to be used during the authentication process to enforce network security policies. For example, Herrmann teaches a system in which a client device attempts to access a network and information is collected to determine whether the client can gain

access to protected network resources. Ex.1206, [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.1206, [0018], [0053], [0063].



Ex.1206, Fig. 3.

In Figure 4, “a client device 310 connects to the NAS 320 to access the protected network or resources 390.” Ex.1205, [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.1206, [0062], [0067].



Ex.1206, 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.1206, [0064]. This allows “the policy server 460 [to] evaluate whether or not the client device 310 has a correct, up-to-date version of the applicable security policy.” Ex.1206, [0067].

C. The Combination of Krantz and Herrmann

It would have been obvious to include Herrmann’s techniques for obtaining system data from an access device (e.g., whether it includes antivirus software) in the system of Krantz for the reasons explained below. In particular, Krantz already discloses that “access point 209 may block [] protocols ... from being transferred **until client 205 is authenticated (and authorized).**”³ Ex.1205, [0072]. Furthermore, “[w]hen credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) **and compare the credentials to entries in user database 218.**” Ex.1205, [0076]; Ex.1203, ¶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 authentication process already disclosed in Krantz. Like Krantz, Herrmann discloses a “policy server 460 [which] may enforce a variety of different types of security policies or rules.” Ex.1206, [0068]. One such rule would be “a policy

³ Emphasis added throughout in bold unless otherwise indicated.

requiring that a **specific virus protection program** is operational on each client device that is connected to a network.” Ex.1206, [0068]; Ex.1206, [0012] (noting it is critical that all machines in a network maintain updated antivirus software so the network is not infiltrated by newly released viruses). Ex.1203, ¶52.

Krantz’s authentication module, which compares the credentials of a user against a database (e.g., user-identifier and password), as modified by Herrmann, would 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.1203, ¶53.

The 444 Patent itself confirms a POSITA would recognize the need for the authentication module of Krantz to check for approved antivirus programs. In the background of the 444 Patent, it discusses a **prior art** GateKeeper 110 (Ex.1201, 2:34-36) and articulates that “GateKeeper 110 may make certain that Access Device 160 has up-to-date virus software and encryption protocols as proscribed by [a] security policy.” Ex.1201, 2:27-30; Ex.1203, ¶54.

Both Krantz and Herrmann are analogous art to the 444 Patent for at least two reasons. *First*, Krantz and Herrmann are both directed toward the same field of endeavor of the 444 Patent—network security. Ex.1201, 1:26-27; Ex.1205, Abstract Ex.1206, Abstract; Ex.1203, ¶55.

Second, Krantz and Herrmann are reasonably pertinent to a problem described in the 444 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.1201, 1:49-51, 1:60-63. Ex.1203, ¶56.

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**. Depending on the EAP type, other credential information may also be exchanged between client 205 and server 215.” Ex.1205, [0074]. Krantz discloses that the security policy can include “a configuration sub-file to indicate whether or not **operating system credentials** should be used for authentication.” Ex.1205, [0099]; Ex.1203, ¶57.

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.1205, [0056]; Ex.1203, ¶58.

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.1206, [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.1206, [0067]. This policy server is notified by the client, containing policy agent 413, through periodic status messages called “IA_HEARTBEAT(s)” in order to authenticate the access device. Ex.1206, [0080], [0098]; Ex.1203, ¶59.

Herrmann also discloses that “[n]ew viruses are frequently released that cannot be identified using older anti-virus engines and definition files. It becomes critical, therefore, to promptly update **anti-virus applications on all machines in a network** in a timely fashion before the network is infiltrated by a newly released virus.” Ex.1206, [0012]. Herrmann also discloses that “a network administrator may require all users accessing the network to implement a **virus definition update (e.g., DAT file)** that is targeted at a particular virus.” Ex.1206, [0071]; Ex.1203, ¶60.

Herrmann discloses that “[t]he policy server 460 may enforce a variety of different types of security policies or rules ... for instance, rules which require client devices connecting to a given network to be using particular security or anti-virus programs. For example, a system administrator may establish a policy requiring that

a specific virus protection program is operational on each client device that is connected to a network.” Ex.1206, [0068]; Ex.1203, ¶61.

It would have been obvious to combine Herrmann’s techniques regarding determining whether an access device is authorized for network access (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.1203, ¶62.

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. For example, Krantz explains its system 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.1205, [0002]. Similarly, Herrmann explains that “[t]he present invention relates to ... policy enforcement on **computer systems** connected on one or more networks...” Ex.1206, [0003]; Ex.1203, ¶63.

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.1206, [0068] (“[S]ystem administrator may establish a policy requiring that **a specific virus protection program is operational on each client device** that is connected to a network. **The policy server would then evaluate whether or not each client device was in compliance** with the specified policy before approving the client device for network access.”). Security and automation are two stated goals of Krantz. *E.g.*, Ex.1205, [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 providing network security. Additionally, 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.1203, ¶64.

VIII. CLAIMS 1-7, 10, 12, 17, and 22 ARE UNPATENTABLE

A. Ground 1: Claims 1-7, 10, 12, 17, and 22 are Obvious Based on Krantz in view of Herrmann

1. Claim 1

i. [1.0] *A method for auditing a device...*

Krantz discloses receiving audit data from a client 205 (i.e., “device”). Ex.1205, [0016], [0071]. Krantz discloses that the “server (**based at least in part on received credentials**) [*audit data*] may authorize the client for at least partial access to the single network.” Ex.1205, [0017]; *see also* [0074]-[0076], [0104], [0107]-[0109] (collectively describing techniques for requesting access in a VLAN environment). Credentials supplied by the device/user in Krantz are used to control access to the protected network resources (“*auditing a device*”). Ex.1205, [0016], [0068]-[0071], [0099], [0104], [0107]-[0109]. Dr. Houh explains that this access control process would be “*auditing*” as the server of Krantz is inspecting credentials (*id.*, 0016, 0071) and can authorize access based on the audit (*id.*, 0076, 0104, 0106-0109). Ex.1203, ¶¶65-66.

The credentials, or “*audit data*,” “can include sending an Extensible Authentication Protocol (‘EAP’) Response/Identity message from the client to the server. If the client is attempting to connect to a network via an access point, the EAP Response/Identity message may be encapsulated within some other type of

message that can be transferred through the access point.” Ex.1205, [0018]. Other “*audit data*” provided by Krantz’s “*device*” may include, for example, “user-identifier[s] and password[s].” Ex.1205, [0076]. Krantz further explains that “[a]fter an EAP type is selected . . . computer systems can attempt to authenticate with one another through the transfer of EAP messages . . . in accordance with the selected EAP type ...” Ex.1205, [0068]. Dr. Houh explains that EAP-TLS (*e.g.*, Ex.1205, [0067]-[0074], [0100]) was a known authentication protocol that would be used to authenticate client devices. Ex.1205, [0099] (describing EAP-MSChap V2); Ex.1203, ¶67.

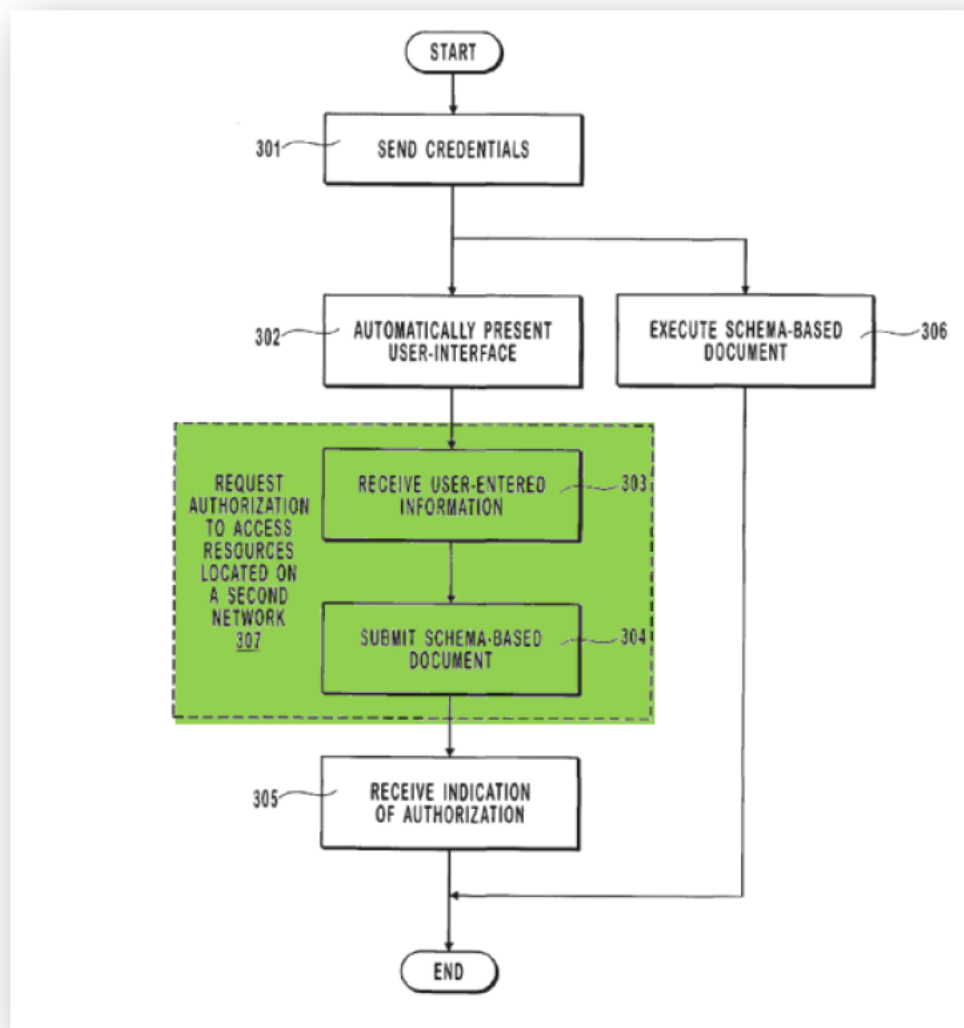
Krantz explains that the credentials are “*audited*” at the server:

[A]uthentication module 217 can receive the credentials (e.g., user-identifier and password) and compare the credentials to entries in user⁴ database 218. If credential information matches an entry in user database 218, the identity of a user is authenticated...

Ex.1205, [0076]; Ex.1203, ¶68.

⁴ The 444 Patent explains that user authentication can be part of the audit: “[i]n some embodiments, Authenticate User Step [] is considered part of the security policy audit.” Ex.1201, 12:9-11.

Krantz explains that 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.1205, [0070]. Furthermore, “method 300 includes a functional, result-oriented step for **requesting authorization to access resources located on a second network (step 307).**” Ex.1205, [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.1205, [0104]; Ex.1203, ¶69.



Ex.1205, Figure 3 (annotated).

Step 307 “includes [the] corresponding act of receiving user-entered information (act 303). A presented user-interface can [] receive user-entered information (e.g., user-identifier, password, name, address, credit card information, etc.) from a user at client 205” (“*auditing a device*”). Ex.1205, [0104]; Ex.1203, ¶70.

The access “device”—i.e., “Client 205”—being audited in Krantz is depicted in Figure 2 in blue and annotated below:

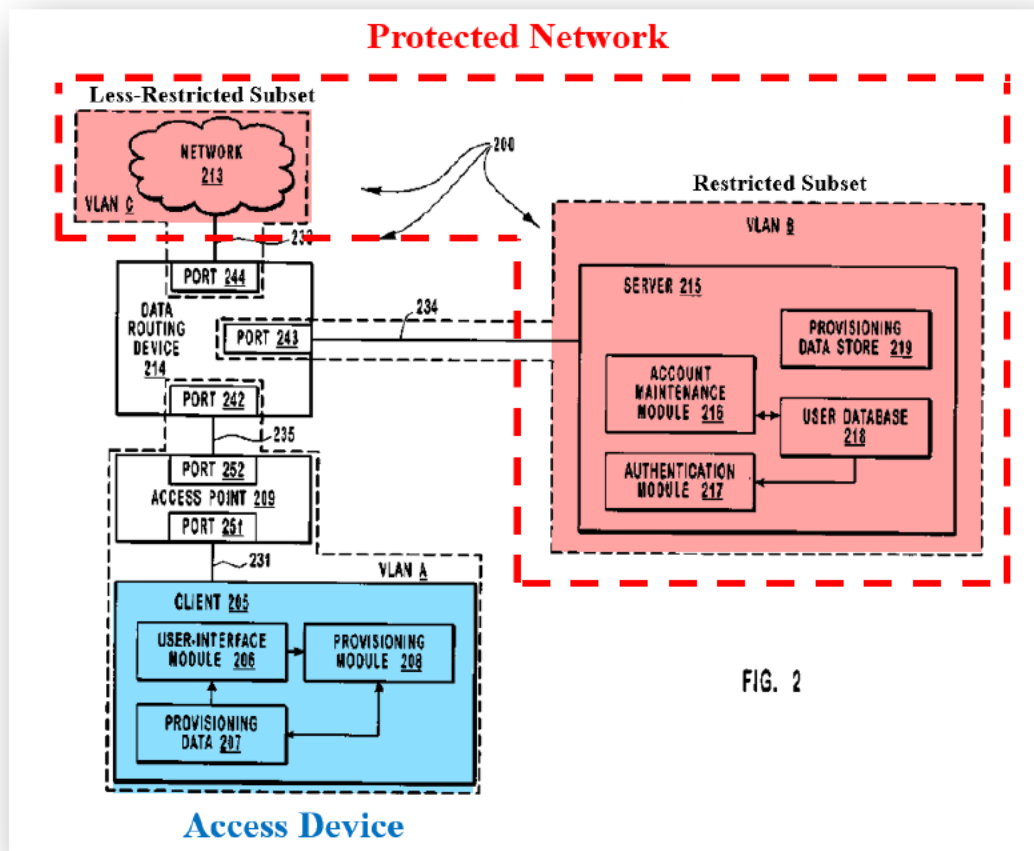


FIG. 2

Ex.1205, Figure 2 (annotated); Ex.1203, ¶71.

Accordingly, Krantz teaches or suggests this limitation. Ex.1203, ¶72.

ii. *[1.1] performing an authentication...*

Krantz discloses: “[a] client sends credentials to the server to attempt to authenticate with the server.” Ex.1205, [0016]. Specifically, “[s]ending credentials can include sending an Extensible Authentication Protocol (‘EAP’)

Response/Identity message from the client to the server [*performing an authentication using an EAP protocol from the device*']. If the client is attempting to connect to a network via an access point, the **EAP Response/Identity message** may be encapsulated within some other type of message that can be transferred through the access point. ... The access point may also be configured to **block communications from the client that use protocols other than EAP and 802.1X.**" Ex.1205, [0018]; Ex.1203, ¶73.

The Krantz system "*performs an authentication.*" For instance, server 215 in Krantz is shown below in gray (a "*gatekeeper*" as discussed in claim [1.4]). Ex.1203, ¶74.

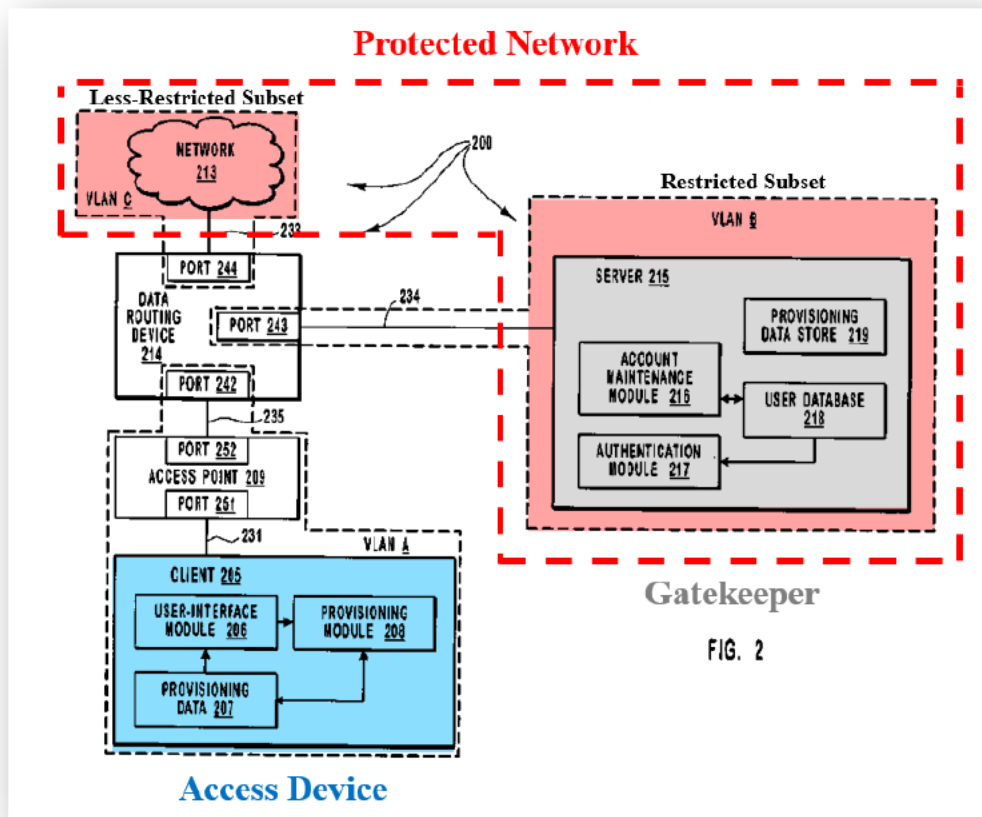


FIG. 2

Ex.1205, Figure 2 (annotated).

Krantz discloses that authentication of the device can occur in a variety of ways, including exchanging a user-identifier/password, **EAP-messages** to pass certificate keys, as well as cipher suites; Krantz discloses that the “*EAP protocol [is] from the device.*” Ex.1205, [0073] (“**Server 215 can receive the EAPOL packet** ... 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 ... the **EAP-Response/Identity message** can be

transferred through these other servers to server 215.”); [0074] (“Depending on the particular **EAP type**, server 215 can **respond to the EAP-Response/Identity message** ... 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.1205, [0058], [0067]-[0072], [0078], [0099]-[0101]; Ex.1203, ¶75.

Krantz discloses that “[w]hen **EAP-MSChap V2** is indicated, the MS Chap V2 Parameters element at line 67 can be included in a configuration sub-file to indicate **whether or not operating system credentials should be used for authentication.**” Ex.1205, [0099]; Ex.1203, ¶76.

Krantz explains that EAP-TLS and EAP-MSCHAP V2 can be required from a client seeking access and authorization. Ex.1205, [0099] (“[B]oth of the elements . . . can be included in a configuration sub-file to indicate different EAP types, such as, for example, **EAP-TLS and EAP Microsoft/Challenge/Replay Handshake Protocol Version** (‘EAP-MSChapV2’)).” Ex.1203, ¶77.

As Dr. Houh explains, a POSITA would have understood each of the above techniques in Krantz to disclose authenticating the device and/or user of client 205

(“*performing an authentication using an EAP protocol from the device.*”) before authorization is granted:

EAP-TLS. TLS (SSL) is [] used... The computer first authenticates to the network using a machine certificate; ... In Windows, PEAP supports MS-CHAPv2 in addition to TLS. **PEAP-MSCHAPv2 uses machine and user credentials for authentication.** ... Certificates are still required for the authentication sever (IAS) and are used for server-to-client authentication; credentials, **carried inside MSCHAPv2, are used for client-to-server authentication.**

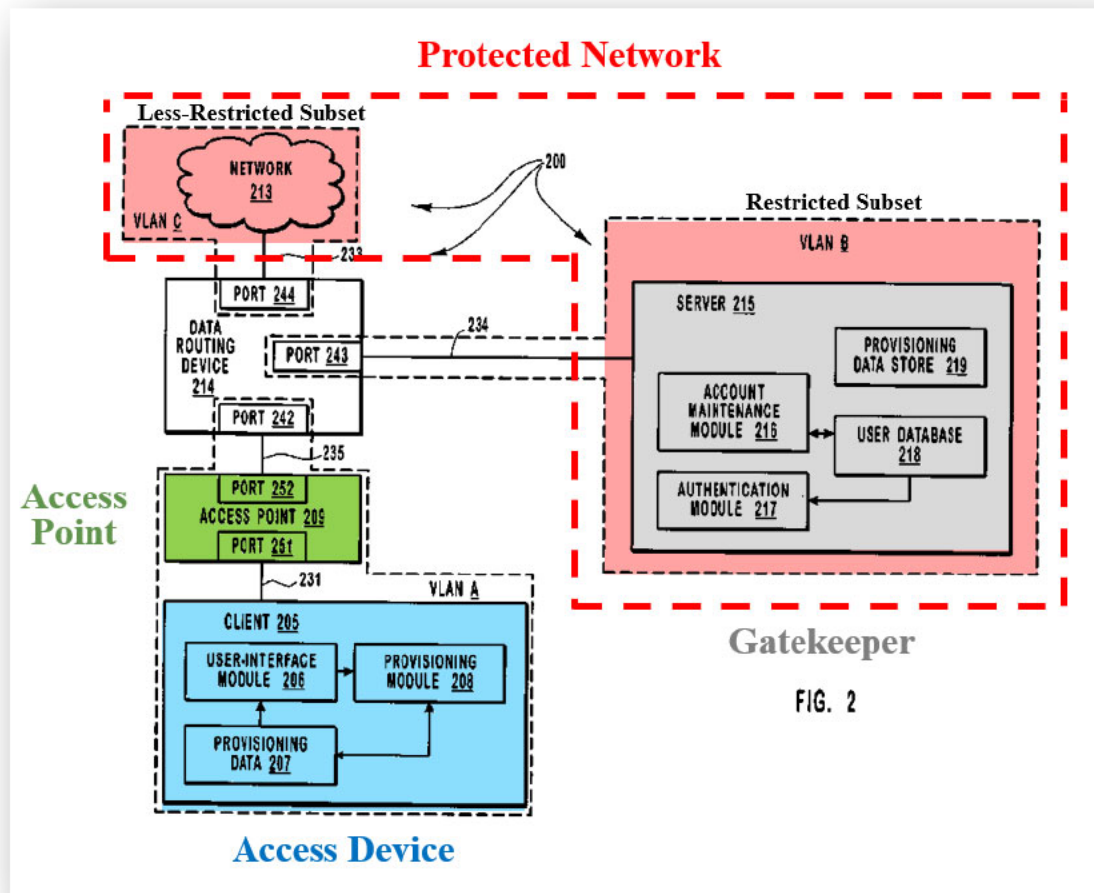
Ex.1217, 2; Ex.1203, ¶78.

Accordingly, Krantz teaches or suggests this limitation. Ex.1203, ¶79.

iii. [1.2] the device being connected...

The 444 Patent explains: “Access Point 215 is, for example, a network switch, a wireless access point, a remote access virtual private network (VPN), secure socket layer VPN, firewall, or the like... **Access Point 215 includes a series of communication ports . . . configured for communication with devices such as Access Device 230, Router 220, Less-Restricted Subset 210 and/or Restricted Subset 205.**” Ex.1201, 7:62-8:3; Ex.1203, ¶81.

Like the 444 Patent, the access “*device*” (client 205) disclosed in Krantz is “*connected via a computer network to an access point*”—annotated in green as “Access Point 209,” in Figure 2:



Ex.1205, Figure 2 (annotated); Ex.1203, ¶82.

Krantz explains: “[n]etwork architecture [“computer network”] also includes access point 209. Access point 209 can be a wired or wireless access point that facilitates communication between client 205 [“device being connected via a computer network”] and data routing device 214 ... access point 209 is connected to client 205 by corresponding logical communication link 231 [i.e., a “computer network connect[ion]” between “device” and “access point”]. ... Access point 209

includes ports 251 and 252. Data can be transferred between access port [sic]⁵ 209 and client 205 through port 251. Likewise, data can be transferred between access point 209 and data routing device 214 through port 252.” Ex.1205, at [0063]; Ex.1203, ¶83.

With respect to logical communication link 231, Krantz elaborates:

A logical communication link can include portions of a system bus, **a local area network (e.g., an Ethernet network), a wide area network, the Internet, combinations thereof**, or portions of any other path that may facilitate the transport of electronic data. ...

Ex.1205, [0038]; Ex.1203, ¶84.

Krantz discloses that “*access point [is] configured to use an 802.1x protocol.*” Krantz explains that “[i]n some embodiments, EAP messages are encapsulated within other protocols One protocol used for encapsulation is the **802.1x protocol, which may be referred to as EAP encapsulation over LANs (‘EAPOL’)**. **Access point 209** and data routing device 214 **can be configured to support EAPOL.**” Ex.1205, [0069]; *see also* Ex.1205, [0072] (“**Access point 209 can enable the transfer of EAPOL packets** for port 251. That is, EAPOL packets

⁵ Typo in original. “Access port 209” should refer to “Access **Point** 209.”

received at port **251** can be transferred out of access point **209** at port 252.”). Ex.1203, ¶85.

Accordingly, Krantz teaches or suggests this limitation. Ex.1203, ¶86.

iv. *[1.3] sending a request...*

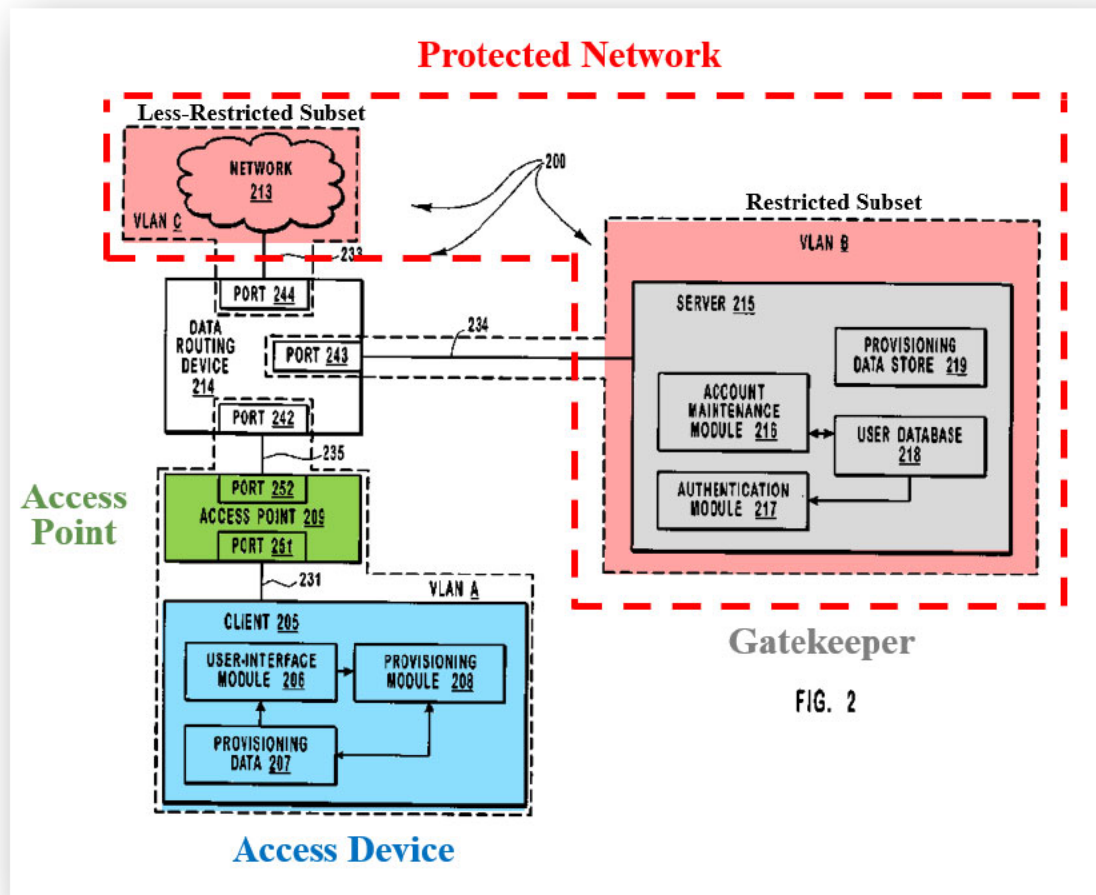
Krantz does not expressly disclose “*sending a request for audit data to an agent running on the device*,” but a POSITA would have found it obvious in view of Herrmann. As discussed for claim [1.1], Krantz discloses a method for “*auditing a device*.” Ex.1203, ¶87.

Krantz discloses that “client 205 and server 215 **exchange EAP-messages** to pass certificates, keys, and supported cipher suites. Depending on the EAP type, other credential information may also be exchanged between client 205 and server 215.” Ex.1205, [0074]. Additionally, a handshake protocol may be used between the access device and gatekeeper:

A configuration sub-file to indicate a type of EAP [is] used to authenticate a server with a client and/or to authenticate a client with a server... such as, for example, **EAP-TLS and EAP Microsoft Challenge/Replay Handshake Protocol Version (“EAP-MSChapV2”)**...

Ex.1205 [0099]; *see also*, Ex.1205, [0013], [0032], [0072], [0078] (outlining other security policies that may be implemented (specifying certain “*audit data*”), e.g.,

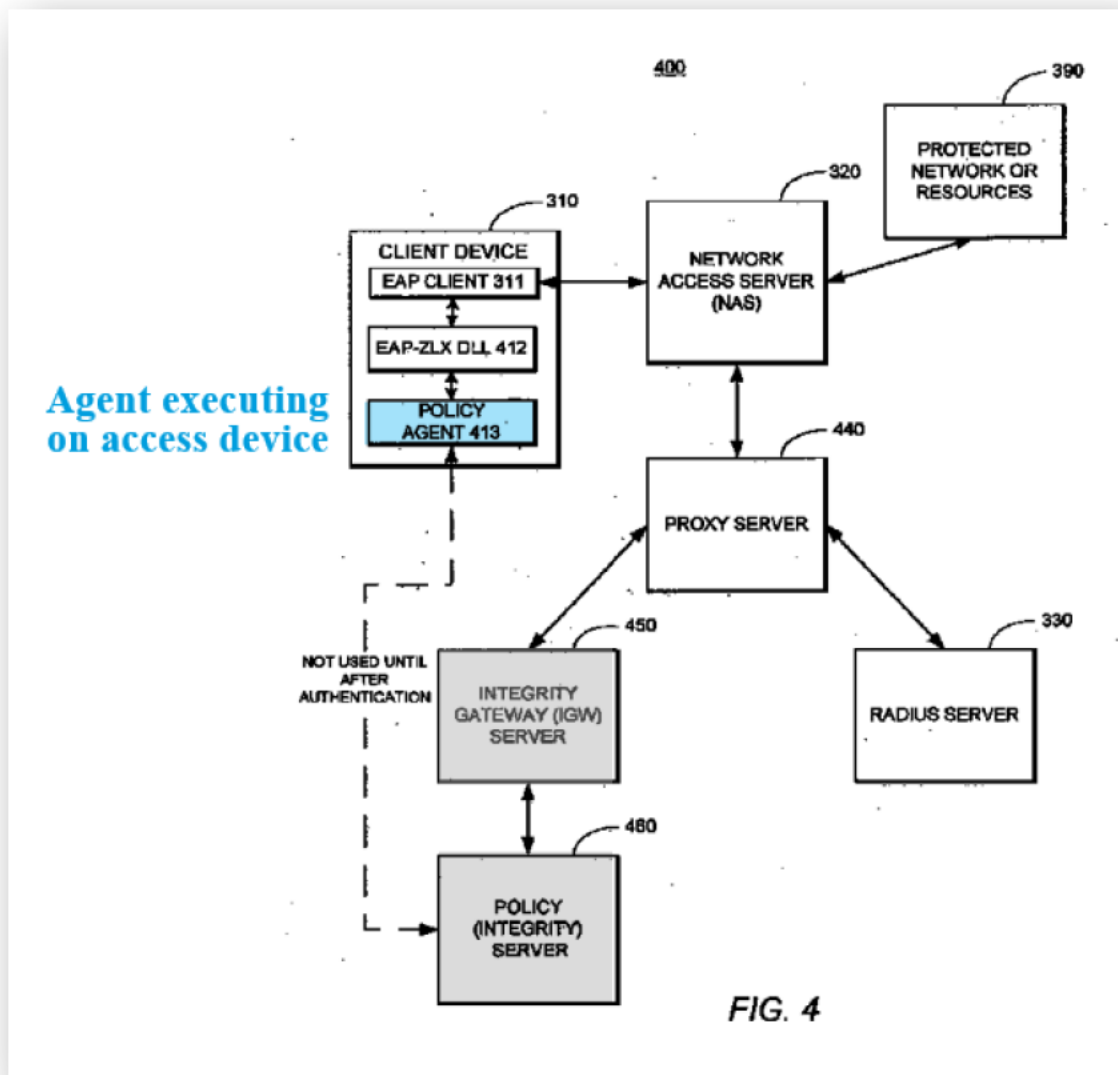
requiring a user download provisioning files to access resources). The request for “*audit data*” is **sent from the server to the client device** in Krantz. As shown below, server 215 can “*send a request for audit data*,” e.g., exchange EAP-messages, via logical communication link 234, 235, and 251 to client device 205. Ex.1205, [0060], [0063]; *see also*, Ex.1205, [0073] (EAP messages can be transferred via communication link 234) and [0074] (server 215 may make requests for credentials to client 205). Therefore, Krantz teaches or suggests “*sending a request for audit data*.” Ex.1203, ¶88.



Ex.1205, Figure 2 (annotated); Ex.1203, ¶88.

The “*audit data*” (EAP-messages, operating system credentials, certificates, keys, and supported cipher suites, etc.) disclosed in Krantz would be retrieved by, e.g., utilizing a client “*agent*.” Ex.1203, ¶89. Krantz does not expressly 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 above in §VII.C. Ex.1203, ¶89.

Specifically, Herrmann discloses “POLICY AGENT 413” (i.e., an “agent”) (in blue) executing on client access device (i.e., “running on the device”), interacting with “POLICY (INTEGRITY) SERVER 460” and “INTEGRITY GATEWAY (IGW) SERVER 450” (collectively emphasized in gray) as shown below.



Ex.1206, Fig. 4 (annotated); Ex.1203, ¶90.

Herrmann discloses: “policy agent (or integrity agent) 413 [is used] to **retrieve information about the current security policy in operation on the client device 310** [*i.e.*, “*request for audit data*”].” Ex.1206, [0064]. Herrmann explains: “[i]n response to a message from the IGW server 450 (or a subsequent message from the policy agent 413 on the client device 310) [*i.e.*, in response to ‘*sending a request for audit data to an agent running on the device*’], the policy server 460 evaluates [if] the client device 310 has a correct, up-to-date version of the applicable security policy.” Ex.1206, [0067]. The policy server is notified by the **client, containing policy agent 413**, through periodic status messages called “IA_HEARTBEAT(s)” to authenticate the access device. Ex.1206, [0080], [0098]. Herrmann’s disclosure is consistent with the 444 Patent’s disclosure of a software agent configured to monitor local security and report results to a policy auditor. Ex.1201, 11:60-64; Ex.1203, ¶91.

A POSITA would be motivated to add the security policy agent of Herrmann to the client device of Krantz for several reasons. As discussed previously (*see* §VII.C) two stated goals of Krantz involve automation and security. Ex.1205, [0014], [0019]. Because of these similarities, Dr. Houh explains that a POSITA would have recognized that the policy **agent** of Herrmann would be complimentary

to Krantz's system in providing automated methods of network security. Ex.1203, ¶92.

Lastly, there would be a reasonable expectation of success in adding the policy agent of Herrmann to the client device of Krantz, as Herrmann 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.1206, [0064]; [Fig. 4]. This is the same protocol used in Krantz. Ex.1205, [0018] (“Sending credentials can include sending an Extensible Authentication Protocol (**EAP**) **Response/Identity message** from the client to the server.”). Additionally, this modification to Krantz can be implemented as a simple software modification to include a policy agent. Ex.1203, ¶93.

Accordingly, Krantz and Herrmann render obvious this limitation. Ex.1203, ¶94.

v. *[1.4] receiving the audit data...*

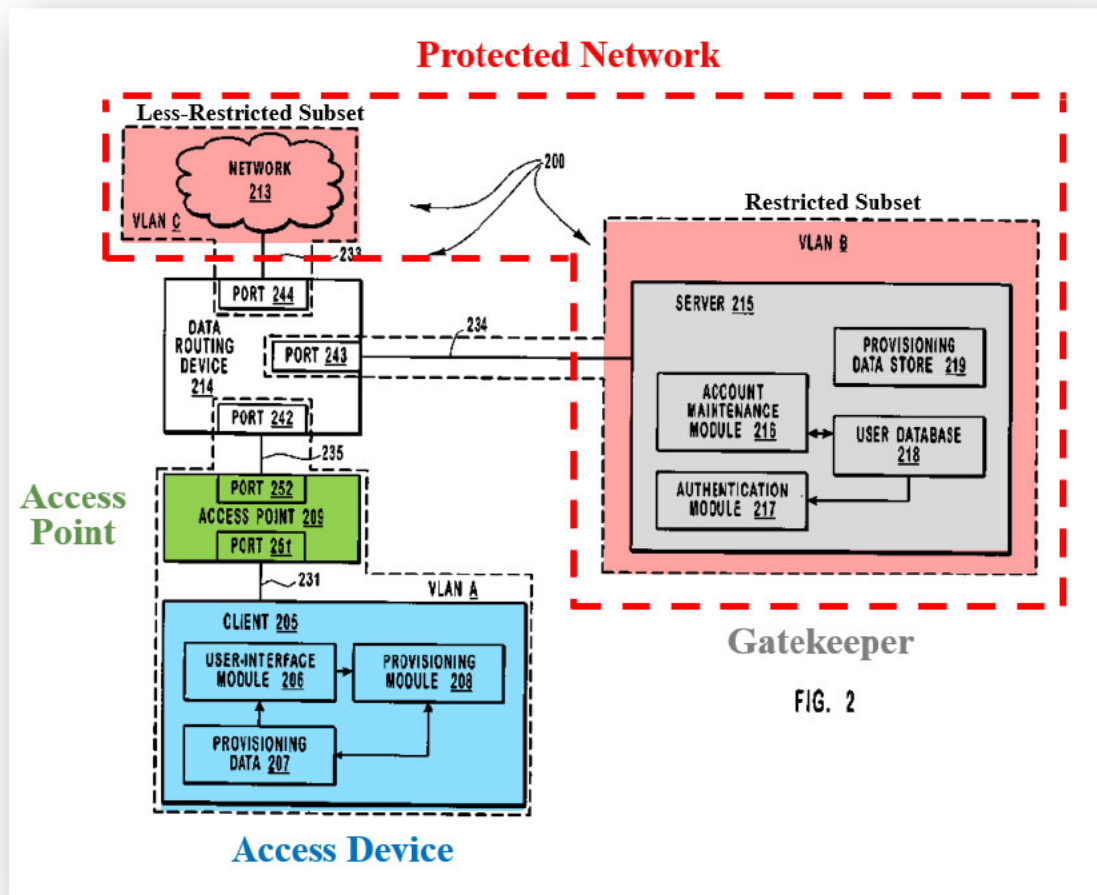
As discussed in claim [1.3], Krantz and Herrmann disclose “*sending a request for audit data to an agent running on the device.*” Krantz and Herrmann also disclose “*receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been*

obtained by the agent.” The limitations would have been obvious in view of Herrmann, and a POSITA would have been motivated to combine Krantz and Herrmann for reasons stated above in §VII.C. Ex.1203, ¶95.

Initially, the Abstract of the 444 Patent explains: “[t]he gatekeeper⁶ is configured to enforce a security policy ... before granting access to a less-restricted subset of the computing network.” Ex.1201, Abstract; Ex.1203, ¶96.

Krantz similarly discloses that “[a] client attempts to become authorized to access resources located on a second network ... [and] sends credentials to an access point that is communicatively coupled to a server (located on a first network or located on the second network) that can authorize access to the second network.” Ex.1205, [0031]. This is generally shown in Fig. 2:

⁶ Notably, Applicant admits that this Gatekeeper is prior art. Ex.1201, 2:34-36 (“GateKeeper ... [is] practiced in the prior art.”).



Ex.1205, Figure 2 (annotated); Ex.1203, ¶97.

- a. “receiving the audit data at a gatekeeper configured to control access to a network”

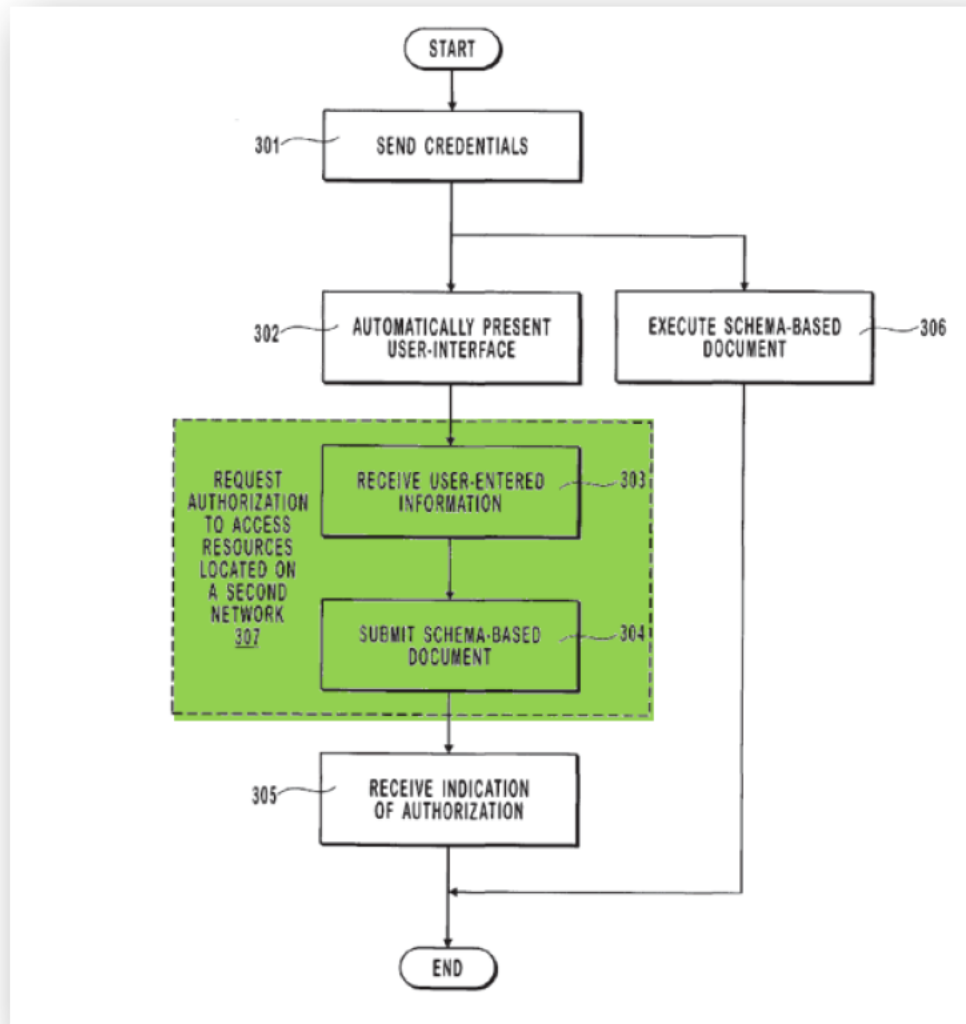
Krantz discloses that “a server has the functionality to authorize access” to a network and/or selected elements within a network after the client 205 (“device”) sends credentials to the server 215 (“receiving audit data at a gatekeeper”). Ex.1205, [0016], [0071]. Krantz discloses that the “server (based at least in part on received credentials) may authorize the client for at least partial access to the

single network.” Ex.1205, [0017]; *see also* [0074]-[0076], [0104], [0107]-[0109] (describing techniques for requesting access). For example, to gain access to the protected network, Krantz includes a server (“*gatekeeper*”) which can authorize access to the protected network resources based on credentials supplied by the device or user. Ex.1205, [0016], [0068]-[0071], [0099], [0104], [0107]-[0109]; Ex.1203, ¶¶98-99.

The credentials “can include sending an Extensible Authentication Protocol (‘EAP’) Response/Identity message from the client to the server. If the client is attempting to connect to a network via an access point, the EAP Response/Identity message may be encapsulated within some other type of message that can be transferred through the access point.” Ex.1205, [0018]. Other “*audit data*” provided by Krantz’s “*device*” may include, “user-identifier[s] and password[s]” (Ex.1205, [0076]) or “*device*” credentials such as operating system or other credentials used to authenticate a device. Ex.1205, [0067]-[0074], [0099]-[0100]; Ex.1203, ¶100.

Krantz’s 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.1205, [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.1205, [0104]. Krantz continues: “[s]tep 307 may include any corresponding acts for accomplishing the result of requesting authorization to access resources located on the second network.” Ex.1205, [0104].



Ex.1205, Figure 3 (annotated); Ex.1203, ¶101.

Krantz explains step 307 (above) “includes [the] corresponding act of receiving user-entered information (act 303). A presented user-interface can be used

to receive user-entered information (e.g., user-identifier, password, name, address, credit card information, etc.) from a user at client 205” and step 307 further includes “a corresponding act of submitting a schema-based document (act 304).” Ex.1205, [0104]. For instance, a client **submitting** a first schema-based document that includes user-entered information **to a server**. [*i.e.*, “*receiving audit data at a gatekeeper*”]. Ex.1205, [0105]; Ex.1203, ¶102.

The “*device*”—*i.e.*, “Client 205”—sending “*audit data*” to server 215 (“*gatekeeper*”) in Krantz is depicted in Figure 2 in blue below:

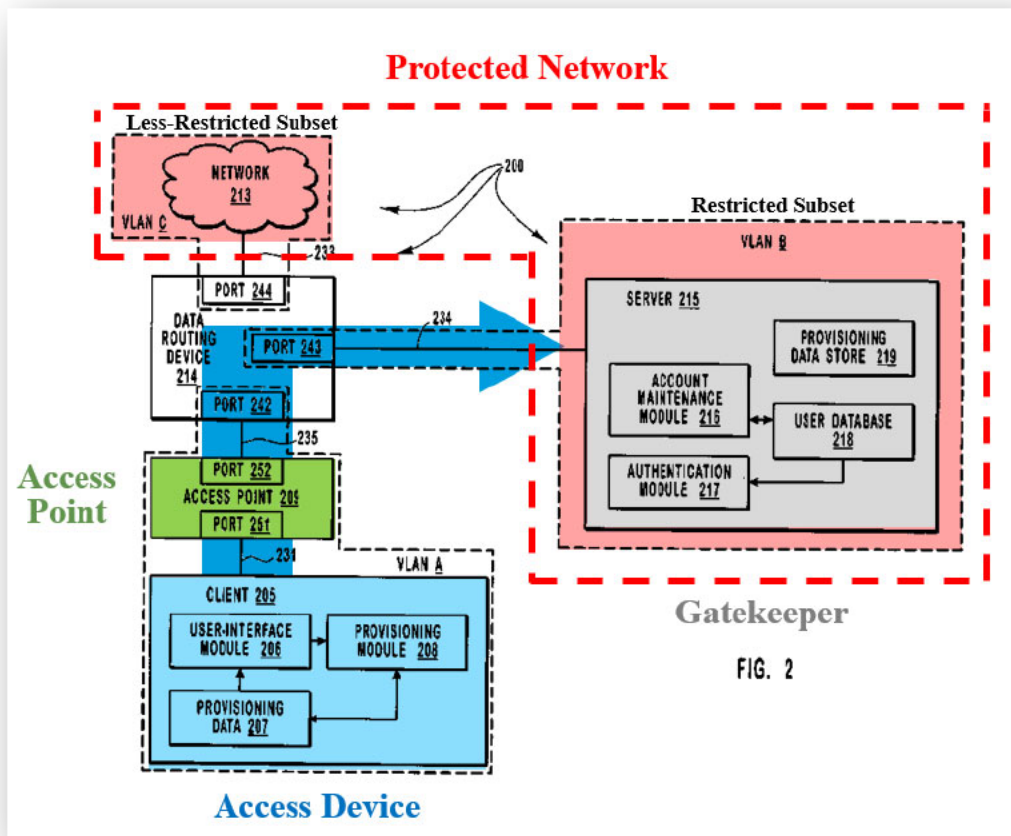


FIG. 2

Ex.1205, Figure 2 (annotated); Ex.1203, ¶103.

Krantz therefore teaches or suggests “receiving audit data at a gatekeeper. . .” Ex.1203, ¶104.

To the extent one asserts Krantz does not teach or suggest “receiving audit data,” it would have been obvious based on Krantz and Herrmann, and a POSITA would have been motivated to combine Krantz with Herrmann for the reasons described above. See §VII.C; Ex.1203, ¶105.

It would have been obvious to include Herrmann's techniques for "receiving *audit data at a gatekeeper*" (e.g., evaluating whether a device includes antivirus software) in the system of Krantz. The Krantz system already similarly discloses that "access point 209 may block [] protocols ... from being transferred **until client 205 is authenticated (and authorized)**. Ex.1205, [0072]. It also discloses that "[w]hen credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) **and compare the credentials to entries in user database 218.**" Ex.1205, [0076]; Ex.1203, ¶106.

A POSITA would have understood that checking for anti-virus software would merely be an additional item for server 215 ("*gatekeeper*") to check in the authentication process disclosed by Krantz. Like Krantz, Herrmann discloses a "policy server 460 [which] may enforce a variety of different types of security policies or rules." Ex.1206, [0068]. One being "a policy requiring that a **specific virus protection program** is operational on each client device that is connected to a network." Ex.1206, [0012] (emphasizing criticality that all machines in a network maintain updated antivirus software so network is not infiltrated by new viruses). A POSITA would be motivated to modify the system of Krantz to include the additional security policy requiring proof of ("*audit data*") a specific virus-protection program because Krantz is focused on network authentication/security. Ex.1205, [Abstract].

Krantz and Herrmann therefore also disclose “*receiving audit data at a gatekeeper. . . .*” Ex.1203, ¶107.

Krantz also teaches or suggests “. . . *a gatekeeper configured to control access to a network*” The “*network*” of the 444 Patent can include multiple networks as opposed to single network implementation. For instance, “[i]n various embodiments, Protected Network 200 includes . . . private network, local area network, wide area network, wireless network, communication network . . . and/or the like.” Ex.1201, 6:8-13; Ex.1203, ¶108.

The network disclosed in Krantz is such a “*network*.” As demonstrated below, VLAN B and VLAN C of Krantz (e.g., as depicted in Fig. 4) constitute a protected network consistent with the “*network*” of the 444 Patent. Krantz explains that the disclosed networks “can be implemented using any number of techniques, such as, for example, **Virtual Local Area Networks (“VLANs”), Internet Protocol (“IP”) filtering, Virtual Private Networks (“VPNs”), or use of IPSecurity (“IPSec) protocols.**” Ex.1205, [0017]. These techniques are methods for creating a protected “*network*” because they facilitate, e.g., the access control capabilities described in Krantz. Ex.1205, [0017] (“[T]he server (based [] on received credentials) may authorize the client for at least partial access to the single network, such as, for

example, by authorizing client access to selected computer systems or modules on the single network.”); Ex.1203, ¶109.

Krantz’s system can be “*configured to control access*” to this protected “*network*.” For instance, Krantz discloses network access protocols whereby “[a] server includes the **functionality to authorize clients to access a second network** ...” Ex.1205, [0016]. Krantz elaborates: “[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.1205, [0016]; Ex.1203, ¶110.

Based on Krantz, a POSITA would understand that by combining (either physically or logically) the first/second networks, a “network” is formed, as explained in Krantz:

[A] “logical communication link” is [] any communication path [enabling] transport of electronic data between two entities such as computer systems or modules. **The actual physical representation of a communication path between two entities is not important and can change over time. A logical communication link can include portions of . . . a local area network (e.g., an Ethernet network), a wide area network, the Internet,**

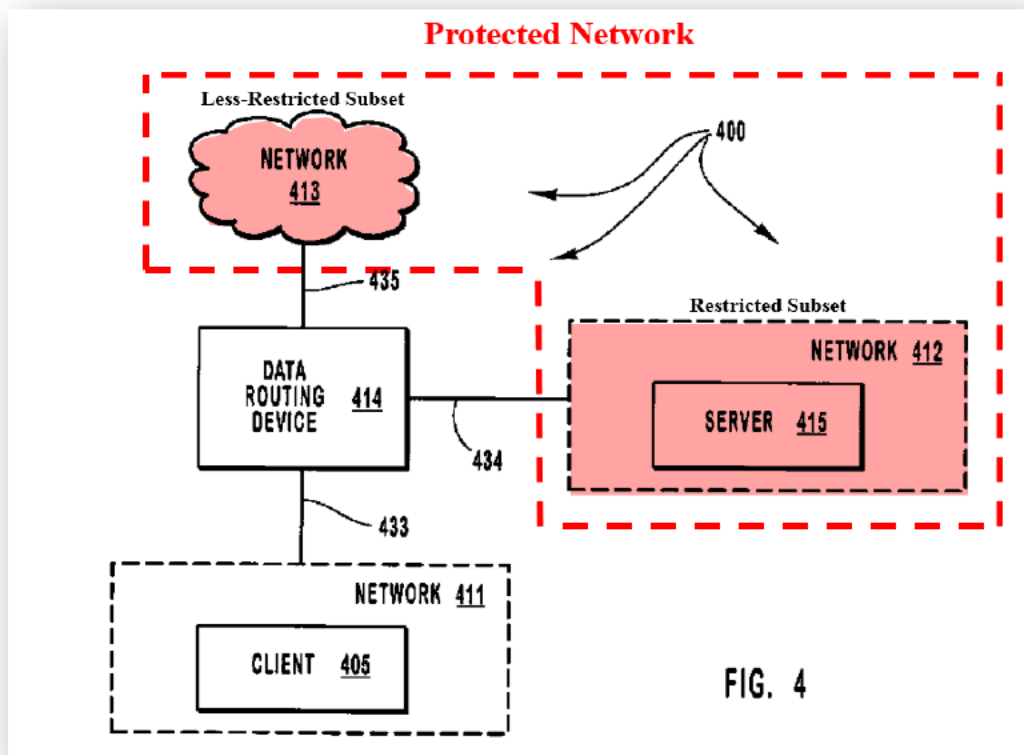
combinations thereof, or portions of any other path that may facilitate the transport of electronic data. . . .

Ex.1205, [0038]; Ex.1203, ¶111.

Combining two (or more) physical networks was commonly done and well-known to POSITAs at the time. Ex.1211, 223 (“logical network” is “[a] network as it appears to the user ... the network could be composed of two or more physical networks, or portions of these... linked and coordinated [such] that they appear to be a unit.”); Ex.1212, 317 (the “difference between a network as logical or physical is sometimes subtle because the physical network (the actual layout of hardware and cabling) doesn’t necessarily resemble the logical network (the path followed by transmissions.”); Ex.1203, ¶112.

This is consistent with the 444 Patent, i.e., the “*network*” may be “**physically or logically divided** into a restricted subset and one or more less-restricted subsets.” Ex.1201, 2:56-58. The 444 Patent elaborates that the restricted and less-restricted subsets “are [typically] characterized by Virtual Local Area Networks (e.g., VLANs),” (Ex.1201, 3:3-8), and explains that the protected “*network*” may include “access restrictions” (i.e., the claimed “*access control*”). Ex.1201, 6:25-41; Ex.1203, ¶113.

The protected “network” described in Krantz is depicted in Figures 4 and 2, reproduced and annotated below.



Ex.1205, Figure 4 (annotated).

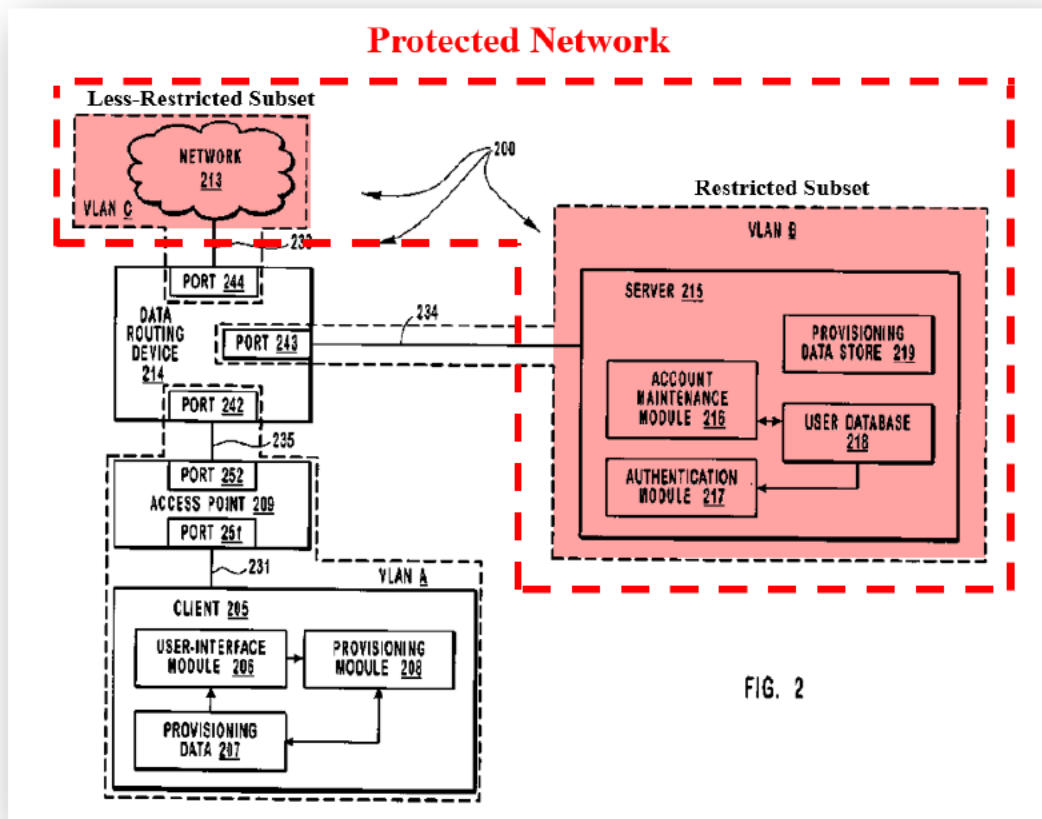


FIG. 2

Ex.1205, Figure 2 (annotated); Ex.1203, ¶114..

Figure 4 is “an example of a network architecture 400 that can provide access to a first network while restricting access to a second network.” Ex.1205, 5:65-6:2. Krantz explains that “in some embodiments, access to resources located in network 413 can be restricted [through] Virtual Local Networks (“VLANs”).” Ex.1205, [0052]; *see also* [0054] (explaining that access to resources located on network 413 can also be restricted using VPNs). Figure 2 provides an example of this embodiment implementing the general architecture of Figure 4 and “using VLAN

techniques,” which “can facilitate increasing the level of automation when provisioning a client.” Ex.1205, [0057]. Figure 2 and its description provide certain specific techniques to be implemented in Krantz’s networking architecture. *See* Ex.1205, Figures 2 and 4 and related descriptions. Thus, the combination of Network 413 and Network 412 (also annotated as VLAN C and VLAN B) constitute a single logical “*network*.” Given the similar disclosure of Figure 2 and the 444 Patent, analysis in this petition will focus on Figure 2 and its description. Ex.1203, ¶115.

To the extent one asserts that the “*network*” is required to be a single network, Krantz explains that its techniques regarding “*control[ling] access to a network*” can also be used “**within a single network**.” Ex.1205, [0017]; *see also* Ex.1205, [0055]; Ex.1203, ¶116.

As Krantz explains, the system “**may authorize the client for at least partial access to the single network**” (“*configured to control access to a network*”), and one example of granting or “*control[ling]*” such “*access*” in Krantz is “by authorizing client access to selected computer systems or modules on the single network.” Ex.1205, [0017]; *see also* Ex.1205, [0016], [0071] [0074]-[0076] (“If credential information matches an entry in user database 218, 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.1203, ¶117.

Accordingly, Krantz teaches or suggests that “. . . *a gatekeeper configured to control access to a network* . . . Ex.1203, ¶118.

- b. Receiving . . . “from the agent, the audit data pertaining to the device and having been obtained by the agent,”

Krantz does not expressly disclose gatekeeper receiving this claim element, but it would have been obvious based on the teachings of Krantz and Herrmann. A POSITA would have been motivated to combine Krantz with Herrmann for the reasons described above. *See* §VII.C; Ex.1203, ¶119.

Krantz discloses that “[w]hen credentials are sent to **server 215** [the “*gatekeeper*”], **authentication module 217 can receive the credentials (e.g., user-identifier and password)** [“*receiving ... audit data*”] and compare the credentials to entries in user database 218. If credential information matches an entry in user database 218, the identity of a user is authenticated (server 215 believes that the user represented by the user-identifier is the user who entered the credential information). . . .” Ex.1205, [0076]. In addition, this “*audit data*”—including “*audit data*” related to the device—is analyzed in response to the client requesting access to resources on

VLAN C [*“gatekeeper configured to control access to a network”*]. E.g., Ex.1205, [0016-0018], [0071]-[0072], [0076], [0104]-[0109]; Ex.1203, ¶120.

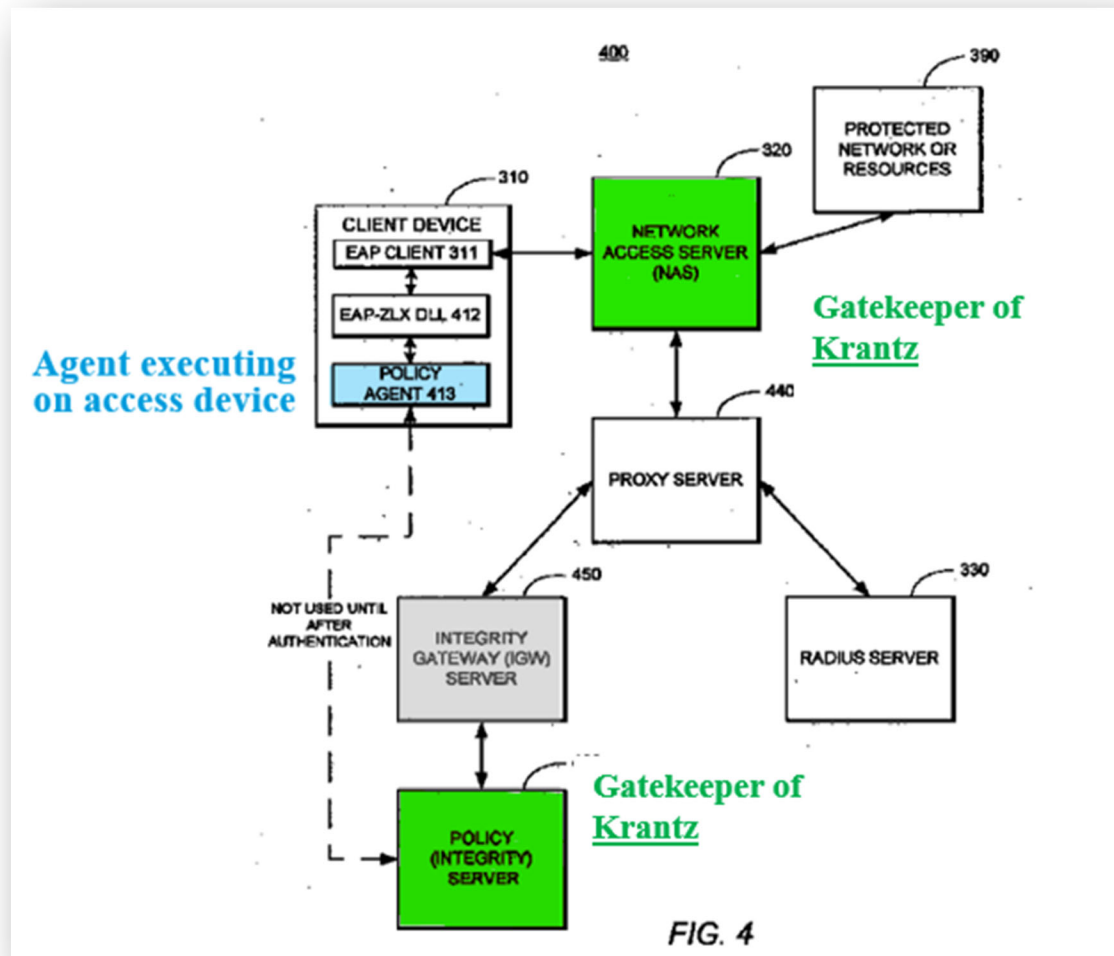
As explained above in claim element [1.3], Herrmann discloses that “**policy agent (or integrity agent) 413 to retrieve information about the current security policy in operation on the client device 310** [i.e., “*audit data pertaining to the device and having been obtained by the agent*”].” Ex.1206, [0064]. This “*audit data*” includes “a policy requiring that a **specific virus protection program is operational on each client device** [i.e., “*audit data pertaining to the device*”] that is connected to a network.” Ex.1206, [0012]; Ex.1203, ¶121.

Herrmann explains that “[i]n 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 [i.e., *audit data pertaining to the device*”].” Ex.1206, [0067]. The **policy server is notified by the client, containing policy agent 413** [i.e., “*receiving the audit data at a gatekeeper ... from the agent*”], **through periodic status messages called “IA_HEARTBEAT(s)” in order to authenticate the access device** [*“configured to control access to a network”*]. Ex.1203, ¶122.

As Dr. Houh explains, the agent of Herrmann can obtain the “*audit data pertaining to the device*” (e.g., antivirus software and applicable security policy status) and the gatekeeper can *receiv[e] the audit data “from the agent”* through a periodic check where the audit data is “*obtained by the agent*” from the device. As shown below, the combined disclosures of Krantz and Herrmann disclose this limitation. Krantz and Herrmann disclose “*receiving the audit data at a gatekeeper configured to control access to a network*” as discussed *supra*. Herrmann discloses how this “*audit data pertaining to the device [is] obtained by the agent*” (shown below in blue). The agent can transmit the audit data to a gatekeeper so the gatekeeper “*receive[s the audit data] from the agent.*” As shown below in green, Herrmann includes two direct connections to the client device (the “Network Access Server” and the “Policy (Integrity) Server”). Ex.1203, ¶123.

The server components in Herrmann are similar to the “*gatekeeper*” of Krantz. Herrmann explains that “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.1206, [0053]; *see also*, Ex.1206, [0065] (describing the “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 (i.e., gatekeeper) of Krantz.



Ex.1206, Fig. 4 (annotated); Ex.1203, ¶124.

Therefore, Krantz and Herrmann teach or suggest receiving the audit data at a gatekeeper ... “from the agent, the audit data pertaining to the device and having been obtained by the agent.” Ex.1206, [0080], [0098]; Ex.1203, ¶125.

A POSITA would be motivated to add the security policy agent of Herrmann to the client device of Krantz for several reasons. As explained (*see* §VII.C), two stated goals of Krantz are automation and security. Ex.1205, [0014], [0019]. Because of this, Dr. Houh explains that policy **agent** of Herrmann would be complimentary to the system of Krantz, as it would automate means of providing network security. Ex.1203, ¶126.

There would be a reasonable expectation of success for adding the policy agent of Herrmann to the client device of Krantz, as Herrmann itself describes the policy agent as a “client-side component” that can communicate with an “EAP-ZLX extension DLL [which] is an implementation of the EAP protocol that is utilized to provide support for security policy negotiation and enforcement.” *E.g.*, Ex.1206, [0064]; [Fig. 4]. This is the same protocol used in Krantz. Ex.1205, [0018] (“Sending credentials can include sending an Extensible Authentication Protocol (‘EAP’) Response/Identity message from the client to the server.”). Ex.1203, ¶127.

Accordingly, Krantz and Herrmann renders obvious this limitation. Ex.1203, ¶128.

vi. [1.5] applying a security policy...

Krantz discloses several specific “*security polic[ies]*” that can “*take place under control of the 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** that is associated with a user-identifier. A user of client 205 can respond by providing a password to server 215.” Ex.1205, [0074]; Ex.1203, ¶130.

With respect to Fig. 2, Krantz discloses that “[w]hen credentials are sent to server 215 [a “*gatekeeper*”], **authentication module 217 can receive the credentials** (e.g., user-identifier and password) **and compare the credentials to entries in user database 218. If credential information matches an entry in user database 218, the identity of a user is authenticated** [*“the applying of the security policy taking place under control of the gatekeeper”*] (server 215 believes that the user represented by the user-identifier is the user who entered the credential information). If an authenticated user of client 205 is authorized to access resources located on VLAN C ... client 205 can then be authorized to access resources located on VLAN C.” Ex.1205, [0076]. In addition, this “*security policy*” is in response to the client requesting access to resources on VLAN C. Ex.1205, [0016-0018], [0071]-[0072], [0076], [0104]-[0109]; Ex.1203, ¶131.

The gatekeeper of Krantz can enforce *security policies* including “*at least one requirement pertaining to the audit data.*” For example, “[i]t may also be that **client**

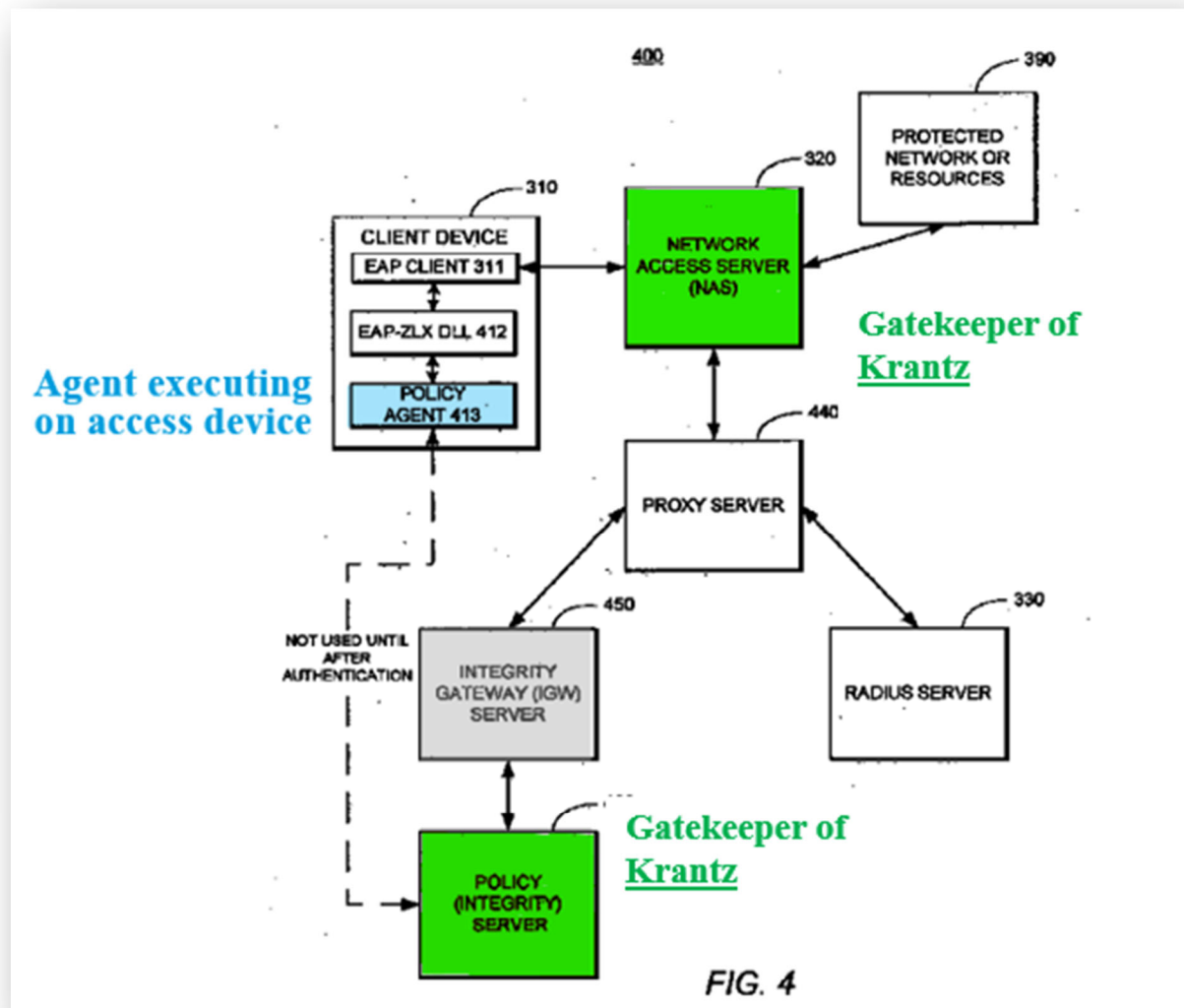
205 and server 215 exchange EAP-messages to pass certificates, keys, and supported cipher suites [“audit data”]. Depending on the EAP type, other credential information may also be exchanged between client 205 and server 215.” Ex.1205, [0074]; Ex.1203, ¶132.

Additionally, the combined Krantz/Herrmann system would include “*applying a security policy that includes at least one requirements pertaining to the audit data*” such as requiring antivirus software as described in Herrmann. Herrmann, for example, specifically discloses: “[n]ew viruses are frequently released that cannot be identified using older anti-virus engines and definition files. **It becomes critical, therefore, to promptly update anti-virus applications on all machines in a network** in a timely fashion before the network is infiltrated by a newly released virus.” Ex.1206, [0012]; Ex.1203, ¶133.

Herrmann also discloses that “a network administrator **may require all users accessing the network to implement a virus definition update (e.g., DAT file)** that is targeted at a particular virus.” Ex.1206, [0071]. This may be implemented using security rules and **checking system data [“audit data”] for connecting devices to ascertain compliance.** *Id.*, [0068] (“The policy server 460 may enforce a variety of different types of security policies or rules ... [including] rules which require client devices connecting to a given network **to be using particular security**

or anti-virus programs. For example, a system administrator may establish a policy requiring that **a specific virus protection program is operational on each client device that is connected to a network.**”); Ex.1203, ¶134.

A POSITA would have found it obvious to implement “*applying of the security policy taking place under control of the gatekeeper*” as described *supra* with respect to Herrmann, in the gatekeeper of Krantz. The server components in Herrmann are similar to the gatekeeper of Krantz. For instance, Herrmann explains that “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.1206, [0053]; *see also*, Ex.1206, [0065] (describing the “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...” This is similar to the server 215 “*gatekeeper*” of Krantz. Additionally, both Herrmann and Krantz discuss logical implementations of server techniques and therefore the “*gatekeeper*” of Krantz would easily integrate with the policy agent of Herrmann, as again depicted below.



Ex.1206, Fig. 4 (annotated); *see also*, Ex.1205, [0038], [0051] (describing logical communication links and computer systems); Ex.1206, [0026] (with reference to “an environment in which the present invention is implemented” an Open Systems Interconnection Reference Model is used, which “is a **logical structure** for

communication systems standardized by the International Standards Organization (ISO) as ISO/IEC standard 7498-1:1994.”); Ex.1203, ¶135.

Krantz discloses “*at least one requirement pertaining to the authentication.*” For instance, “[w]hen EAP-MSChapV2 [Extensible **Authentication** Protocol] is indicated, the MSChapV2 Parameters element at line 67 can be included in a configuration sub-file to indicate whether or not operating system credentials should be used **for authentication**” (security policy includes ... “*at least one requirement pertaining to the authentication*”). Ex.1205, [0099]; *see also*, exemplary XML configuration schema at [0091]; *see also*, Ex.1205 [0013], [0032], [0072], [0078] (outlining additional security policies that may be implemented such as requiring a user to download provisioning files for gaining access to resources); Ex.1203, ¶136.

Krantz discloses:

When credentials are sent to server 215, authentication module 217 can receive the credentials (**e.g., user-identifier and password**) and compare the credentials [“*apply[ing] a security policy*”] to entries in **user database** 218. If credential information matches ... **the identity of a user is authenticated** (server 215 believes that the user represented by the user-identifier is the user who entered the credential information) [“*that includes at least one requirement pertaining to authentication*”]. If an

authenticated user of client 205 [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.1205, [0076]; *see also* Ex.1205, [0074] (using EAP to authenticate user, e.g., through exchange of “certificates, keys, and supported cipher suites.”). Krantz’s disclosure is consistent with the 444 Patent which describes requirements related to user identification and passwords/configuration requirements related to the access device (such as aspects of the operating system), (Ex.1201, 6:42-56), or to authenticate an access device, or user, of the access device. Ex.1201, 11:65-12:11; Ex.1203, ¶137.

Accordingly, Krantz and Herrmann render obvious this limitation. Ex.1203, ¶138.

2. Claim 2

Krantz discloses “access point 209 (i.e., “*access point*”) is a wireless access point enabling access to wired computer systems on VLAN B (e.g., server 215) and VLAN C (e.g., computer systems included in network 213).” Ex.1205, [0064]; Ex.1203, ¶140.

As Krantz explains, “if an authenticated user of client 205 is authorized to access resources located **on VLAN C** (e.g., the user is up to date on payments for their account), client 205 can then be authorized to access resources located on VLAN C.” Ex.1205, [0076]. Krantz discloses other “*security polic[ies]*” including user-identifiers and passwords. Ex.1205, [0076]; Ex.1203, ¶141.

Additionally, the “*security policy*” is applied in response to the client requesting access to resources on VLAN C. Ex.1205, [0016-0018], [0071]-[0072], [0076], [0104]-[0109]. After the “requirements of the security policy are satisfied,” the access point facilitates transfer of data between client 205 (the access “*device*”) and, ultimately VLAN C. Ex.1205, at [0063]-[0064]. As shown below, “*applying the security policy includes configuring the access point*” to allow access to VLAN C.

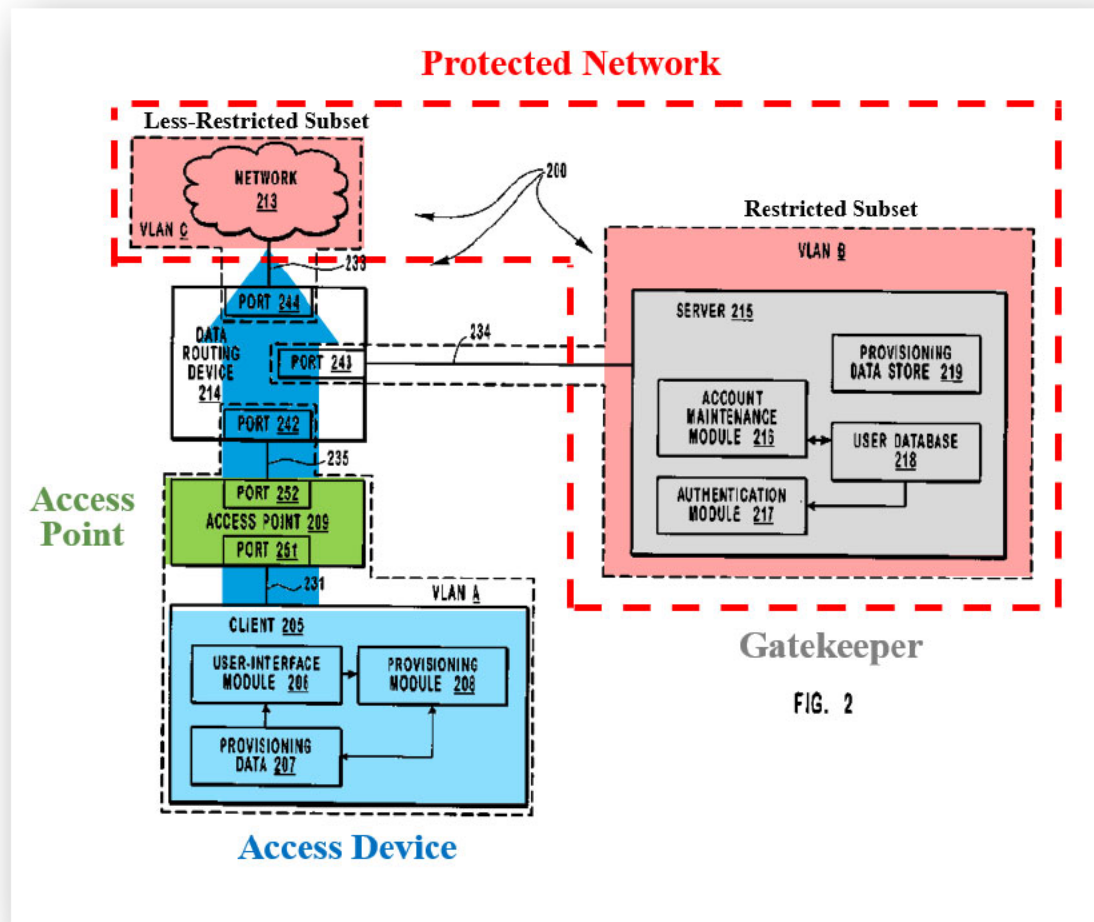


FIG. 2

Ex.1205, Figure 2 (annotated); Ex.1203, ¶142.

Krantz explains that “[a]ccess point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 that are to be transferred to VLAN B and/or VLAN C.” Ex.1205, [0064]; *see also* Ex.1205, [0061], [0023]. Ex.1203, ¶143.

Krantz explains 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.1205, [0107]. Access Point 209/Port 251 is “*configur[ed]*” because it previously tagged incoming data from client 205 with headers that enabled access to VLAN B. Ex.1203, ¶144.

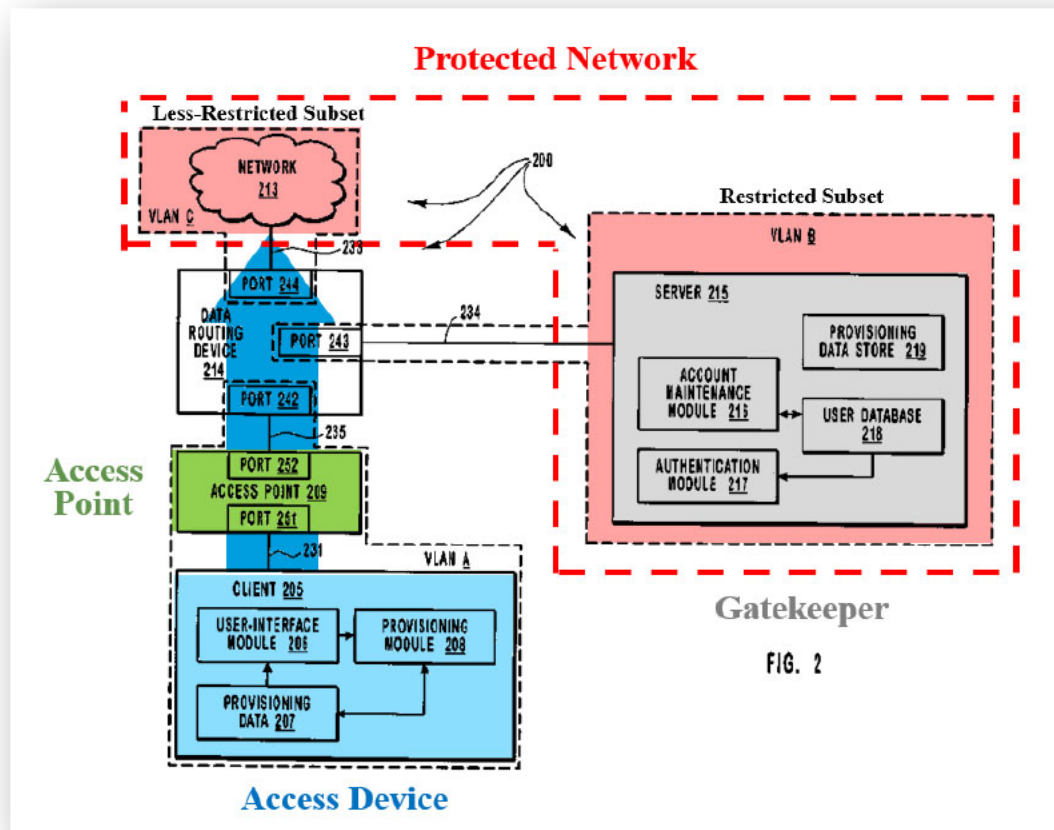
Krantz discloses that “[w]hen client 205 is authorized to access resources located on VLAN C, access point 209 may enable any protocols that are currently blocked for port 251 and may insert Tag Headers indicating that data from client 205 is to be transferred to VLAN C. Server 215 can send commands to access point 209 to cause access point 209 to enable protocols and cause access point 209 to insert appropriate Tag Headers.” Ex.1205, [0107]. Configuring input ports in VLAN aware devices to tag incoming data was a well-known technique to POSITAs by 2003. Ex.1207 (IEEE 802.1Q), 11 (Table 5-1) (explaining, when “Reception Port receives as (and does not discard)” untagged data, it “shall support the insertion of tag headers of a format appropriate to the destination MAC, carrying a non-null VID.”); Ex.1208 (U.S. Patent No. 6,430,621), 4:42-47 (“[S]ource node A transmits the packet. No VLAN tag information is present in a packet transmitted from a source node. At 415, the packet is received at switch 305, port 2. Port 2 is configured

as a member of LAN 1. Thus, a VLAN tag header is inserted in the packet with a VID=1.”); Ex.1209 (U.S. Patent No. 6,032,194), 16:4-13 (“[E]very time a message is received by the switch on a local port the VLAN designation of that port is associated with the message. Association is accomplished by a flow processing element which looks up the VLAN designation in a memory based on the local port where the message originated. ...”); Ex.1210 (Cisco IOS 12.0 Switching Services), p.210 (“The switch that receives the frame from the source station inserts the VLAN ID and the packet is switched onto the shared backbone network. When the frame exits the switched LAN, a switch strips the header and forwards the frame to interfaces that match the VLAN color.”); Ex.1203, ¶145.

Krantz discloses: “data routing device 214 can be configured to separate computer systems into different VLANs. As depicted in FIG. 2, **data routing device 214 has been configured to separate network architecture 200 into VLANs A, B, and C.** Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.” Ex.1205, [0060]; [0064] (“Access point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) [] to be transferred to VLAN B and/or VLAN C.”). Thus, by configuring the flow of data this way, the “*gatekeeper*” (server 215) may

apply security policies to authorize the access device access to data—such as the resources on VLAN C. Ex.1205, [0062] (“Any of the ports included in data routing device 214 (e.g., ports 242, 243, and 244) can be configured to transfer tagged data frames but drop untagged data frames.”); Ex.1203, ¶146.

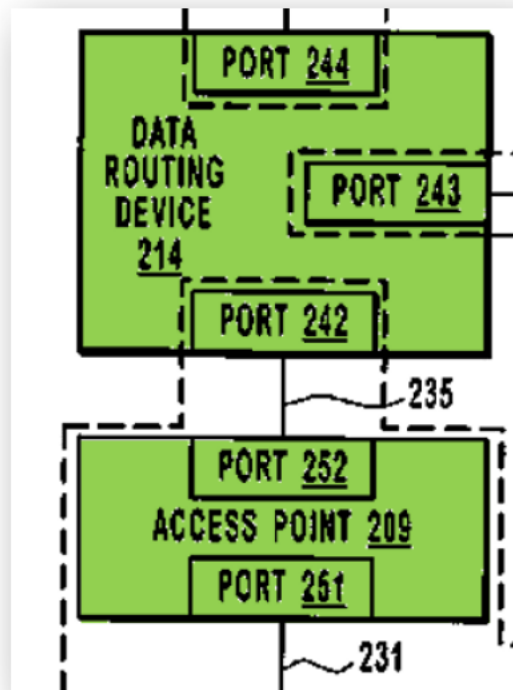
“*[S]ecurity polic[ies]*” can be applied, e.g., exchanging user-identifier/password, EAP-messages to pass certificate keys, cipher suites. Ex.1205, [0074]. “When credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) and compare the credentials to entries in user database 218.” *Id.*, [0076]. Once applied, “[i]f credential information matches an entry in user database 218, the identity of a user is authenticated (i.e., server 215 believes that the user represented by the user-identifier is the user who entered the credential information). **If an authenticated user of client 205 is authorized to access resources located on VLAN C (e.g., the user is up to date on payments for their account), client 205 can then be authorized to access resources located on VLAN C.**” *Id.*, [0076]. Thus, a POSITA would understand “*access point*” is “*configured*” (*id.*, [0053]) when audit data demonstrates that the access “*device*” is appropriately audited. Based on Krantz’s disclosure, the communication path for an authorized access “*device*” flows through “communication port” 244, as depicted in the annotated figure below in blue.



Ex.1205, Figure 2 (annotated); Ex.1203, ¶147.

To the extent one asserts Krantz does not expressly disclose “*wherein applying the security policy includes configuring the access point,*” it would have been obvious to implement the Data Routing Device disclosure of Krantz within the Access Point 209 itself. Ex.1203, ¶148.

Access Point 209 is connected to Data Routing Device 214, both containing several communication ports (shown below) and 235 is a logical communication link connecting the two. Ex.1205, [0060].



Ex.1205, Figure 2 (annotated and focused); Ex.1203, ¶149.

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.1205, [0061]; Ex.1203, ¶150.

Krantz states:

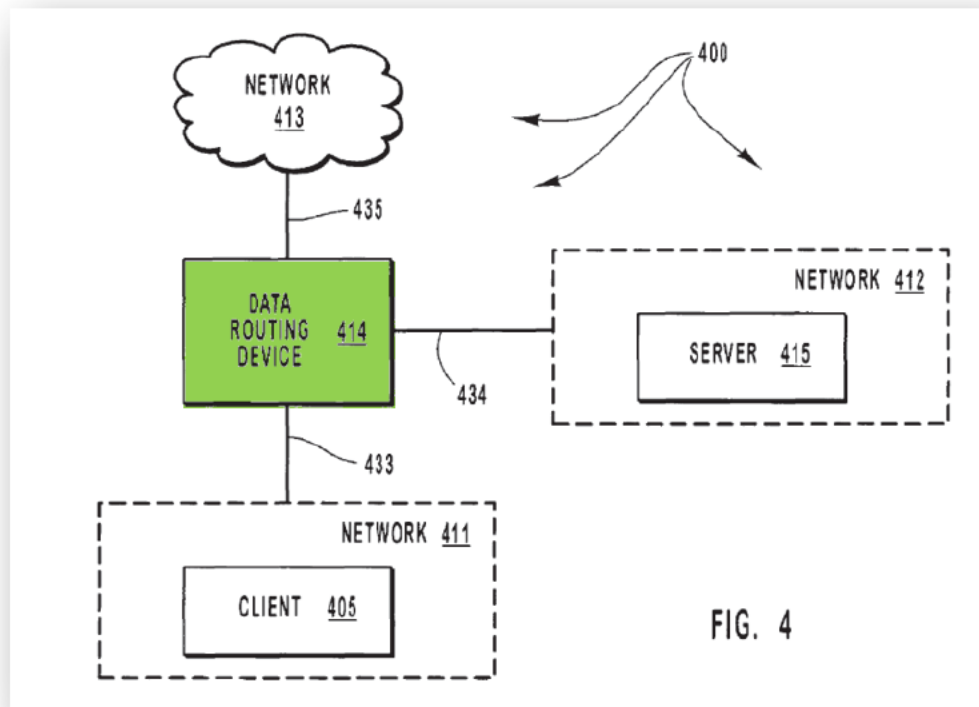
Data routing device 214 logically represents a special-purpose computer system, such as, for example, **a router and/or a switch, that can determine how to transfer data between the ports included in data routing device 214.** That is, when a portion of data [] is transferred in at a first port (e.g., port 242) **data routing device 214**

can determine, based on configuration rules, that the frame is to be transferred out at a second port (e.g., port 243)...

Ex.1205, [0059]; [0060] (“[D]ata routing device 214 can be configured to separate computer systems into different VLANs.”); *see generally, id.* [0064]. This configuration sending data to VLAN C (the “*network*” that has controlled access) is pursuant to a security policy requiring authorization and authentication as described in Krantz. Ex.1203, ¶151.

A POSITA would have found it obvious that “data routing device 214” functionality 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.1205, [0059]; Ex.1203, ¶152.

Indeed, Krantz contemplates combining the functionality of “access point” and “data routing device” in a single physical/logical representation. Figure 4 demonstrates this:



Ex.1205, Figure 4 (annotated); Ex.1203, ¶153; *see also* Ex.1205, [0051] (describing logical aspects of data routing device 414); Ex.1203, ¶154.

Krantz expressly discloses: “Data routing device 214 **logically represents** a special-purpose computer system ... that can determine how to transfer data between the ports included in data routing device 214.” Ex.1205, [0059]. A POSITA would understand this “logical” architecture could be implemented in a single device (an access point). Krantz repeatedly describes “data routing device” and “access point” as having **the same functionality**. *Compare, e.g.,* Ex.1205, [0060] (Data routing device 214); [0064] (Access point 209); *see also* [0069], [0073] (describing same

functionality for both). Thus, the functionality can occur at access point and data routing device combined **or** access point alone, without impacting functionality of the Krantz system. Using one technique or the other would have been a 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.1203, ¶155.

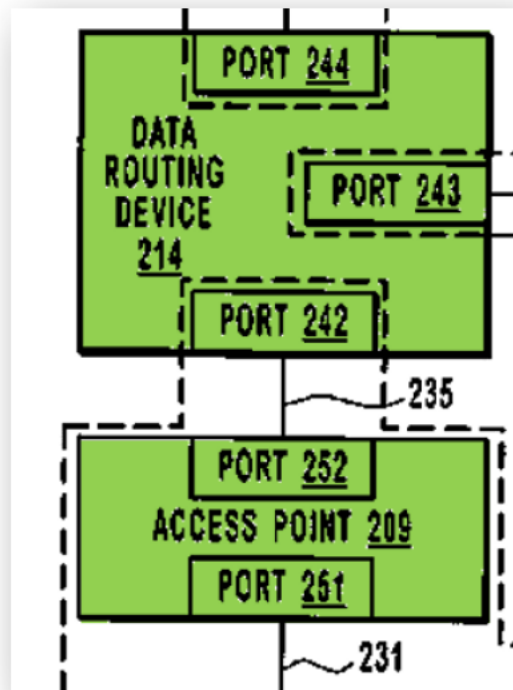
Accordingly, Krantz and Herrmann renders obvious this claim. Ex.1203, ¶156.

3. Claim 3

Krantz and Herrmann render obvious this claim for the same reasons as claim 2.

The 444 Patent explains that “access control lists within Router 220 are optionally used to independently **control access to specific devices** within Less-Restricted Subset 210.” Ex. 1201, 6:33-35; Ex.1203, ¶158.

Krantz discloses how “*configuring the access point*” is involved in, and “*includes assigning an access control list.*” For reference, data routing device 414 can be considered part of the access point in Krantz.



Ex.1205, Figure 2 (annotated); Ex.1203, ¶159.

Krantz explains: “access to resources located on network 413 can be restricted by the use of Internet Protocol (‘IP’) filtering. **Data routing device 414** [‘*access point*’], components in network 411, or components in logical communication link 433 can filter Internet Protocol (‘IP’) address to **limit client 405’s access to resources with particular IP addresses.**” Ex.1205, [0053]. In other words, the access point in conjunction with the data routing device can be “*configure[ed]*” based on what the client is authorized to access. Ex.1205, [0064] (“**[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.”); *see also*, Ex.1205, [0023] (“In VLAN embodiments, when a client is authorized to access resources located on the second network, the access point may insert Tag Headers into client data to indicate to the **data routing device** [*‘configur[ed] access point’*] that client data is to be transferred to the second network.”). As discussed, Krantz is 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.1205, [0107]. Access Point 209/Port 251 is “*configur[ed]*” because it was previously tagging incoming data from client 205, as described above, with headers that enabled access to VLAN B. Ex.1203, ¶160.

A POSITA would understand that the configuring step could utilize the database or list of clients to filter as disclosed in Krantz (i.e., *configuring the access point* also includes “*assigning*” an *access control list*). Krantz explains that “[w]hen **client 405 is not authorized** to access resources located on network 413, **IP addresses can be filtered** such that client 405 is exposed to IP addresses of resources located on network 412 but is not exposed to IP addresses of resources located on network 413. **When client 405 is authorized** to access network 413, IP addresses

can be filtered such that client 405 is exposed to IP addresses of resources located on both networks 412 and 413. Alternately, **when client 405 is authorized to access network 413 IP filtering may cease altogether.**” Ex.1205, [0053]. In effect, if the client (“*access device*”) is on an authorized list (“*access control list*”) it is permitted access and no filtering takes place (i.e., it is part of the “*assign[ed] access control list*” of devices permitted to access resources). Even without the specific disclosure of a database, a POSITA would have understood that limiting access to server resources for specific clients through IP filtering is a form of an “*access control list*” because that in essence “controls access to specific devices.” *E.g.*, Ex. 1201, 6:33-35; Ex.1203, ¶161.

A POSITA would have similarly found it obvious to use an “*access control list*” in a VLAN embodiment because such an embodiment has client access control considerations. Ex.1205, [0052] (“For example, **when client 405 is not authorized to access resources** located network 413, components in network 411 or logical communication link 433 can Tag data frames from client 405 indicating that the data frames are to be routed to server 415 (or other resources located on network 412). **When client 405 is authorized to access network 413**, components in network 411 or logical communication link 433 can Tag data frames from client 405 indicating

that the data frames are to be routed to resources on network 413 (e.g., to the Internet) or to resources on network 412 (e.g., server 412) as appropriate.”); Ex.1203, ¶162.

Krantz describes additional techniques where an “*access control list*” is utilized, which Dr. Houh explains would be understood to be stored in a database. In Krantz, a database is described as follows: “[w]hen credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) and compare the credentials to entries in **user database** 218. If credential information matches an entry in user database 218, **the identity of a user is authenticated** (i.e., server 215 believes that the user represented by the user-identifier is the user who entered the credential information).” Ex.1205, [0076]. A POSITA would understand this to be an “*access control list*,” i.e., list of users and/or devices that can access the network resources described with respect to claim [1]; Ex.1203, ¶163.

To the extent one asserts a user database is not a list of devices, that distinction is not persuasive. The 444 Patent discusses controlling specific devices (Ex. 1201, 6:33-35) but **does not limit** the access control list to a list of devices. Additionally, Dr. Houh explains that device information (e.g., IP addresses) could just as easily be stored in a database as users/usernames as Krantz specifically discusses filtering IP addresses. Ex.1205, [0053]; Ex.1203, ¶164.

Accordingly, Krantz and Herrmann renders obvious this claim. Ex.1203, ¶165.

4. Claim 4

Krantz and Herrmann discloses this limitation for the same reasons demonstrated for claim 2. Ex.1203, ¶166.

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.1205, at [0063]-[0064]. As shown below, Krantz discloses “*configuring access point and assigning access to a VLAN*,” i.e., **VLAN C**. Ex.1203, ¶167.

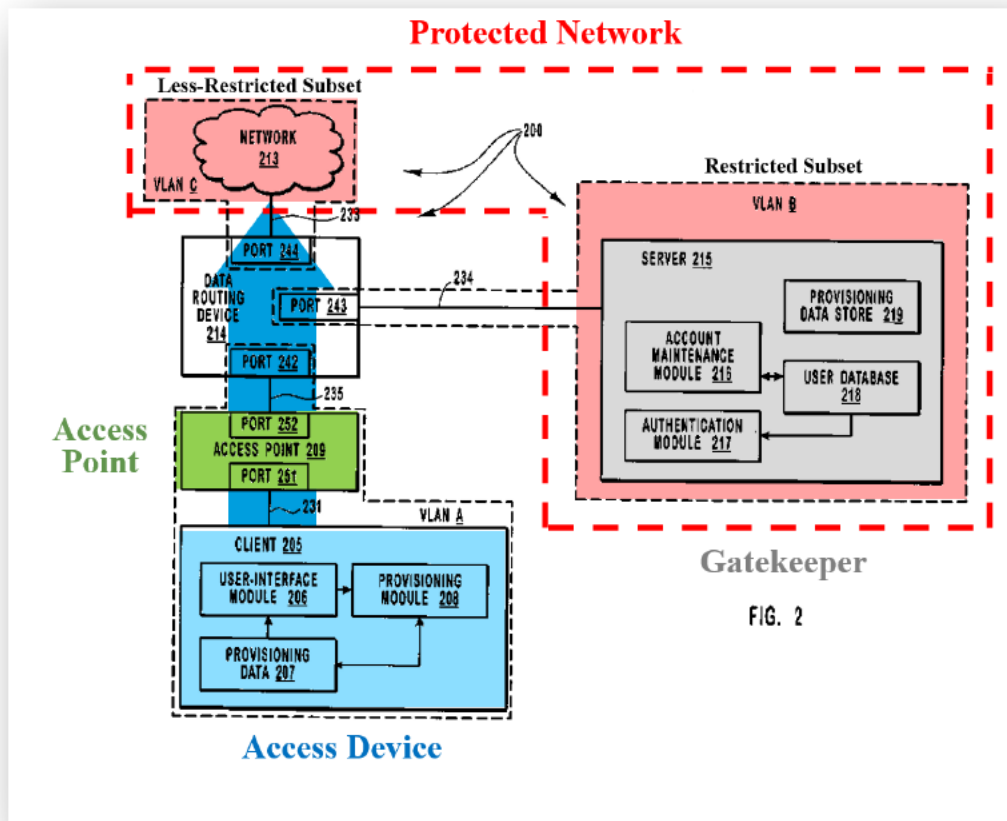


FIG. 2

Ex.1205, Figure 2 (annotated).

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.1205, [0064]; *see also* Ex.1205, [0061], [0064] (“In some embodiments, **access point 209** is a wireless access point **that enables access to wired computer systems on VLAN B (e.g., server 215) and VLAN C (e.g., computer systems included in network 213)**); Ex.1203, ¶168.

Accordingly, Krantz and Herrmann renders obvious this claim. Ex.1203, ¶169.

5. Claim 5

Krantz and Herrmann disclose “*receiving the audit data (at a gatekeeper configured to control access to a network), from the agent*” and how “*the audit data pertains to the device*” with respect to claims 1 and 2. Ex.1203, ¶170.

Krantz and Herrmann additionally disclose that “*updated audit data pertaining to the device*” continues to be received from the agent after configuring the access point. Krantz explains: “[i]t may be that server 215 sets a **session timeout**, such as, for example, one hour, after which access point 209 **will request client 205 to re-authenticate** [request the device provide “*updated audit data pertaining to the device*”]. If a subscription is still valid at the time of re-authentication [i.e., at the time it “*receiv[es]*” updated audit data], client 205 can re-authenticate **in the background** by submitting appropriate credentials to server 215. . . . **A subscription period can expire after a specified period of time (e.g., one month, 24 hours, etc.) or after a specified number of connections (e.g., one connection, ten connections, etc) through a particular service provider. After appropriate completion of the renewal user-interface client 205 can be re-authenticated**”

[“*updated audit data*” continues to be received from the agent “*pertaining to the device after configuring the access point*”]. Ex.1205, [0108]; Ex.1203, ¶171.

Similarly, Herrmann discloses continuous monitoring, including after reconfiguration. Herrmann explains: “the IGW server can direct the NAS to remove the restrictive filter **once the client has established compliance** with the required policy. When the client has taken the necessary steps to comply with the policy, **the policy server is notified by the client** [*‘receiving from the agent’*] (e.g., through an ‘IA_HEARTBEAT’ message, which is a periodic status message sent from the client directly to the policy server) [*‘updated audit data pertaining to the device after configuring the access point’*]. If the policy server verifies that the client is indeed in compliance with the assigned policy, it sends an ‘ISS_AUTH_OK’ message to the IGW server to indicate that the session should be unrestricted. In response ... the IGW server directs the NAS to remove the restrictive filter.” Ex.1206, [0080]. Nothing in Krantz or Herrmann suggests that continuing to collect audit data would cease once a reconfiguration occurs; instead using a session timeout and/or a periodic “IA_HEARTBEAT” protocol suggests it would continue even after reconfiguring the access point. Ex.1203, ¶172.

Accordingly, Krantz and Herrmann renders obvious this claim. Ex.1203, ¶173.

6. Claim 6

Krantz and Herrmann disclose “*receiving the audit data ... from the agent*” and how “*the audit data pertain[s] to the device*” as explained for claims 1 and 2. Ex.1203, ¶174.

Krantz discloses that 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.1205, [0070]. Krantz discloses that “the method 300 includes a functional, result-oriented step for **requesting authorization to access resources located on a second network (step 307)**” (“*to the less-restricted subset of a network*”). Krantz explains that if a device’s authorization expires and is not renewed, “**access point 209 may cease inserting Tag Headers for VLAN C** [*‘to the less restricted subset of a network’*] in data from client 205 and may instead begin inserting Tag Headers for VLAN B into data from client 205.” Ex.1205, [0109]; Ex.1203, ¶176.

As discussed for claim 5, Krantz explains: “[i]t may be that server 215 sets a **session timeout**, such as, for example, one hour, after which access point 209 **will request client 205 to re-authenticate** ... A subscription period can expire after a specified period of time (e.g., one month, 24 hours, etc.) or after a specified number of connections (e.g., one connection, ten connections, etc) through a particular

service provider. **After appropriate completion of the renewal user-interface** [“receiving ... updated audit data”] client 205 can be re-authenticated.” Ex.1205, [0108]; Ex.1203, ¶177.

Similarly, Herrmann discloses continuously monitoring the device even while it has access to the less-restricted subset of the network. Ex.1206, [0080] (describing use of a use of a session timeout and/or periodic “IA_HEARTBEAT” protocol); Ex.1203, ¶178.

As with claim 5, nothing in Krantz or Herrmann suggests the continued collection of audit data would cease while the device has access to the less-restricted subset of the network; instead, use of a session timeout and/or periodic “IA_HEARTBEAT” protocol suggests it would continue even while the device has access to the less-restricted subset of the network (“*while the device has access to a less-restricted subset of the network*”). Ex.1203, ¶179.

Accordingly, Krantz and Herrmann renders obvious this claim. Ex.1203, ¶180.

7. Claim 7

Krantz and Herrmann disclose “receiving at the gatekeeper, from the agent, audit data pertaining to the device” as discussed with respect to claim [1.4]. The gatekeeper also continues “receiving, from the agent, updated audit data pertaining

to the device after configuring the access point” as discussed with respect to claim 5 . Ex.1203, ¶181.

Accordingly, Krantz and Herrmann render obvious this claim. Ex.1203, ¶182.

8. Claim 10

Krantz and Herrmann disclose “[t]he method of claim 1, wherein the request includes a request for audit data pertaining to an application.” Ex.1203, ¶183.

One “request” which “includes a request for audit data pertaining to an application” regards antivirus software described in Herrmann. Herrmann discloses the criticality “to promptly **update anti-virus applications on all machines** in a network ... before the network is infiltrated by a newly released virus.” Ex.1206, [0012]; Ex.1203, ¶184.

Herrmann discloses that “a network administrator **may require** [“request”] **all users accessing the network to implement a virus definition update (e.g., DAT file)** that is targeted at a particular virus.” Ex.1206, [0071]. This may be implemented using security rules/checking system data for connecting devices to assure compliance. Ex.1206 [0068]; Ex.1203, ¶185.

Herrmann further 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.1206, [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.1206, [0067]; Ex.1206, [0068] (“[P]olicy server 460 may enforce a variety of different types of security policies or rules ... for instance, rules which require client devices connecting to a given network **to be using particular security or anti-virus programs.**”) (*“the request includes a request for audit data pertaining to an application”*). The **policy server is notified by the client** containing policy agent 413, through periodic status messages called “IA_HEARTBEAT(s)” to authenticate the access device. Ex.1206, [0080], [0098]; Ex.1203, ¶186.

A POSITA would be motivated to modify the system of Krantz in view of Herrmann to include audit data requiring a specific “*application*” (for the reasons discussed above and in § VII.C) including requiring a specific virus-protection program, because Krantz is focused on network authentication and security. Ex.1205, [Abstract]. A POSITA would have had a reasonable expectation that this additional provision would be successful because Krantz already discloses conditions for client access, e.g., “signup” or “renewal” conditions to authorize access to network resources. Ex.1205, [0019]. Requiring the client device be

audited for data indicating it uses a specific “*application*” such as antivirus software described in Herrmann would merely be an additional condition for a client to maintain access. Ex.1203, ¶187.

Accordingly, Krantz and Herrmann renders obvious this claim. Ex.1203, ¶188.

9. Claim 12

As discussed for claim [10], Krantz in view of Herrmann discloses a request for “*audit data*.” As also discussed with respect to claim [1.4], such “*audit data*” is received (at a gatekeeper). Ex.1203, ¶189.

Krantz further discloses that the *audit data includes information that concerns [the] operating system of the device*. As discussed *supra*, the “*audit data*” may include configuration requirements relating to the access device. Ex.1201, 6:38-48. As I discuss with respect to claim [1.3], Krantz discloses that “client 205 and server 215 **exchange EAP-messages** to pass certificates, keys, and supported cipher suites. Depending on the EAP type, other credential information may also be exchanged between client 205 and server 215.” Ex.1205, [0074]. With respect to the XML configuration schema disclosed in [0091] of Krantz, a handshake protocol may be used between the device and gatekeeper and the data may include “*information that concerns operating system of the device*.” Ex.1205 [0099]:

a **configuration sub-file** to indicate a type of EAP [is] used to authenticate a server with a client and/or to authenticate a client with a server. ... [an] element can be included in a configuration sub-file **to indicate whether or not operating system credentials** should be used for authentication.

Ex.1203, ¶190.

Accordingly, Krantz and Herrmann renders obvious this claim. Ex.1203, ¶191.

10. Claim 17

As discussed in claims [1.4] and [13], respectively, Krantz and Herrmann disclose both how a “*gatekeeper [is] configured*” to control access to a network and that “*audit data includes information that concerns antivirus software on the device.*” Ex.1203, ¶192.

Krantz and Herrmann further disclose a “*gatekeeper is configured to take part in bringing a software on the device up to date in response to applying the security policy.*” Krantz states that “**software incompatibilities must be worked out** by a user that may lack the technical expertise or desire to **re-configure software** for compatibility with the service” (“*must be configured to take part in bringing a software on the device up to date*”). Ex.1205, [0013]; Ex.1203, ¶193.

Krantz discloses how a connecting device may be required to have “provisioning files [] for gaining full access to network 413.” Ex.1205, [0056]; Ex.1205, [0032], [0078]-[0079] (discussing provisioning clients for gaining access to the network). Dr. Henry explains that provisioning files relate to network connectivity and security. Ex.1203, ¶194.

Herrmann discloses that “[i]t becomes critical... to promptly update anti-virus applications on all machines in a network [] before the network is infiltrated by a newly released virus.” Ex.1206, [0012]; Ex.1203, ¶195.

Herrmann discloses that “a network administrator **may require all users accessing the network to implement a virus definition update (e.g., DAT file)** that is targeted at a particular virus.” Ex.1206, [0071] (“*gatekeeper is configured to take part in bringing a software on the device up to date in response to applying the security policy*”). This may be implemented using security rules/checking system data for connecting devices to ascertain compliance. Ex.1206, [0068]; Ex.1203, ¶196.

A POSITA would be motivated to modify Krantz to include requiring a specific virus protection program be brought up to date as in Herrmann for the reasons already discussed. *See* §VII.C. A POSITA would have had a reasonable expectation this additional provision would be successful because Krantz already

discloses conditions for client access, such as “signup” or “renewal” conditions to authorize access. Ex.1205, [0019]. Requiring clients update antivirus software would merely be an additional condition, which a POSITA would understand the importance of as confirmed by the 444 Patent, which discusses a **prior art GateKeeper 110** (Ex.1201, 2:34-35) and explains that “**GateKeeper 110** may make certain that Access Device 160 has up-to-date virus software and encryption protocols as proscribed by [a] security policy.” Ex.1201, 2:25-30. Moreover, because prior art GateKeepers were known to control security policies (Ex.1201, 2:22-39), Dr. Houh explains that the disclosed gatekeeper of Krantz in combination with Herrmann renders obvious that the “*gatekeeper is configured to take part in bringing the device software up to date.*” Ex.1203, ¶197.

Accordingly, Krantz and Herrmann render obvious this claim. Ex.1203, ¶198.

11. Claim 22

i. [22.0]

See [1.0]. Ex.1203, ¶199.

ii. [22.1]

See [1.1]. Ex.1203, ¶200.

iii. [22.2]

See [1.2]. Ex.1203, ¶201.

iv. [22.3]

See [1.3]. Ex.1203, ¶202.

v. [22.4]

See [1.4]. Ex.1203, ¶203.

vi. [22.5]

See [1.5]. Ex.1203, ¶204.

vii. [22.6]

See [2.0]. Ex.1203, ¶205.

viii. [22.7]

See [6.0]. Ex.1203, ¶206.

ix. [22.8]

As discussed in claim [5], Krantz discloses “*receiving, from the agent, updated audit data pertaining to the device after configuring the access point.*” Krantz discloses that the device is monitored (“*re-audit[ed]*”) in the background, for continued compliance with the security policy, using the updated audit data. Krantz explains: “[i]t may be that **server 215 sets a session timeout, such as, for example, one hour, after which access point 209 will request client 205 to re-authenticate** [*re-auditing the device in accordance to ...*’]. If a subscription is still valid at the time of re-authentication, client 205 **can re-authenticate in the background by**

submitting appropriate credentials to server 215 [*‘the security policy using the received updated audit data’*] . . .” Ex.1205, [0108]. Thus, the device is continually monitored in the background for compliance with a security policy by requiring the device and/or user to reauthenticate credentials and provide updated audit data at certain time increments. Ex.1203, ¶208.

Accordingly, Krantz teaches or suggests this limitation. Ex.1203, ¶209.

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 444 Patent (or related patents), as neither Krantz nor Herrmann was cited or considered by the Examiner during prosecution of the 444 Patent. The references in this Petition were neither relied upon during prosecution nor are they cumulative of art relied upon during prosecution. Further, the 444 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)) (“As to factor 1, there is no evidence as to whether there will be a stay in the parallel case, so we regard this factor as neutral.”).

2. Parallel Proceeding Trial Date

Regarding factor 2, no trial date has been set. In addition, according to the most recent statistics⁷ on median time-to-trial for civil actions in the Northern District of California, the median time from filing to trial was 48.9 months. The related litigations were filed in May and August of 2023, so trial can be expected in approximately May 2027 and August of 2027. Any Final Written Decision can be

⁷ <https://www.uscourts.gov/statistics-reports/federal-court-management-statistics-december-2023>

expected in August of 2025, likely over a year before trial. Accordingly, this factor **weighs against** discretionary denial.

3. Parallel Proceeding Investment

Factor 3 **weighs against** discretionary denial. The related litigations are in the early stages of discovery, a motion to dismiss has been filed, and the investment by the parties has been relatively minimal. In addition, claim 7 is not at issue in the related litigations. *Samsung Bioepis Co. Ltd v. Regeneron Pharmaceuticals, Inc.*, IPR2023-00739, Paper 9 at 57 (Oct. 20, 2023) (“[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 strikingly similar disclosure to that of the 444 Patent, is directed at the same problem and proposes the same solutions as the 444 Patent and discloses nearly identical architecture. The evidence presented, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.

X. CONCLUSION

Claims 1-7, 10, 12, 17, and 22 of the 444 Patent are unpatentable for the reasons demonstrated above.

Dated: March 26, 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 13,997 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: March 26, 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 26th day of March, 2024, I caused to be served a true and correct copy of the foregoing and any accompanying exhibits by priority mail on the following:

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: March 26, 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