

Filed: March 8, 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.

IPR2024-00540
U.S. Patent No. 8,347,350

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 8,347,350**

TABLE OF CONTENTS

	Page
<u>TABLE OF AUTHORITIES</u>	V
<u>EXHIBIT LIST</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 350 PATENT	4
A. Effective Filing Date	4
B. Person of Ordinary Skill in the Art.....	4
C. Overview of the 350 Patent	4
VI. CLAIM CONSTRUCTION	7
VII. PRINCIPAL PRIOR ART	7
A. Summary of Krantz	7
B. Summary of Herrmann.....	9
C. The Combination of Krantz and Herrmann	13
VIII. CLAIMS 1, 2, 4-10, 13, 16, AND 18-19 ARE UNPATENTABLE	20
A. Ground 1: Claims 1, 2, 4, 5 and 16 are Obvious Based on Krantz	20
1. Claim 1	20
i. [1.0] A method for network access control, the method comprising:	20
ii. [1.1] receiving audit data pertaining to a device that does not have access to a less-restricted subset of a network;	26

iii.	[1.2] auditing the device in accordance with a security policy based at least in part on the audit data,.....	31
iv.	[1.3] reconfiguring an access point to allow access to the less restricted subset of the network in response to the security policy audit, ...	35
v.	[1.4] receiving updated audit data pertaining to the device subsequent to reconfiguring the access point; and	44
vi.	[1.5] monitoring continued compliance of the device with the security policy using the updated audit data.....	46
2.	Claim 2	48
i.	[2.0] The method of claim 1, wherein monitoring of the device for continued compliance with the security policy includes continued communications with the device.....	48
3.	Claim 4.....	49
i.	[4.0] The method of claim 1, wherein the access point is reconfigured to allow access to a different subset of the network in response to the device failing to comply with the security policy while being monitored.....	49
4.	Claim 5	53
i.	[5.0] The method of claim 1, wherein the security policy includes authentication of the user of the device.	53
5.	Claim 16.....	54
i.	[16.0] The method of claim 1, wherein the security policy audit is based at least in part on the information concerning an identity of a user of the device.	54
B.	Ground 2: Claims 6-10, 13, 18 and 19 are Obvious Based on Krantz and Herrmann	55
1.	Claim 6.....	55

i.	[6.0] The method of claim 4, wherein an agent running on the device collects the audit data.....	55
2.	Claim 7	59
i.	[7.0] The method of claim 6, further comprising updating the device to comply with the security policy when the device fails to comply with the security policy.	59
3.	Claim 8	61
i.	[8.0] The method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent concerning operating system of the device.....	61
4.	Claim 9	62
i.	[9.0] The method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent, and that concerns antivirus software on the device.	62
5.	Claim 10	65
i.	[10.0] The method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent, and that concerns other devices coupled to the device.	65
6.	Claim 13	68
i.	[13.0] The method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent, and that concerns applications executing on the device.....	68
7.	Claim 18	70
i.	[18.0] The method of claim 6, wherein updated audit data pertaining to the device continues to be received from the agent after reconfiguring the access point.....	70
8.	Claim 19	72
i.	[19.0] The method of claim 6, wherein updated audit data pertaining to the device continues to be	

	received from the agent while the device has access to the less-restricted subset of the network.	72
IX.	THE BOARD SHOULD NOT EXERCISE ITS DISCRETION AND DENY INSTITUTION	74
A.	The Board Should Not Deny Institution Under 35 U.S.C. § 325(d).....	74
B.	The Board Should Not Deny Institution Under 35 U.S.C. § 314(a).....	74
1.	No Evidence Regarding a Stay	74
2.	Parallel Proceeding Trial Date	75
3.	Parallel Proceeding Investment.....	75
4.	Overlapping Issues with the Parallel Proceeding.....	76
5.	Overlapping Parties.....	76
6.	Strength of Petition and Other Considerations	76
X.	CONCLUSION.....	77

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
1101	U.S. Patent No. 8,347,350
1102	U.S. Patent No. 8,347,350 File History
1103	Declaration of Henry Houh, Ph.D
1104	CV of Henry Houh, Ph.D
1105	U.S. Patent Pub. No. 2004/0111520 to Krantz et al
1106	U.S. Patent Pub. No. 2004/0107360 to Herrmann et al
1107	IEEE Std 802.1Q-1998 – IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
1108	U.S. Patent No. 6,430,621 to Srikanth et al.
1109	U.S. Patent No. 6,032,194 to Gai et al.
1110	Cisco IOS 12.0 Switching Services (1999)
1111	Microsoft Computer Dictionary 5 th Edition (2002)
1112	Webster’s New World Computer Dictionary (2001)
1113	[Reserved]
1114	U.S. Patent No. 5,987,611 to Freund
1115	[Reserved]
1116	RFC 2716 – PPP EAP TLS Authentication Protocol
1117	Wireless security with 802.1x and PEAP (2003)

I. INTRODUCTION

Petitioner Cisco Systems, Inc. and Fortinet, Inc. submits this Petition for *Inter Partes* Review of claims 1, 2, 4-10, 13, 16, and 18-19 (the “Challenged Claims”) of U.S. Patent No. 8,347,350 (the “350 Patent” (Ex.1101)), assigned to Patent Owner, InfoExpress Inc. Petitioner respectfully submits that the Challenged Claims of the 350 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 350 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 350 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 350 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 350 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 350 Patent.

B. Identification of Challenged Claims

Ground 1: Claims 1, 2, 4, 5 and 16 are unpatentable as obvious under 35 U.S.C. § 103 based on Krantz (Ex.1105).

Ground 2: Claims 6-10, 13, 18 and 19 are unpatentable as obvious under 35 U.S.C. § 103 based on Krantz in view of Herrmann (Ex.1106).

V. THE 350 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 350 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.1105, ¶21.

C. Overview of the 350 Patent

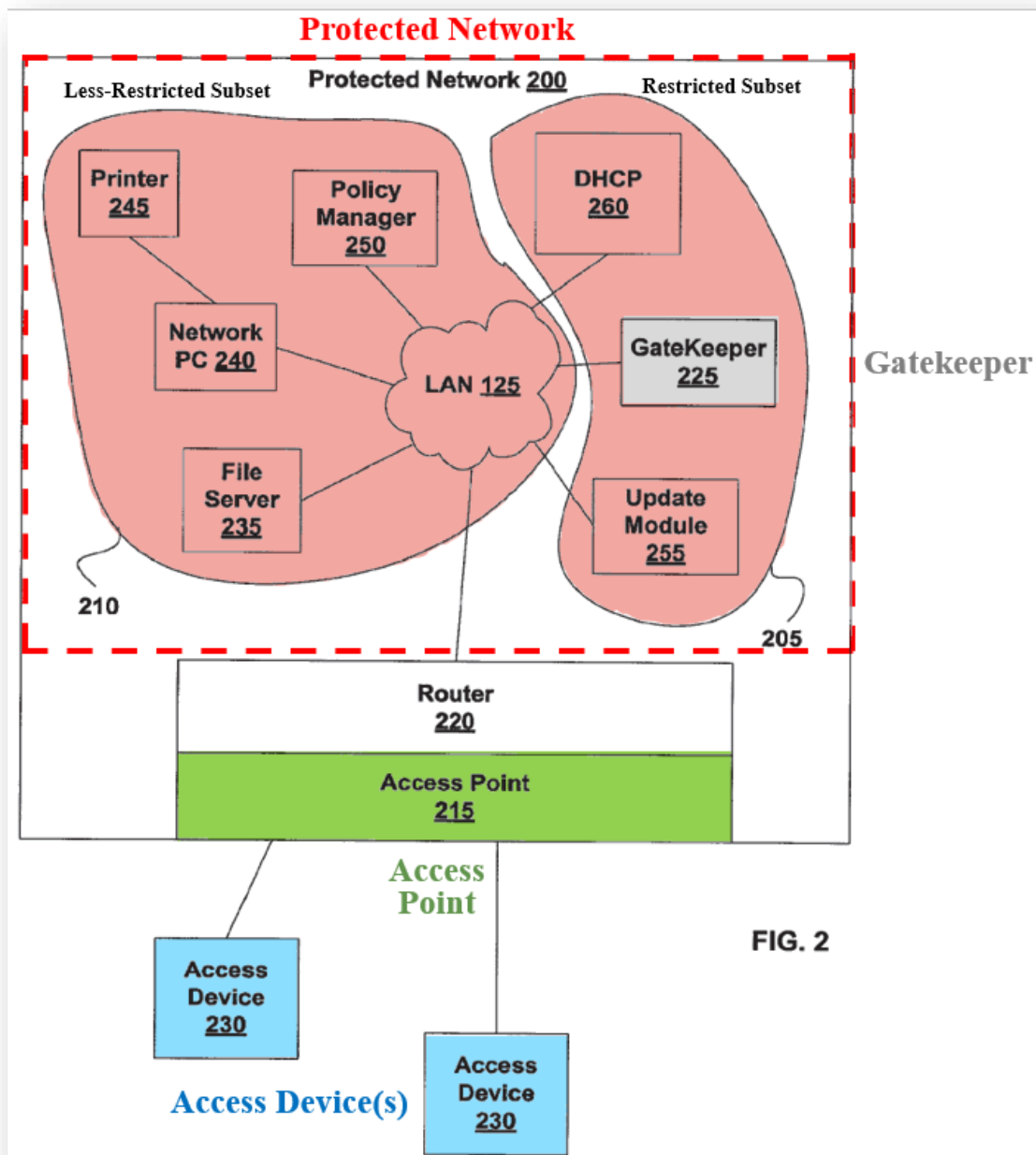
The 350 Patent describes “a protected network¹ physically or logically divided into a restricted subset and one or more less-restricted subsets.” Ex.1101, 2:53-54. Access to less-restricted networks from a device “are first passed to the restricted subset.” Ex.1101, 2:54-56. Elements of the “restricted subset”—such as a “gatekeeper”—“apply security policies” to the device requesting access.

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

Ex.1101, 2:56-58. If the requesting device satisfies the “security policies,” access is then granted “to a less-restricted subset of the protected network.” Ex.1101, 2:58-60. 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. 1101, 4:1-3. The 350 Patent articulates that “[i]n some embodiments, Authenticate User Step [] is considered part of the security policy audit.” Ex.1101, 12:2-4; *see also*, Ex.1101, 11:42-53 (giving examples of audit/system data including, operating system status, antivirus software status, information about devices connected to the Access Device, MAC address, IP address, etc.).

The 350 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.1101, 2:61-63.

Figure 2 depicts embodiments of the invention described in the 350 Patent:



Ex.1101, Fig. 2 (annotated); Ex.1103, ¶33

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

Ex.1101, 5:55-58. Access to Protected Network 200 is “under the control of a

GateKeeper 225,” which “enforce[s] a security policy against one or more Access Device 230 requesting access.” Ex.1101, 5:59-64.

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

VII. PRINCIPAL PRIOR ART

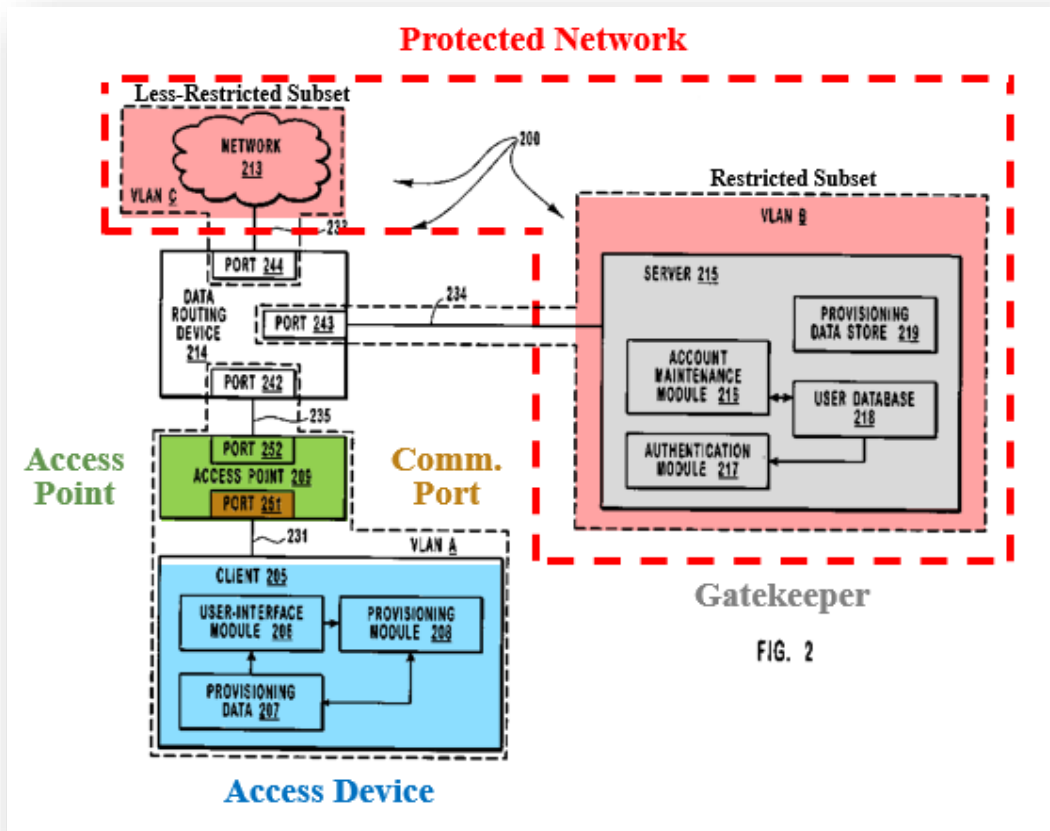
A. Summary of Krantz

U.S. Patent Pub. No. 2004/0111520 to Krantz et al. (Ex.1105) was filed on December 6, 2002, and published on June 10, 2004. Krantz is prior art to the 350 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.1105, [0015].

Krantz teaches a system in which a device attempts to access a protected network. Ex.1105, [Abstract]. To gain access to such a protected network, Krantz includes a server which can authorize access to the protected network resources

based on credentials supplied by the device or user. Ex.1105, [0016], [0068]-[0071], [0099], [0104], [0107]-[0109]. An embodiment of this network architecture is depicted below with respect to annotated Figure 2:



Ex.1105, Fig. 2 (annotated).

Krantz utilizes Virtual Local Area Network (“VLAN”) techniques. Ex.1105, [0057]. Krantz discloses that “network architecture 200 data routing device 214 is connected to network 213, server 215, and access point 209 by corresponding logical communication links 233, 234, and 235 respectively. Network 213 can be virtually any type of network, such as, for example, a corporate or enterprise-wide

network ... [and] data routing device 214 can be a device capable of grouping computer systems together in a single broadcast domain based on criteria other than physical location.” Ex.1105, [0060]. Access Point 209 utilizes ports which can be configured for data transfer. Ex.1105, [0062].

Krantz teaches a client requesting access to the network can send credentials to a server to authenticate itself. Ex.1105, [0016]. Based upon the credentials supplied, the server “may authorize the client for at least partial access” or access to the entire network. Ex.1105, [0016], [0104], [0107]-[0109] Authentication may be made by server 215. Ex.1105, [0068]-[0071], [0099]. The server is also responsible for ensuring that the client device adheres to certain configuration settings—including the established encryption protocol—for gaining access to the network authorized to be accessed. Ex.1105 [0110]-[0111].

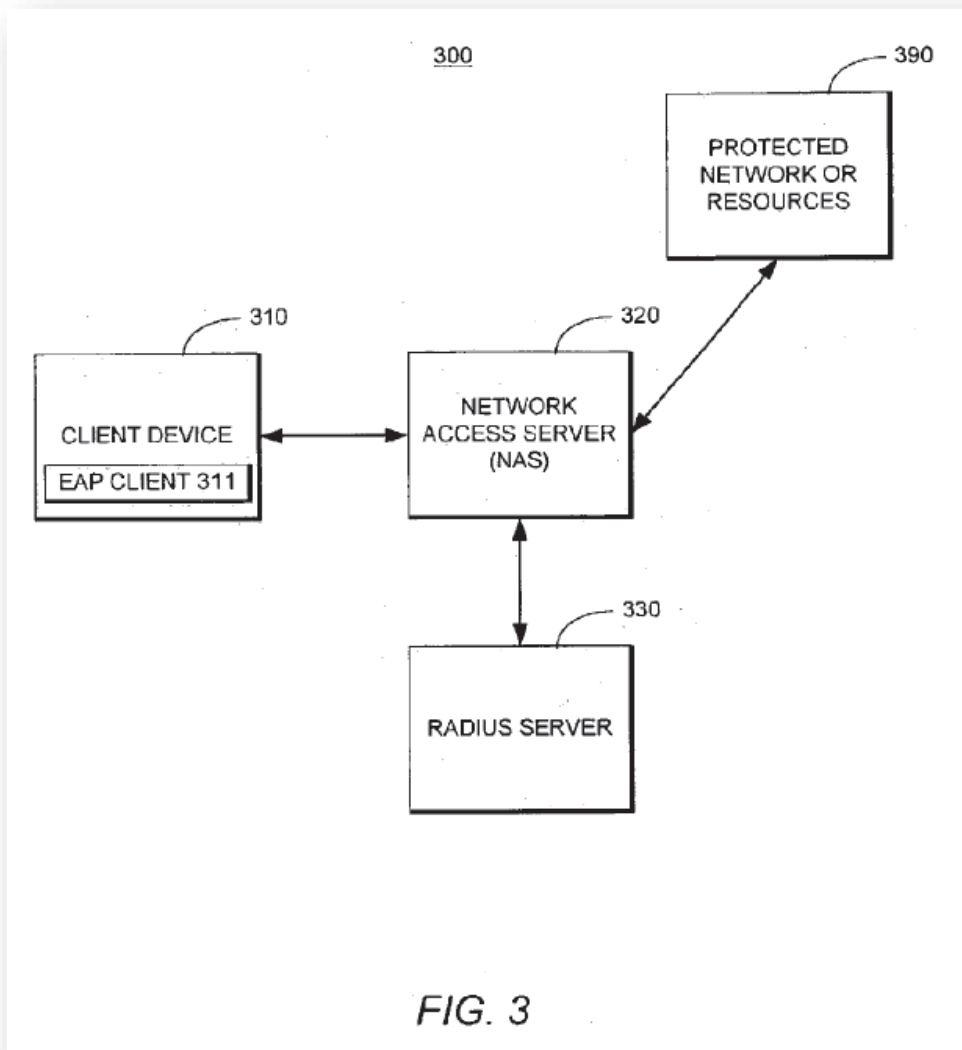
B. Summary of Herrmann

U.S. Patent Pub. No. 2004/0107360 to Herrmann et al. was filed on March 13, 2003, and published on June 3, 2004. Herrmann is prior to the 350 Patent at least under 35 U.S.C. § 102(e).

Herrmann describes enforcing security policies when providing access to a network. Herrmann explains that if a client device connected to a network . . . [and] is infected with a virus or worm, it may infect other machines on the same

network. Ensuring that devices connected to the network are running current anti-virus programs is particularly important. Ex.1106 [0012].

As a solution, Herrmann proposes the collection of information from a client device to be used during the authentication process to enforce network security policies. For example, Herrmann teaches a system in which a client device attempts to access a network and information is collected to determine whether the client can gain access to protected network resources. Ex.1106, [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.1105, [0018], [0053], [0063].

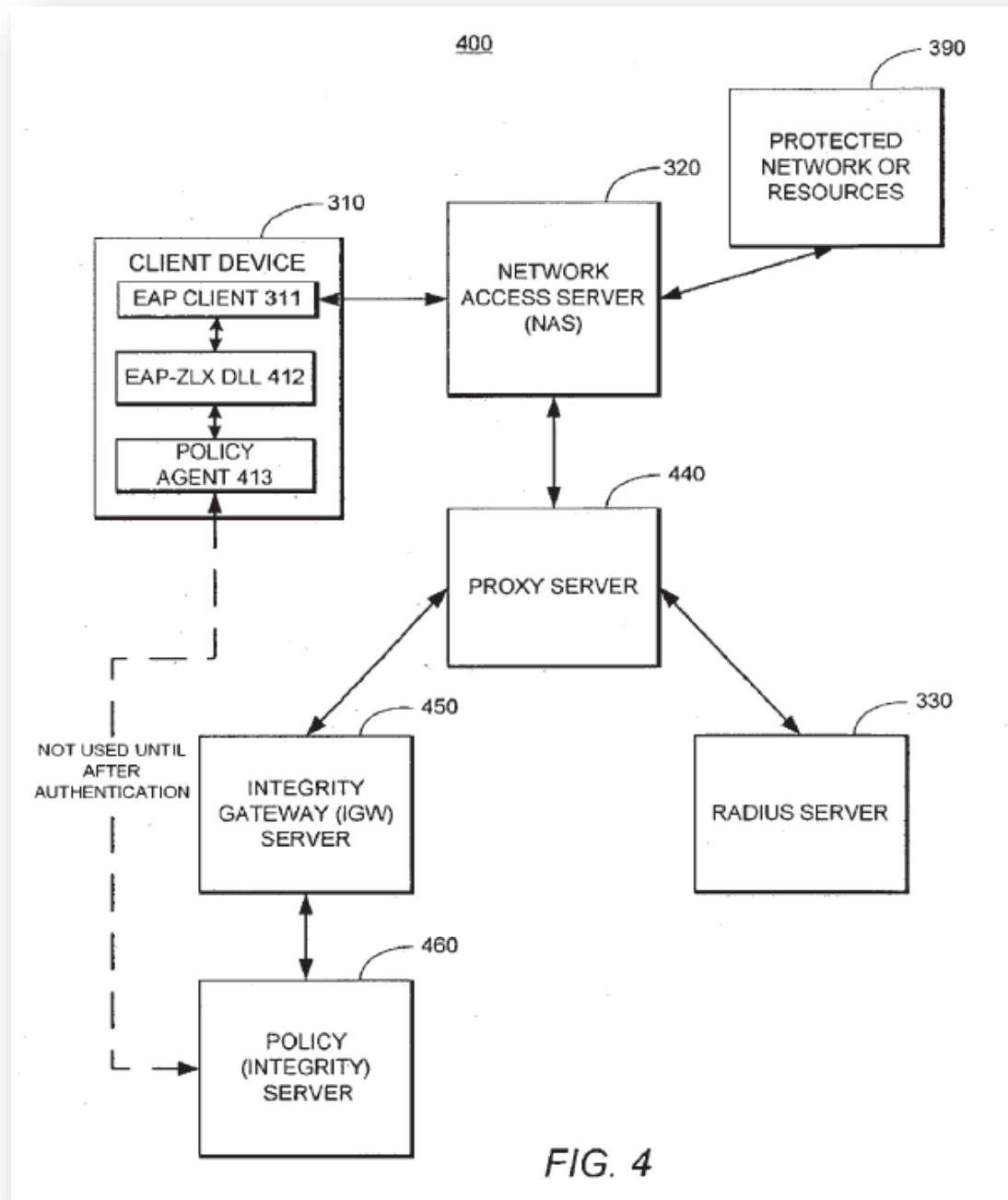


Ex.1106, Fig. 3.

In Figure 4, “a client device 310 connects to the NAS 320 to access the protected network or resources 390.” Ex.1105, [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.1105, [0062], [0067].



Ex.1106, 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.1106, [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.1106, [0067].

C. The Combination of Krantz and Herrmann

It would have been obvious to include Herrmann’s techniques related to enforcing security policies (including checking for anti-virus protection at the client) and obtaining system data from an access device in the system of Krantz for the reasons explained below. In particular, the Krantz system already discloses that “access point 209 may block [] protocols ... from being transferred **until client 205 is authenticated (and authorized)**². Ex.1105, [0072]. Specifically, Krantz explains that as part of its security policies, client devices are authenticated, (Ex.1105, [0067]-[0074], [099]) and users of client devices are authenticated, Ex.1105, [0074], [0076]. Ex.1105, [0076].

A POSITA would recognize that checking for anti-virus software as part of a security policy would merely be an additional item for server 215 to check in the process already disclosed by Krantz. Ex.1105, [Fig. 3], [0068]-[0076] (describing

² Emphasis added throughout unless otherwise indicated.

the steps of authenticating client devices and users). Like Krantz, Herrmann discloses a “policy server 460 [which] may enforce a variety of different types of security policies or rules.” Ex.1106, [0068]. One such rule, to be authorized for network access, would be “a policy requiring that a **specific virus protection program** is operational on each client device that is connected to a network.” Ex.1106, [0012]. Herrmann expressly recites that the policy server determines whether the client device 310 complies with applicable security policies. Ex.1106 [0066].

A POSITA would also be motivated to modify the teachings of Krantz to include determining whether the requirements of a security policy that include checking for virus protection are satisfied as taught by Herrmann for several reasons. As explained in detail below, Krantz already describes a security policy that includes requiring authentication of a client device and users. Krantz also teaches providing a configuration file with the proper encryption protocol (and other necessary configuration information), the client device is configured for compatible operation with the network. Herrmann discloses that it is “particularly important” that devices connected to the network are running current anti-virus programs, and that one way of ensuring this is implementing a “policy requiring that a **specific virus protection program**.” Ex.1106, [0068]; *see also*, Ex.1106, [0012] (noting it is critical that all machines in a network maintain updated

antivirus software so the network is not infiltrated by newly released viruses).

Herrmann expressly recites that the policy server determines whether the client device 310 complies with applicable security policies, which would include specific virus detection. Ex.1106, [0066]. Thus, a POSITA would be motivated to modify the teachings of Krantz to include in a security policy's requirements that a specific virus protection program be utilized, and to determine if the client device satisfies the applicable security policies before allowing the client device to access protected networks to prevent viruses from infecting the protected network and to ensure network compatibility.

Krantz's server 215, which compares the credentials of a user against a database (e.g., user-identifier and password), as modified by Herrmann, would additionally compare a virus protection program on an access device against approved antivirus programs. Information regarding approved antivirus software and approved connected devices could be stored in the User Database or an additional Database could be added.

The 350 Patent itself confirms that a POSITA would recognize the need for the authentication module of Krantz to check for up-to-date and approved antivirus programs. In the background section of the 350 Patent, it discusses GateKeeper 110 (Ex.1101, 2:18-19) 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.1101, 2:23-26.

Both Krantz and Herrmann are analogous art to the 350 Patent for at least two reasons. *First*, Krantz and Herrmann are both directed toward the same field of endeavor of the 350 Patent—network security. Ex.1101, 1:23-24 (“The invention is in the field of computing systems and more specifically in the field of network security.”); Ex.1105, Abstract (“A computer system attempts to authenticate with a server to gain authorization to access a first network.”); Ex.1106, Abstract (“A system and methodology for policy enforcement during authentication of a client device for access to a network is described.”).

Second, both Krantz and Herrmann are reasonably pertinent to a problem described by the 350 Patent: the reliance “on mere user authentication” and the need to “assure that **an access device** used by the authenticated user meets network security policies” such as current anti-virus software. *E.g.*, Ex.1101, 1:46-48; *see also, id.*, 1:57-60 (“A greater level of access control may be achieved by including a gatekeeper between the secure network and the access device. The gatekeeper is configured to ensure that the access device conforms to a predetermined security policy.”).

Krantz discloses a security policy beyond user authentication and encryption protocols. For instance, “[a]fter an EAP type is selected . . . **computer systems**

can attempt to authenticate with one another through the transfer of EAP messages . . . in accordance with the selected EAP type. For example, when EAP-TLS is selected, **client 205 may communicate with server 215** through a series of EAP messages in accordance with EAP-TLS **so as to be authenticated and possibly authorized to access resources located on VLAN C.**” Ex.1105, [0068]. The use of EAP-TLS (*e.g.*, Ex.1105, [0067]-[0074], [0100]) was a known authentication protocol that would be used to authenticate client devices. Ex.1116 [RFC2716] at 1, 2. Krantz further discloses that the security policy can include “a configuration sub-file to indicate whether or not **operating system credentials** should be used for authentication.” *Id.*, [0099].

Krantz discloses that “[i]n some embodiments, a server on a network can provide a client with limited access to the network. For example, a server located on network 413 may implement IP filtering to provide client 405 with limited access to network 413. Included in the limited access can be access to computer systems or modules that store **provisioning files needed for gaining full access to network 413.**” *Id.*, [0056].

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.1106, [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.**” *Id.*, [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. *Id.*, [0080], [0098].

Herrmann further 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.” *Id.*, [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.” *Id.*, [0071].

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

It would have been obvious to combine Herrmann with Krantz because a POSITA would have been motivated to do so based on the teachings of Krantz. For example, Krantz explains that its system relates to a server that “includes the functionality to authorize clients to access a second network” EX.1105, [0016]. EX.1105, [0002]. Similarly, Herrmann explains that “[t]he present invention relates to ... policy enforcement on **computer systems** connected on one or more networks...” EX.1106, [0003].

A POSITA would have also been motivated to apply Herrmann’s technique of checking connecting computer systems for antivirus software as it would not only provide added security but increase automation when connecting to a network. *Id.*, [0068] (“a system administrator may establish a policy requiring that **a specific virus protection program is operational on each client device** that is connected to a network. **The policy server would then evaluate whether or not each client device was in compliance** with the specified policy before approving the client device for network access.”). These are two stated goals of Krantz. EX.1105, [0014] (“Therefore what would be advantageous are systems, methods, computer program products, and data structures for increasing the level of automation when provisioning and configuring a computer system to access a network.”); *id.*, [0019] (“If credentials do not authorize full access ... the server can respond by sending a notification ... [including] conditions (e.g., signup,

renewal etc.) a user must satisfy to become authorized for full access to resources ...” Thus, A POSITA would have recognized that Herrmann’s disclosure of a policy server checking that a computer device complies with, e.g., an antivirus security policy, would be complimentary to the system of Krantz, which seeks an automated process for providing network security. In addition, a POSITA would have had a reasonable expectation of success in implementing these techniques into a combined Krantz/Herrmann system as doing would involve minimal changes to the existing Krantz system.

VIII. CLAIMS 1, 2, 4-10, 13, 16, and 18-19 ARE UNPATENTABLE

A. Ground 1: Claims 1, 2, 4, 5 and 16 are Obvious Based on Krantz

1. Claim 1

i. *[1.0] A method for network access control, the method comprising:*

The protected “*network*” of the 350 Patent can include multiple networks as opposed to only single network implementation—the 350 Patent explains, for example, that “[i]n various embodiments, Protected Network 200 includes a corporate network, telephone network, private network, local area network, wide area network, wireless network, communication network, government network, university network, and/or the like.” Ex.1101, 6:5-9. Ex.1103, ¶65.

The network disclosed in Krantz is the type of protected “*network*” described in the 350 Patent. As demonstrated in detail below, VLAN B and VLAN

C of Krantz (e.g., as depicted in Fig. 2) constitute a protected network consistent with the “*network*” of the 350 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.1105, [0017]. Each of these techniques are methods of creating a protected “*network*” because they facilitate, for example, the access control capabilities described in Krantz. Ex.1105, [0017]; Ex.1103, ¶66.

Krantz also discloses a method for “*network access control*” 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.1105, [0016]. For example, Krantz explains that “[a] client sends credentials to the server to attempt to authenticate with the server. Based on the credentials, the **server may authorize the client for at least partial access to the second network** and/or may deny access to the second network and **authorize the client for at least partial to access to the first network.**” Ex.1105, [0016]. Ex.1103, ¶67.

Based on Krantz, Dr. Houh explains that a POSITA would understand that combining the first and second networks into a logical “*network*” would be done

physically or logically. Ex.1105, [0038]. Krantz focuses on logical representations:

[A] “logical communication link” is defined as any communication path that can enable the transport of electronic data between two entities such as computer 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.1105, [0038]. Ex.1103, ¶68.

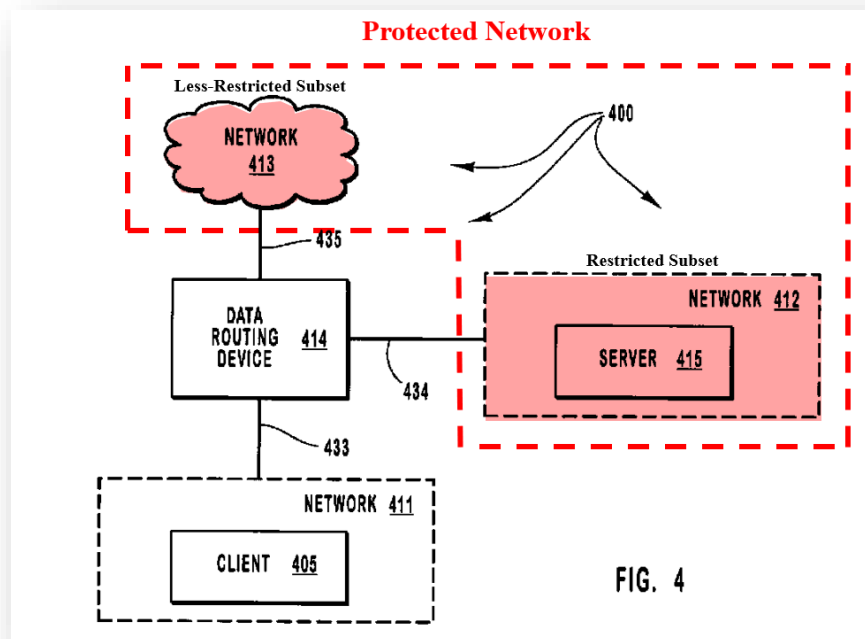
Moreover, as Dr. Houh explains, combining two (or more) physical networks together was a common technique in networking at the time. Ex.1111, 223 (defining “logical network” as “[a] network as it appears to the user. In fact, the network could be composed of two or more physical networks, or portions of these, that are linked and coordinated in a such a way that they appear to be a unit.”); Ex.1112, 317 (explaining the “difference between a network as logical or physical is sometimes subtle because the physical network (the actual layout of hardware and cabling) doesn’t necessarily resemble the logical network (the path followed by transmissions.”). Krantz itself explains that “[l]ogical communication

links **can include hardwired links, wireless links, or a combination**” thereof.

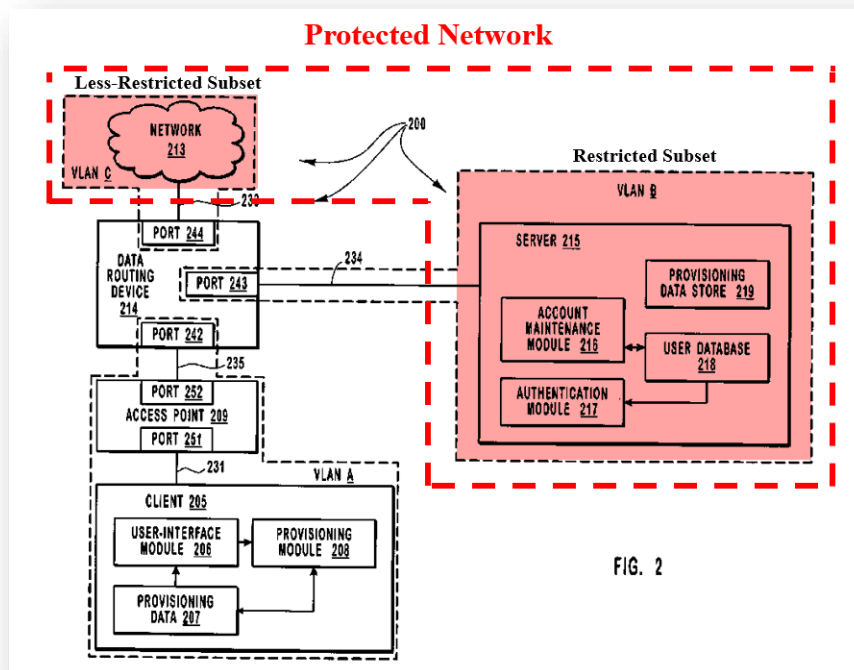
Ex.1105, [0038]. Ex.1103, ¶69.

Similarly, the 350 Patent explains that such a “*network*” may be “**physically or logically divided** into a restricted subset and one or more less-restricted subsets.” Ex.1101, 2:52-54. The 350 Patent also explains that such restricted and less-restricted subsets “are typically characterized by Virtual Local Area Networks (e.g., VLANs),” (Ex.1101, 2:66-3:4), and further explains that the protected “*network*” may include “access restrictions” (i.e., “*access control*”). Ex.1101, 6:21-33. Ex.1103, ¶70.

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



Ex.1105, Figure 4 (annotated). Ex.1103, ¶71.



Ex.1105, Figure 2 (annotated). Ex.1103, ¶71.

Krantz describes Figure 4 as “illustrat[ing] generally an example of a network architecture 400 that can provide access to a first network while restricting access to a second network.” Ex.1105, [0050]. Krantz further explains that “in some embodiments, access to resources located on network 413 can be restricted [using] Virtual Local Networks (‘VLANs’).” Ex.1105, [0052]. Ex.1103, ¶72.

Figure 2 depicts an embodiment implementing the architecture of Figure 4 and “using VLAN techniques,” which “facilitate increasing the level of automation when provisioning a client.” Ex.1105, [0057]. Figure 2 and its description thus provide specific techniques to be implemented in Krantz’s networking architecture. *See generally* Ex.1105, Figures 2 and 4 and related descriptions, [0050]-[0062].

Accordingly, the combination of Network 413 and Network 412 (annotated as VLAN C and VLAN B) constitute a “*network*.” Ex.1103, ¶72.

To the extent Patent Owner asserts that the “*network*” is required to be a single network, Krantz explains that its “*access control*” techniques can also be used “**within a single network**.” Ex.1105, [0017], [0055]. Ex.1103, ¶73.

As Krantz explains, the disclosed system “**may authorize the client for at least partial access to the single network**” (“*a method for network access control*”), and as explained in more detail below, 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.1105, [0017]; *see also* Ex.1105, [0016], [0068], [0071] [0074]-[0076], [0099], e.g., at [0068] (“[a]fter an EAP type is selected . . . **computer systems can attempt to authenticate with one another** through the transfer of EAP messages . . . in accordance with the selected EAP type. For example, when EAP-TLS is selected, **client 205 may communicate with server 215** through a series of EAP messages in accordance with EAP-TLS **so as to be authenticated and possibly authorized to access resources located on VLAN C**.”); [0104], [0107]-[0109]. Ex.1103, ¶74.

Accordingly, Krantz teaches or suggests this claim element. Ex.1103, ¶75.

- ii. *[1.1] receiving audit data pertaining to a device that does not have access to a less-restricted subset of a network;*

Krantz discloses that “a server includes the functionality to authorize [] access” to a network and/or selected elements within a network after the client 205 (“*device*”) sends credentials to the server (“*receiving audit data pertaining to a device*”). Ex.1105, [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” (it did “*not have access to a less-restricted subset of a network*” prior to sending the credentials). Ex.1105, [0017]; *See also* [0068]-[0076], [0099], [0104], [0107]-[0109] (collectively describing techniques for requesting access in a VLAN environment). Ex.1103, ¶77.

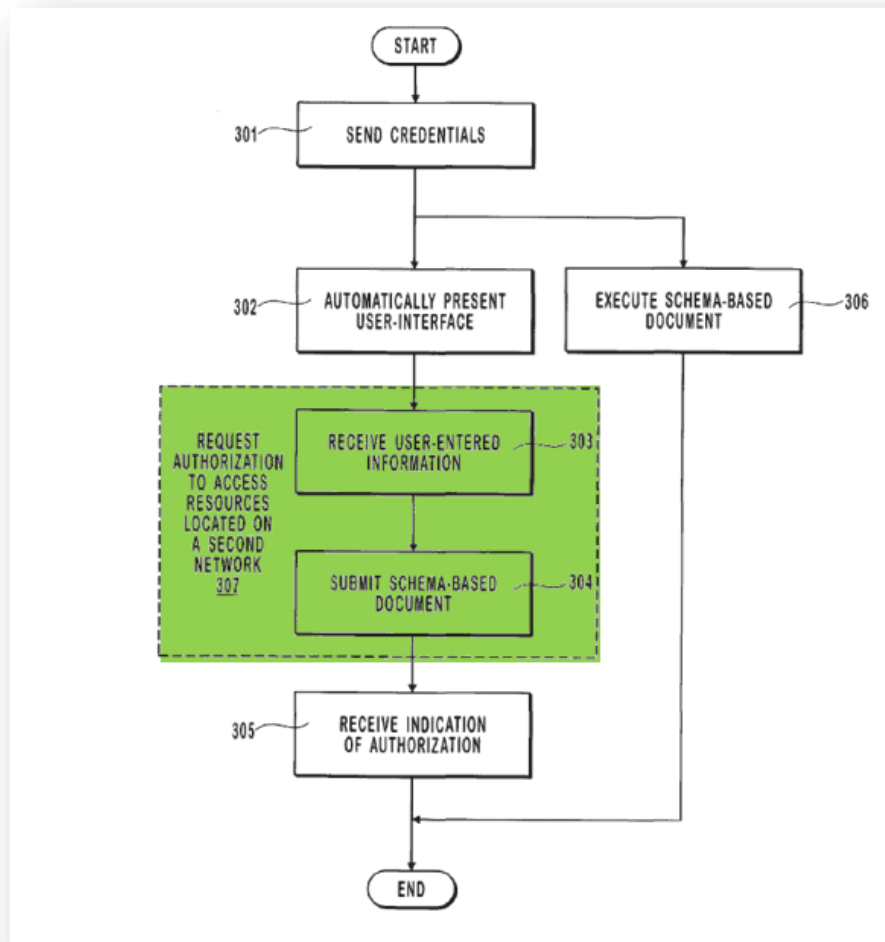
Such credentials in Krantz “can include sending an Extensible Authentication Protocol (“EAP”) Response/Identity message from the client to the server. If the client is attempting to connect to a network via an access point, the EAP Response/Identity message may be encapsulated within some other type of message that can be transferred through the access point.” Ex.1105, [0018]. Other credentials provided from Krantz’s access “*device*” may include, for example, “user-identifier[s] and password[s].” Ex.1105, [0071], [0074], [0076]. Ex.1103, ¶78.

Krantz explains that credentials are audited at the server as “authentication module 217 can receive the credentials (e.g., user-identifier and password) **and compare the credentials to entries in user database 218**. If credential information matches an entry in user database 218, the identity of a user is authenticated (i.e., server 215 believes that the user represented by the user-identifier is the user who entered the credential information). **If an authenticated user of client 205 is authorized to access resources located on VLAN C (e.g., the user is up to date on payments for their account), client 205 can then be authorized to access resources located on VLAN C.**” Ex.1105, [0076]. Krantz’s disclosure is consistent with the 350 Patent’s description that audit data can be used to authenticate a user. Ex.1101, 12:2-4 (“In some embodiments, **Authenticate User Step 440** is considered part of the **security policy audit**”); *see also*, Ex.1101, 11:34-42 (“In optional Authenticate User Step 440, Policy Auditor 325 **authenticates the identity of Access Device 230 and/or a user of Access Device 230 ... the authentication may include receipt of a user name and password ... or the like.**”). Ex.1103, ¶79.

Krantz also discloses that Figure 3 “is a flow diagram illustrating a method 300 for provisioning a computer system,” and that the disclosed “method 300 [is] described with respect to components depicted in network architecture 200.” Ex.1105, [0070]. Krantz discloses that “the method 300 includes a functional,

result-oriented step for **requesting authorization to access resources located on a second network (step 307)** (“to a less-restricted subset of a network”).

Ex.1105, [0104]; [0071]. Krantz further explains that “[s]tep 307 may include any corresponding acts for accomplishing the result of requesting authorization to access resources located on the second network.” Ex.1105, [0104]. Ex.1103, ¶80.



Ex.1105, Figure 3 (annotated). Ex.1103, ¶80.

As depicted in Figure 3, Krantz explains that the “method 300 includes act of [client 205] sending credentials to a server to attempt to authenticate with the

server,” (Ex.1105, [0071]), and step 307 “includes [the] corresponding act of receiving user-entered information (act 303). A presented user-interface can be used to receive user-entered information (e.g., user-identifier, password, name, address, credit card information, etc.) from a user at client 205” (*i.e.*, “*receiving audit data pertaining to a device that does not have access*”) Ex.1105, [0104]. Ex.1103, ¶81.

The access “*device*”—*i.e.*, “Client 205” (depicted in blue below)—sends “*audit data*” to attempt to gain access to the “*less-restricted subset of [the] network*.”

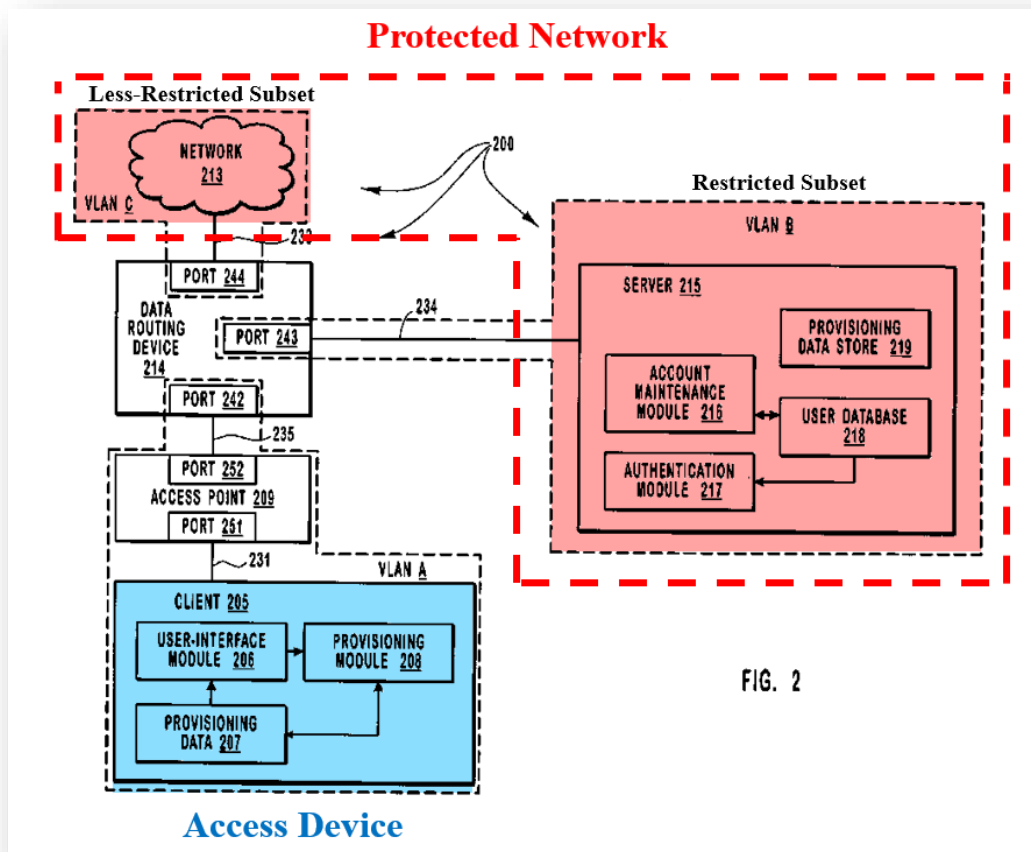


FIG. 2

Ex.1105, Figure 2 (annotated). Ex.1103, ¶82.

Moreover, as described above, *see* § VIII.A.1.i, the combination of second network VLAN C and first network VLAN B constitute a protected “network.” Krantz discloses that “[b]ased on [client] credentials, “the server **may authorize the client for at least partial access to the second network** [*i.e.*, VLAN C] **and/or may deny access to the second network** and authorize the client for at least partial to access to the first network” (*i.e.*, based on the “*audit data pertaining to the device*”) Ex.1105, [0016]; *see also* Ex.1105, [0017] (explaining that “the server (based at least in part on received credentials) may authorize the client for at

least partial access to the single network, such as, for example, by authorizing client access to selected computer systems or modules on the single network.”). Similarly, Krantz explains that its access methods “include[] a functional, result-oriented step **for requesting authorization to access resources located on a second network.**” Ex.1105, [0104]. Ex.1103, ¶83.

In Krantz, the “second network”—VLAN C—is a “*less-restricted subset of a network*” because it provides “full access to [its] resources” to authorized users, *see* Ex.1105, [0019], just like the “*less-restricted subset of a network*” described in the 350 Patent. For example, the 350 Patent explains that “[t]he less-restricted subset being **less restricted** relative to the restricted subset **in terms of what elements may be included in each subset.**” Ex.1101, 5:43-45. The “*less-restricted subset of a network*” as described in the 350 Patent provides greater access to elements and/or resources than the restricted subset³. Ex.1103, ¶84.

Accordingly, Krantz teaches or suggests this claim element. Ex.1103, ¶85.

iii. [1.2] auditing the device in accordance with a security policy based at least in part on the audit data,

As explained above, *see* §VIII.A.1.ii, Krantz discloses “*receiving audit data pertaining to a device that does not have access to a less-restricted subset of a*

³ As described below, the restricted subset of Krantz’s “*network*” is the first network, *i.e.*, VLAN B.

network” because client 205 requests authorization and sends credentials (“*audit data*”) to access resources on the second network and “*less-restricted subset*,” i.e., VLAN C Ex.1103, ¶¶76-86.

Krantz further discloses that the received audit data allows the server to “*audit[] the device in accordance with a security policy based at least in part on the audit data.*” As an initial matter, the 350 Patent explains that “the security policies may include requirements for user identification⁴ such as usernames and passwords, configuration requirements relating to the configuration of Access Device 230 application requirements relating to applications running on Access Device 230, or the like.” Ex.1101, 6:40-45. Ex.1103, ¶¶83, 88.

Krantz discloses several specific examples of “*auditing the device in accordance with a security policy based at least in part on the audit data.*” Ex.1103, ¶89.

For instance, Krantz explains that access to the network may be controlled by “configuration settings,” which can include “supported types of encryption” or “supported types of authentication,” which can include an indication for EAP,

⁴ Krantz’s disclosure of “User Identification” as part of “*applying a security policy . . .*” is described in detail in claim 5 below.

which is short for “Extensible Authentication Protocol.” Ex.1105, [0066]-[0067]; Ex.1103, ¶89.

Krantz explains that “the server **may authorize the client for at least partial access to the second network [VLAN C] and/or may deny access to the second network** and authorize the client for at least partial to access to the first network” (“*auditing the device in accordance with a security policy*”) Ex.1105, [0016]. Krantz elaborates that “the server (based at least in part on received credentials) [*“based at least in part on the audit data”*] 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.1105, [0017]. Similarly, Krantz explains that its access methods “include[] a functional, result-oriented step **for requesting authorization to access resources located on a second network.**” Ex.1105, [0104]; Ex.1103, ¶89.

Krantz further explains that “[a]fter an EAP type is selected . . . **computer systems can attempt to authenticate with one another** through the transfer of EAP messages . . . in accordance with the selected EAP type. For example, when EAP-TLS is selected, **client 205 may communicate with server 215** through a series of EAP messages in accordance with EAP-TLS **so as to be authenticated and possibly authorized to access resources located on VLAN C.**” Ex.1105, [0068]. The use of EAP-TLS (*e.g.*, Ex.1105, [0067]-[0074], [0100]) was a known

authentication protocol that would be used to authenticate client devices. Ex.1116 [RFC2716] at 1; *see also*, Ex.1116 [RFC2716] at 2 (“The Extensible Authentication Protocol (EAP) ... provides a standard mechanism for support of additional authentication methods within PPP ... [and] support for a number of authentication schemes may be added, **including smart cards, Kerberos, Public Key, One Time Passwords, and others. To date however, EAP methods such as [6] [Security Considerations] have focussed [sic] on authenticating a client to a server.**”). Ex.1103, ¶89.

Krantz similarly discloses that “[w]hen EAP-MSChap V2 is indicated, the “MS Chap V2 Parameters element at line 67 can be included in a configuration sub-file to indicate whether **or not operating system credentials should be used for authentication.**” Ex.1105, [0099]. Ex.1103, ¶90.

Krantz also explains that both EAP-TLS and EAP-MSCHAP V2 can both be required from a client seeking access and authorization. Ex.1105, [0099] (“[B]oth of the elements . . . can be included in a configuration sub-file to indicate different EAP types, such as, for example, EAP-TLS and EAP Microsoft/Challenge/Replay Handshake Protocol Version (“EAP-MSChapV2”). Accordingly, a POSITA would understand that each of the above techniques in Krantz would be used to authenticate the client 205 (“*auditing the device in accordance with a security policy based at least in part on the audit data.*”) before authorization is granted.

E.g., Ex.1117, at 2. Ex.1103, ¶91. Moreover, as discussed with respect to [1.1], Krantz's disclosure is consistent with the 350 Patent's description that audit data can be used to authenticate a user. Ex.1101, 12:2-4; *see also*, Ex.1101, 11:34-42; Ex.1103, ¶79.

Accordingly, Krantz teaches or suggests this claim element. Ex.1103, ¶93.

iv. [1.3] reconfiguring an access point to allow access to the less restricted subset of the network in response to the security policy audit,

Krantz discloses that “access point 209 is a wireless access point that enables access to wired computer systems on VLAN B (e.g., server 215) and VLAN C (e.g., computer systems included in network 213).” Ex.1105, [0064]. Ex.1103, ¶94.

Krantz explains that after the client is audited, i.e., “*auditing the device in accordance with a security policy ...*” (*see* §VIII.A.1.iii above), “client 205 can then be authorized to access resources located on VLAN C [*allow access to the less restricted subset of the network*].” Ex.1105, [0076]; *see also* Ex.1105, [0031]. Krantz elaborates that the received credentials (“*audit data*”) are audited at the server in accordance with the security policy as described in the 350 Patent. Ex.1105, [0076]. As Dr. Houh explains, *in response to the security policy audit*, the system of Krantz can allow access to resources, through *reconfiguring an access point*. Ex.1103, ¶95.

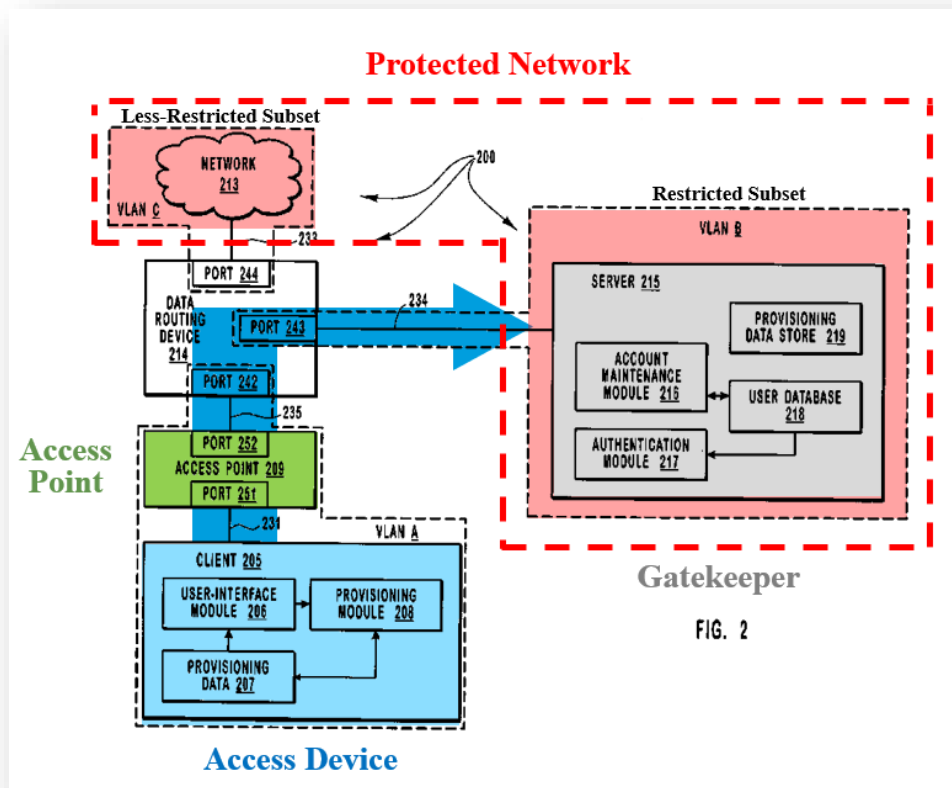
As explained below, Krantz teaches or suggests the claimed *reconfiguring an access point* in several ways.

Mapping #1

First, Krantz discloses that based on the audit results, the access point can be “*reconfigur[ed]*.” Specifically, “[a]ccess point 209 can be a wired or wireless access point **that facilitates communication between client 205 and data routing device 214**. As depicted in network architecture 200, access point 209 is connected to client 205 by corresponding logical communication link 231. ... Access point 209 includes ports 251 and 252. **Data can be transferred between access port [sic]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.** [“*reconfiguring an access point*”]. Ex.1105, at [0063]. Ex.1103, ¶97.

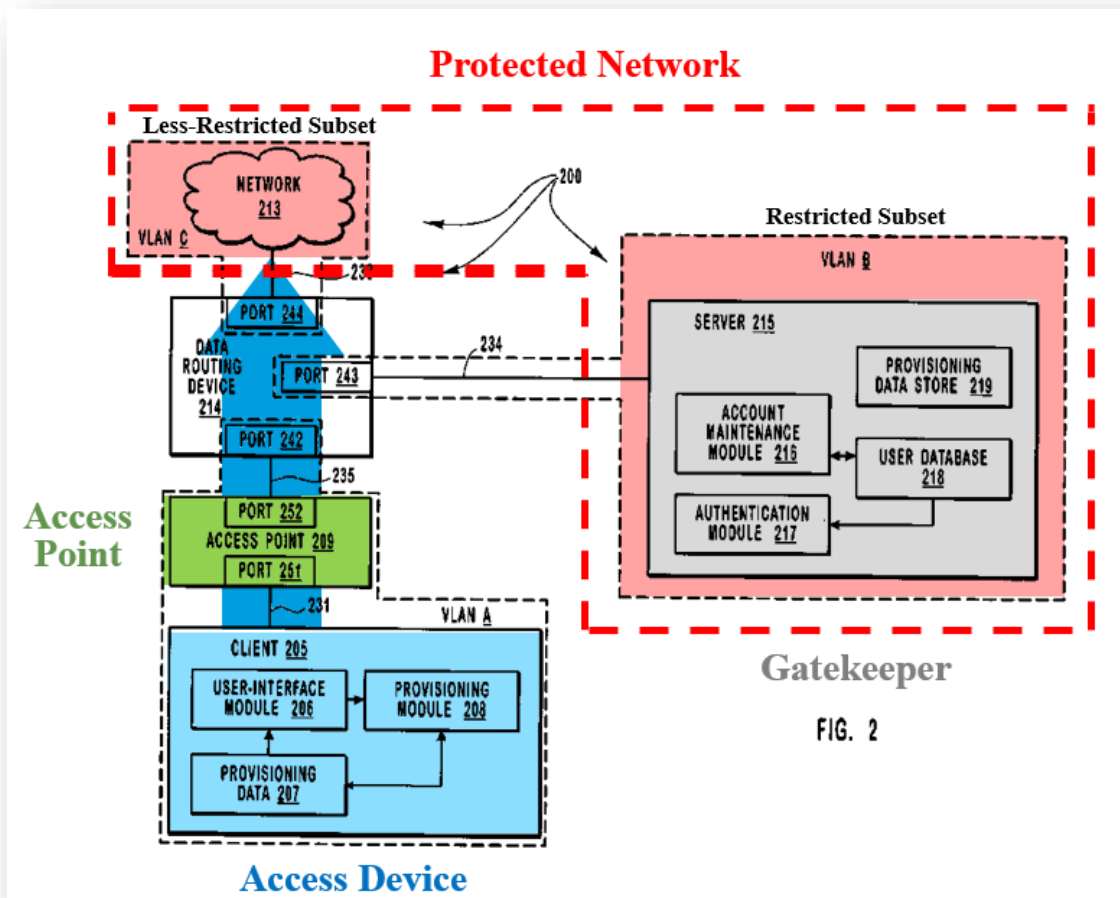
Krantz further discloses that “access point 209” (“*access point*”) is a **wireless access point that enables access to wired computer systems on VLAN B (e.g., server 215) and VLAN C (e.g., computer systems included in network 213).** Ex.1105, [0064]. The communication path between the device and **VLAN B**—the restricted subset of the protected “*network*”—is depicted in the following annotated Figure 2:

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



Ex.1105, Figure 2 (annotated). Ex.1103, ¶98.

In Krantz, access point 209 is initially configured to allow access only to VLAN B—the restricted subset of the protected “network.” Krantz further explains that access point 209 can be “reconfigur[ed]” in order “to allow access to the less restricted subset of the network” because it facilitates the transfer of data between client 205 (“the device”) and, ultimately VLAN C (the “less restricted subset of the network”), Ex.1105, [0063]-[0064], and does so “in response to the security policy audit” as explained above (see also, §VIII.A.1.ii – explaining that the device is audit[ed] in accordance with a security policy), and depicted below. Ex.1103, ¶99.



Ex.1105, Figure 2 (annotated) (“reconfiguring an access point to allow access to the less restricted subset of the network”); Ex.1103, ¶99. As discussed, this reconfiguration occurs “in response to the security policy audit.” Ex.1103, ¶95; see also, §VIII.A.1.iii.

Mapping #2

Second, Krantz explains that “[a]ccess point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to

VLAN B and/or VLAN C.” Ex.1105, [0064]; *see also* Ex.1105, [0061]-[0062]; Ex.1103, ¶¶100-101. As Krantz describes:

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

Ex.1105, [0023]; *see also* Ex.1105, [0107]. Ex.1103, ¶102.

Dr. Houh explains that Krantz is describing that when configured as a “VLAN aware device,” Krantz’s “*access point*” is being “*reconfigure[ed]*,” because Access Point 209 (via Port 251) will insert VLAN Tag Headers into incoming data frames from a client **that may now access VLAN C**, i.e., “*to allow access to the less-restricted subset.*” Ex.1105, [0107]. Port 251 (of the “*access point*”) is “*reconfigur[ed]*” because it was previously tagging incoming data from client 205, with headers that enabled access to VLAN B, i.e., the “*restricted subset*” only. Put another way, Access Point 209 is “*reconfigur[ed]*” using Port 251 to tag incoming data for transfer to VLAN C rather than VLAN B. Ex.1103, ¶103.

Specifically, Krantz discloses “[w]hen client 205 is authorized to access resources located on VLAN C, access point 209 may enable any protocols that are currently blocked for port 251 and may insert Tag Headers indicating that data

from client 205 is to be transferred to VLAN C [the “*less-restricted subset*”].

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

Ex.1105, [0107]; Ex.1103, ¶104.

Configuring input ports in VLAN aware devices to tag incoming data was a well-known technique to POSITAs by 2003. Ex.1107, 11 at Table 5-1 (explaining, for example, that when the “Reception Port receives as (and does not discard)” untagged data, it “shall support the insertion of tag headers of a format appropriate to the destination MAC, carrying a non-null VID.”); *see also* Ex.1108, 4:42-47 (“[S]ource node A transmits the packet. No VLAN tag information is present in a packet transmitted from a source node. At 415, **the packet is received at switch 305, port 2. Port 2 is configured as a member of LAN 1. Thus, a VLAN tag header is inserted in the packet** with a VID=1.”); *see also* Ex.1109, 16:4-13 (“[E]very time a message is received by the switch on a local port the VLAN designation of that port is associated with the message. Association is accomplished by a flow processing element which looks up the VLAN designation in a memory based on the local port where the message originated.”); *see also* Ex.1110, 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

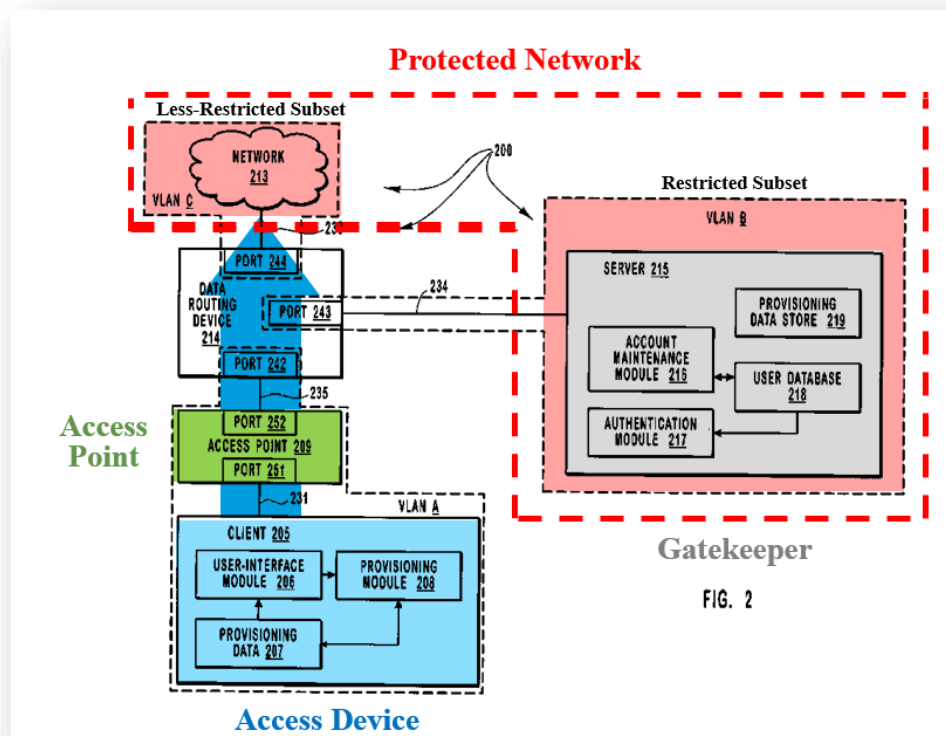
the frame exits the switched LAN, a switch strips the header and forwards the frame to interfaces that match the VLAN color.”). Ex.1103, ¶101.

Lastly, Krantz’s “*reconfiguring*” is “*in response to the security policy audit.*” As explained in §VIII.A.1.iii, Krantz discloses that access to the network may be controlled by “configuration settings,” which can include “supported types of encryption” or “supported types of authentication,” which can include an indication for EAP, which is short for “Extensible Authentication Protocol.” Ex.1105, [0066]-[0067]; Ex.1103, ¶89.

Krantz explains that “the server **may authorize the client for at least partial access to the second network [VLAN C] and/or may deny access to the second network** and authorize the client for at least partial to access to the first network” (“*in response to the security policy audit*”) Ex.1105, [0016]. 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.1105, [0017]. In addition, this “*security policy*” is applied in response to the client requesting access to resources on VLAN C. *E.g.*, Ex.1105, [0016-0018], [0071]-[0072], [0076], [0104]-[0109]. Ex.1103, ¶105.

Thus, access point 209—“*in response to the security policy audit*”—facilitates the transfer of data between client 205 (“*the device*”) and, ultimately VLAN C (“*the less restricted subset of the network.*”), Ex.1105, at [0063]-[0064],

as described above. Thus, access point 209 is “*reconfigur[ed]*” because it did not previously permit client 205 access to a less-restricted subset of the network. The reconfigured communication path between the access “*device*” and the “*less-restricted subset of the network*” is depicted again with respect to annotated Figure 2. Ex.1105, Figure 2 (annotated). Ex.1103, ¶106.



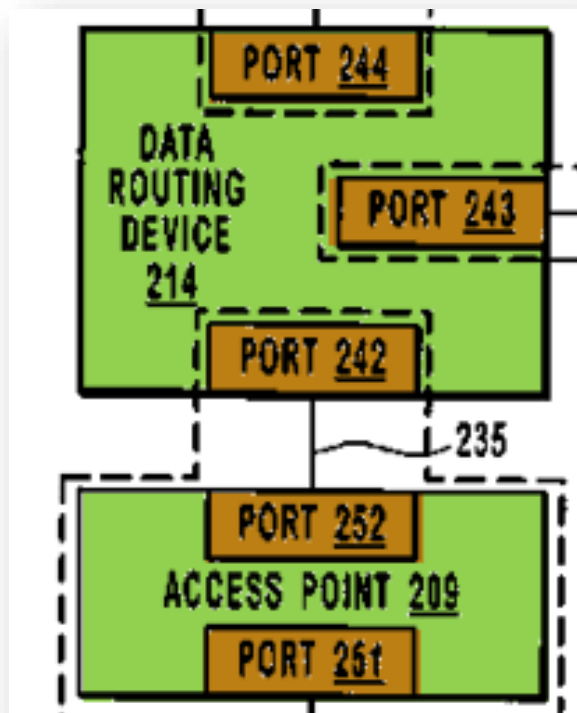
Accordingly, Krantz teaches or suggests this claim element. Ex.1103, ¶107.

Mapping #3

To the extent one may assert that Krantz does not expressly disclose the claimed “*reconfiguring an access point to allow access to the less restricted subset*

of the network,” it would have been obvious to implement other “reconfiguring” techniques in view of Krantz itself. Ex.1103, ¶108.

For example, Access Point 209 is connected to Data Routing Device 214, both of which include several communication ports (as shown below). In particular, 235 is a logical communication link connecting the two. Ex.1105, [0060]. Ex.1103, ¶109.



Ex.1105, Figure 2 (annotated). Ex.1103, ¶109.

In such a combined device, as Krantz explains, “when a portion of data, such as, for example, a data frame, is transferred in at a first port . . . **based on configuration rules**, that the frame is to be transferred out at a second port (e.g., port 243). For example, data routing device 214 can determine that a data frame

received from access point 209 is to be sent to server 215. **It may also be that a data frame is transferred in and out of data routing device 214 at the same port.** Ex.1105, [0059]. The combined device (“access point”) would be further enabled to be “*reconfigure[ed]*” at the communications ports for transfer of data from an authenticated client to VLAN C (*to allow access to the less restricted subset of the network in response to the security policy audit*). Ex.1105, [0059]-[0060] (“Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.”); Ex.1105, [0064] (“Access point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C.”). Ex.1103, ¶¶110-116.

Accordingly, Krantz teaches or suggests this claim element for this additional reason as well. Ex.1103, ¶117.

- v. ***[1.4] receiving updated audit data pertaining to the device subsequent to reconfiguring the access point; and***

Krantz discloses that the security status of the access device is monitored after reconfiguration and will require *updated audit data pertaining to the device subsequent to reconfiguring the access point* if necessary. Krantz explains that “[i]t may be that server 215 sets a **session timeout**, such as, for example, one hour,

after which access point 209 **will request client 205 to re-authenticate** [*“receiv[e] updated audit data pertaining to the device subsequent to reconfiguring the access point”*]. Moreover, Krantz explains that “[i]f 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.” Ex.1105, [0108]. However: “if a subscription period is expired at the time of re-authentication, server 215 may send an EAP-notification (or TLV object) that causes a renewal user-interface to be presented at client 205.” Ex.1105, [0108]. Krantz explains that, “[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.**” Ex.1105, [0108]. In other words, Krantz is describing a system whereby it is constantly “*receiving updated audit data pertaining to the device*” including “*subsequent to reconfiguring the access point.*” Ex.1103, ¶119.

Moreover, Krantz discloses how the “*audit data pertain[s] to the device.*” For instance, Krantz discloses that “[d]epending on the particular EAP type, server 215 can respond to the EAP-Response/Identity message in a variety of ways. Server 215 **may request that client 205 provide a password** that is associated with a user-identifier. A user of client 205 can respond by providing a password to

server 215. It may also be that **client 205 and server 215 exchange EAP-messages to pass certificates, keys, and supported cipher suites** [*“audit data pertaining to the device.”*]. Depending on the EAP type, **other credential information may also be exchanged** between client 205 and server 215.” Ex.1105, [0074]. Ex.1103, ¶120.

Krantz also discloses that “[w]hen EAP-MSChapV2 is indicated, the MSChapV2 Parameters element at line 67 can be included in a configuration sub-file to indicate **whether or not operating system credentials should be used for authentication.**” Ex.1105, [0099]; *see also*, exemplary XML configuration schema at [0091]; *see also*, Ex.1105 [0013], [0032], [0072], [0078] (outlining other security policies that may be implemented such as requiring a user to download provisioning files for gaining access to resources). Ex.1103, ¶121.

Accordingly, Krantz teaches or suggests this claim element. Ex.1103, ¶122.

vi. [1.5] monitoring continued compliance of the device with the security policy using the updated audit data.

As discussed with respect to claim limitation [1.4], Krantz discloses *receiving updated audit data pertaining to the device subsequent to reconfiguring the access point. See § VIII.A.1.v.* Krantz discloses that the device is monitored in the background, for continued compliance with the security policy, using the updated audit data. Ex.1103, ¶119.

In particular, Krantz explains that “[i]t may be that **server 215 sets a session timeout, such as, for example, one hour, after which access point 209 will request client 205 to re-authenticate** [*‘monitoring continued compliance of the device’*]. 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** [*‘with the security policy using updated audit data’*]. On the other hand, if a subscription period is expired at the time of re-authentication, server 215 may send an EAP-notification (or TLV object) that causes a renewal user-interface to be presented at client 205. 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.” Ex.1105, [0108]. In other words, the device may be continually monitored in the background for compliance with the security policy by requiring the device and/or user to reauthenticate credentials and provide updated audit data at certain time increments. Ex.1103, ¶124.

Accordingly, Krantz teaches or suggests this claim element for this additional reason as well. Ex.1103, ¶125.

Therefore, Krantz renders obvious claim 1. Ex.1103, ¶126.

2. Claim 2

- i. ***[2.0] The method of claim 1, wherein monitoring of the device for continued compliance with the security policy includes continued communications with the device.***

Krantz discloses this limitation for the same reasons addressed above with respect to claim limitations [1.4] and [1.5], which relate to “*monitoring of the device for continued compliance with the security policy*” using updated security data received from the device. *See* claim [1.4] and [1.5]. Ex.1103, ¶127.

For instance, Krantz discloses that “[i]t may be that server 215 sets a session timeout, such as, for example, one hour, after which access point 209 will request client 205 to re-authenticate. If a subscription is still valid at the time of re-authentication, client 205 **can re-authenticate in the background by submitting appropriate credentials to server 215** [“*continued communications with the device*”]. On the other hand, if a subscription period is expired at the time of re-authentication, server 215 may send an EAP-notification (or TLV object) that **causes a renewal user-interface to be presented at client 205** [another example of “*continued communications with the device*”]. 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.” Ex.1105, [0108]. Ex.1103, ¶127.

The submission of credentials from client 205 “*device*” to the server 215 and the presentation of a renewal user-interface caused by a server notification sent to the client 205 constitute “*continued communications*” with the device, achieved through what Krantz describes as “logical **communication links**” such as communication link 234. Ex.1105, [0060], Fig. 2; Ex.1103, ¶128.

Accordingly, Krantz renders obvious claim 2. Ex.1103, ¶129.

3. Claim 4

- i. ***[4.0] The method of claim 1, wherein the access point is reconfigured to allow access to a different subset of the network in response to the device failing to comply with the security policy while being monitored.***

As explained with respect to claim elements [1.3] and [1.5], Krantz discloses “*reconfiguring an access point to allow access to the less restricted subset of the network in response to the security policy audit,*” and “*monitoring continued compliance of the device with the security policy using the updated audit data.*”

This monitoring policy may include requiring the “*device*” to re-authenticate and/or renew a subscription after “*failing to comply with the security policy while being monitored.*” Ex.1105, [0108]. Krantz explains that “[a]fter appropriate completion of the renewal user-interface client 205 can be re-authenticated.”

Ex.1105, [0108]. Ex.1103, ¶130.

Krantz further explains that if a device fails to re-authenticate and/or renew a subscription the device would no longer be able to access VLAN C, and instead

would be only have access to VLAN B (“*wherein the access point is reconfigured to allow access to a different subset.*”) Krantz specifically discloses such a “*reconfigur[ation]*” with respect to “**Mapping #1**” and “**Mapping #2**” described above with respect to claim element [1.3]. Ex.1103, ¶131.

In particular, Krantz explains that in the VLAN embodiment, a failed re-authentication or failure to re-new a subscription results in the access point inserting different headers into data from client 205 so that it can only access VLAN B (and no longer VLAN C) (“*wherein the access point is reconfigured to allow access to a different subset.*”):

If a user does not appropriately complete the renewal user-interface, **access point 209 may cease inserting Tag Headers for VLAN C in data from client 205 and may instead begin inserting Tag Headers for VLAN B into data from client 205.** Access point 209 can also begin blocking protocols for port 251. Server 215 can send commands to access point 209 to cause access point 209 to block protocols and to insert appropriate Tag Headers.

Ex.1105, [0109]. A POSITA would have recognized that the techniques described with respect to **Mapping #3**, *see* § VIII.A.1.iv, *see also, e.g.*, Ex.1105, [0055] (“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”), *see also* Ex.1105, [0059] (discussing configuration rules), would also be readily applied in the scenario involving a failed re-authentication or failure to re-new subscription results. Ex.1103, ¶132

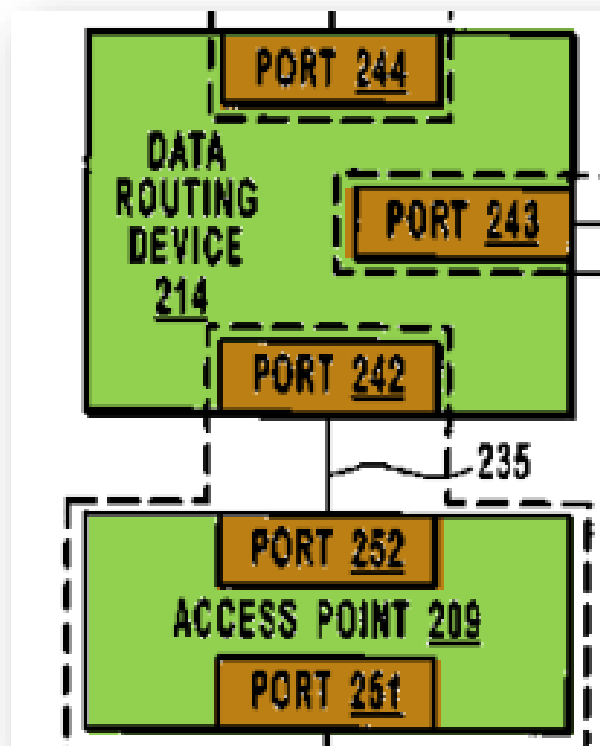
Accordingly, Krantz renders obvious claim 4. Ex.1103, ¶133.

To the extent claim 4 requires that the access point is reconfigured to allow access to a different subset of the network distinct from VLAN B or VLAN C, such an alternative reconfiguration would have been obvious view of the disclosures in Krantz itself. Ex.1103, ¶134.

As Dr. Houh explains, this is because Krantz discloses that the network architecture of Krantz is logical in nature—“network architecture 200 data routing device 214 is connected to network 213, server 215, and access point 209 by corresponding **logical communication links** 233, 234, and 235 respectively. Network 213 can be virtually any type of network, such as, for example, a corporate or enterprise-wide network ... [and] data routing device 214 can be a device **capable of grouping computer systems together in a single broadcast domain based on criteria other than physical location.**” *Id.*, [0060]. In other words, Dr. Houh explains that a POSITA would recognize that the logical nature of the Krantz network would allow it to be grouped into as many logical divisions as

necessary, for example, including additional VLANs D, E, and F. Ex.1105, [0060]; Ex.1103, ¶134.

Similarly, the access device can be reconfigured to access “*different subsets*” of the network beyond VLANs B and C. Specifically, Krantz discloses that Access Point 209 is connected to Data Routing Device 214, both of which include several communication ports (as shown below). *See also* claim element [1.3] (regarding VLAN tagging). In particular, element 235 is a logical communication link connecting the two. Ex.1105, [0060]. Ex.1103, ¶135.



Ex.1105, Figure 2 (annotated). Ex.1103, ¶135.

Krantz discloses that “data routing device 214 can be configured to separate computer systems into different VLANs. As depicted in FIG. 2, data routing device 214 has been configured to separate network architecture 200 into **VLANs A, B [Restricted Subset], and C [Less-Restricted Subset]**. Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.” Ex.1105, [0061]. While Fig. 2 depicts only 2 port connections to two exemplary VLANs (VLAN B via port 243 and VLAN C via port 244), Krantz specifically notes that additional ports may be included. *Id.*, [0063] (“Access point 209 can include **other ports (not shown)** for communicating with other computer systems.”). In view of Krantz, Dr. Houh explains that this same logic would apply to the Data Routing Device 214, which may also include other ports (not shown) to connect to numerous other VLANs. *Id.*, [0060] (“data routing device 214 can be configured to separate computer systems into different VLANs.”). Ex.1103, ¶136.

Accordingly, Krantz renders obvious claim 4 for this additional reason. Ex.1103, ¶137.

4. Claim 5

- i. ***[5.0] The method of claim 1, wherein the security policy includes authentication of the user of the device.***

Krantz discloses that “access point 209 may block [] protocols ... from being transferred **until client 205 is authenticated (and authorized)**.” Ex.1105,

[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.1105, [0076]); *see also* Ex.1105, [0074] (describing using EAP to authenticate user, including through exchange of “certificates, keys, and supported cipher suites.”. Ex.1103, ¶138.

Accordingly, Krantz renders obvious claim 5. Ex.1103, ¶139.

5. Claim 16

- i. *[16.0] The method of claim 1, wherein the security policy audit is based at least in part on the information concerning an identity of a user of the device.*

Krantz discloses that “access point 209 may block [] protocols ... from being transferred **until client 205 is authenticated (and authorized).**” Ex.1105, [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.1105, [0076]; Ex.1103, ¶176.

Accordingly, Krantz renders obvious claim 16. Ex.1103, ¶177.

B. Ground 2: Claims 6-10, 13, 18 and 19 are Obvious Based on Krantz and Herrmann

1. Claim 6

- i. *[6.0] The method of claim 4, wherein an agent running on the device collects the audit data.*

Krantz does not expressly disclose “*wherein an agent running on the device collects the audit data,*” but it would have been obvious in view of Herrmann. Ex.1103, ¶140.

As demonstrated with respect to claims 1 and 3, Krantz teaches or suggests obtaining “*audit data*” from an access “*device*” and the application of a security policy to determine if access requirements are satisfied. Ex.1103, ¶140.

Dr. Houh explains that a POSITA would have understood that one way to collect client “*audit data,*” as disclosed in Krantz, would be by utilizing an agent (or software) running on a client—although Krantz does not expressly state that such an agent is used. Ex.1106, [0028], [0067]. However, 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 section VII.C. Ex.1103, ¶141.

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.1105, [0074]. With respect to the XML configuration schema disclosed

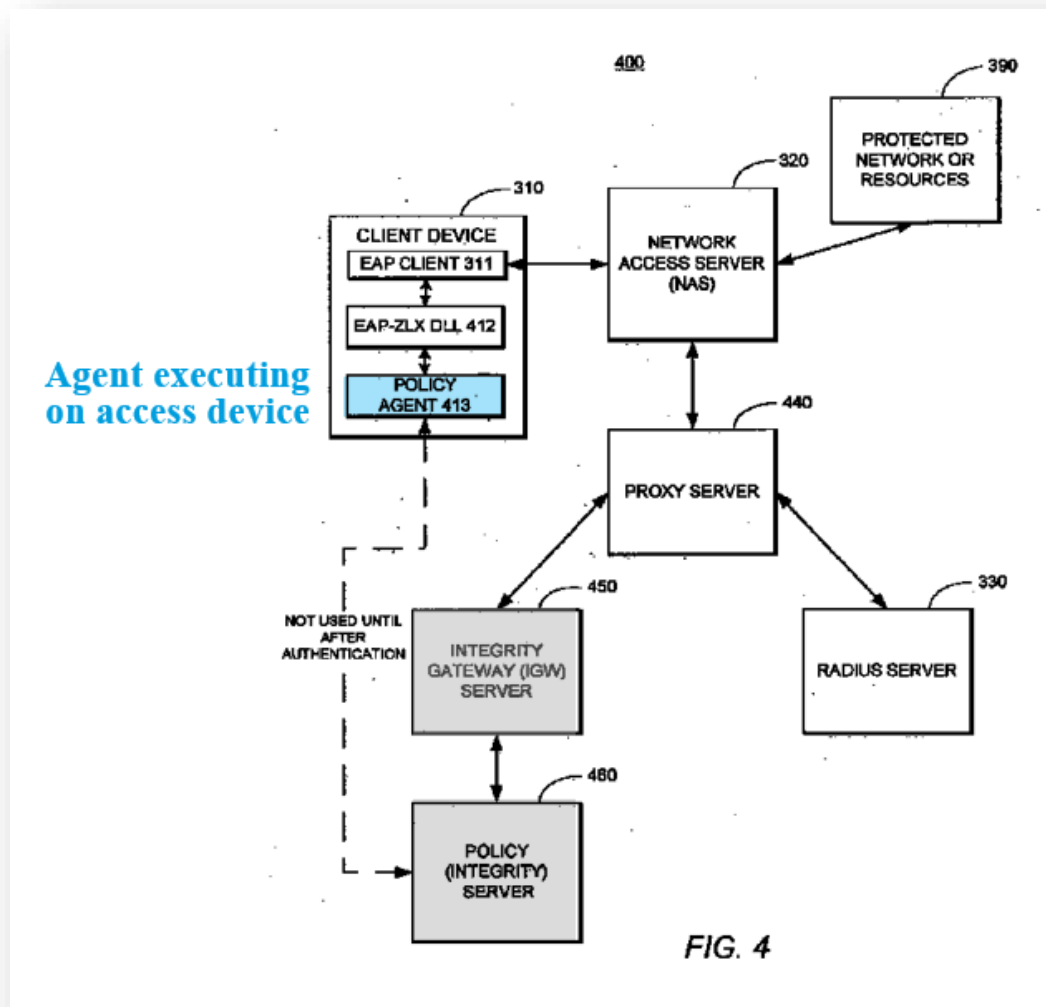
in [0091] of Krantz, a handshake protocol may be used between the access device and the gatekeeper:

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

Ex.1105 [0099]; Ex.1103, ¶143.

Krantz’s audit data (e.g., operating system credentials, certificates, keys, Response/Identity message, user-identifier and password, and supported cipher suites, etc.) would be collected by Herrmann’s Policy Agent. Ex.1103, ¶144.

For example, Herrmann discloses a “POLICY AGENT 413” (emphasized in blue) executing on the client device (an access “*device*”), interacting with a “POLICY (INTEGRITY) SERVER 350” and “INTEGRITY GATEWAY (IGW) SERVER 450” (collectively emphasized in gray) as shown below:



Ex.1106, Fig. 4 (annotated). Ex.1103, ¶145.

Herrmann discloses that “policy agent (or integrity agent) 413 to **retrieve information about the current security policy in operation on the client device 310.**” Ex.1106, [0064]. Herrmann further explains: “In response to a message from the IGW server 450 (or a subsequent message from the policy agent 413 on the client device 310), the policy server 460 evaluates whether or not the client device 310 has a correct, up-to-date version of the applicable security policy.”

Ex.1106, [0067]. The policy server is notified by the client, containing policy agent 413, through periodic status messages called “IA_HEARTBEAT(s)” in order to authenticate the access device. Ex.1106, [0080], [0098]. Ex.1103, ¶146.

A POSITA would be motivated to add the security policy agent of Herrmann to the client device of Krantz for several reasons. As explained previously, two of the stated goals of Krantz involve automation and security. Ex.1105, [0014] (“Therefore what would be advantageous are systems ... for increasing the level of automation when provisioning and configuring a computer system to access a network.”); Ex.1105, [0019] (“If credentials do not authorize full access ... the server can respond by sending a notification ... [including] conditions (e.g., signup, renewal etc.) a user must satisfy to become authorized for full access to resources ...”). Thus, Dr. Houh explains, a POSITA would have recognized that the policy **agent** of Herrmann would be complimentary and improve upon the system of Krantz, as it would provide an automated means of providing network security. Ex.1103, ¶147.

Moreover, there would be a reasonable expectation of success for adding the policy agent of Herrmann to the client device of Krantz, as Herrmann itself describes the policy agent as a “client-side component” that can communicate with an “EAP-ZLX extension DLL [which] is an implementation of the EAP protocol that is utilized to provide support for security policy negotiation and enforcement.”

Ex.1106, [0064]; *see also, id.*, [Fig. 4]. This is the same protocol utilized in Krantz. Ex.1105, [0018] (“Sending credentials can include sending an Extensible Authentication Protocol (‘EAP’) Response/Identity message from the client to the server.”). Ex.1103, ¶148.

Accordingly, Krantz in combination with Herrmann renders obvious claim 6. Ex.1103, ¶149.

2. Claim 7

- i. ***[7.0] The method of claim 6, further comprising updating the device to comply with the security policy when the device fails to comply with the security policy.***

As explained above with respect to claim 6, Krantz in view of the disclosures in Herrmann teaches or suggests “*an agent running on the device that collects the audit data.*” Ex.1103, ¶150.

In addition, Krantz explains that “[w]hen full access to resources located on the second network is not authorized [*“device fails to comply with the security policy”*] as discussed with respect to claim 1.3, *see* VIII.A.1.iii], the server can authorize limited access to the first network or second network such that **the client can download provisioning files for gaining full access [to] resources located on the second network** [*“updating the device to comply with the security policy”*].” Ex.1105, [0032]; *see also* Ex.1105, [0056] (“Client 405 can be authorized to download provisioning files from these computer systems or

modules, while being denied access to other resources located on network 413.’”); *see also* Ex.1103, ¶151.

As discussed *supra*, the claimed “*security policy*” broadly refers to a security requirement of an access device such as a user-identifier and password but can also include configuration requirements of the access device. Ex.1101, 6:38-48 (“The security policies may include requirements for user identification such as user names and passwords, **configuration requirements relating to the configuration of Access Device 230**, application requirements relating to applications running on Access Device 230, or the like.”).

Krantz similarly explains that “[i]n parallel with acts 302 through 305, the method 300 also includes an act of executing a schema-based document (act 306). **This can include executing a third schema-based document to configure a client for accessing the second network [VLAN C]** [*“updating the device to comply with the security policy”*]. Provisioning module 208 can retrieve previously downloaded XML documents, such as, for example, a configuration sub-file, from provisioning data 207.” Ex.1105, [0110] Ex.1103, ¶151.

Accordingly, Krantz and Herrmann renders obvious claim 7. Ex.1103, ¶152.

3. Claim 8

- i. ***[8.0] The method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent concerning operating system of the device.***

As explained above for claim 6, Krantz in view of the disclosures in Herrmann discloses “*an agent running on the device that collects the audit data.*” Ex.1103, ¶153.

Krantz further discloses that the *security policy audit is based at least on audit data*. As discussed *supra*, the “*security policy audit data*” may include configuration requirements relating to the access device. Ex.1101, 6:38-48. Krantz discloses that “client 205 and server 215 **exchange EAP-messages** to pass certificates, keys, and supported cipher suites.” Ex.1105, [0074]. Furthermore, with respect to the XML configuration schema disclosed in [0091] of Krantz, a handshake protocol may be used between the access device and the gatekeeper and some of the data may include “*audit data . . . concerning the operating system of the device*” as shown below:

a configuration sub-file to indicate a type of EAP [is] used to authenticate a server with a client and/or to authenticate a client with a server. Either or both of the elements at lines 61 and 62 can be included in a configuration sub-file to indicate different EAP types, such as, for example, EAP-TLS and EAP Microsoft Challenge/Replay Handshake Protocol Version (“EAP-

MSChapV2”). When EAP-MSChapV2 is indicated, the “MSChapV2 Parameters element at line 67 can be **included in a configuration sub-file** to indicate whether or not **operating system credentials** should be used for authentication.

Ex.1105 [0099]; Ex.1103, ¶154.

Accordingly, Krantz and Herrmann renders obvious claim 8. Ex.1103, ¶155

4. Claim 9

- i. *[9.0] The method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent, and that concerns antivirus software on the device.*

As explained above for claim 6, Krantz in view of the disclosures in Herrmann teaches or suggests “*an agent running on the device that collects the audit data.*” Ex.1103, ¶156.

Krantz in view of the disclosures in Herrmann further teaches or suggests that the “*audit data collected by the agent ... concerns antivirus software on the device.*” Ex.1103, ¶157.

Krantz identifies that one problem in prior art systems was that “software incompatibilities must be worked out by a user that may lack the technical expertise or desire to **re-configure software for compatibility with the service.**” Ex.1105, [0013] (emphasis added). Ex.1103, ¶158.

Krantz also specifically discusses how a connecting device may be required to have “provisioning files [] for gaining full access to network 413.” Ex.1105, [0056]; *see also*, Ex.1105, [0032], [0078] (discussing provisioning clients for gaining access to the network). Provisioning files generally relate to network connectivity and security, Ex.1109, [0079]; Ex.1105, [0016], [0087], Ex.1103, ¶159, although Krantz does not explicitly mention antivirus software as a kind of “*audit data*.” However, as demonstrated above, *see* § VII.C, a POSITA would have found it obvious to check for anti-virus software in view of Herrmann. Ex.1103, ¶159.

Herrmann, for example, specifically 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.1106, [0012]. Ex.1103, ¶160.

Herrmann further discloses that “a network administrator **may require all users accessing the network to implement a virus definition update (e.g., DAT file)** that is targeted at a particular virus.” Ex.1106, [0071]. This may be implemented using security rules and checking system data for connecting devices to ascertain compliance. Ex.1106, [0068] (“The policy server 460 may enforce a variety of different types of security policies or rules. These security policies may

include, 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.1103, ¶161.

Dr. Houh explains that a POSITA would be motivated to modify the system of Krantz to include the additional policy requiring a specific virus protection program because Krantz is specifically focused on network authentication and security. Ex.1105, [Abstract]. Further, a POSITA would have had a reasonable expectation that this additional provision would be successful because Krantz already discloses conditions for client access, such as “signup” or “renewal” conditions to authorize access to network resources. Ex.1105, [0019]. Requiring the client to update antivirus software would merely be an additional condition, which a POSITA would understand to be important as confirmed by the teachings of the 350 Patent itself. Ex.1103, ¶162.

Accordingly, Krantz in combination with Herrmann renders obvious claim 9. Ex.1103, ¶163.

5. Claim 10

- i. ***[10.0] The method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent, and that concerns other devices coupled to the device.***

As explained above for claim 6, Krantz in view of the disclosures in Herrmann teaches or suggests “*an agent running on the device that collects the audit data.*” Ex.1103, ¶164.

Krantz in view of the disclosures in Herrmann further discloses that the “*audit data collected by the agent ... concerns other devices coupled to the device.*” Ex.1103, ¶165.

While Krantz does not expressly disclose that the audit data “*concerns other devices coupled to the device,*” it would have been obvious in view of Herrmann. A POSITA would have been motivated to combine Krantz with Herrmann for the reasons described above. *See* § VII.C, *above*. In particular, it would have been obvious to include Herrmann’s techniques “*for obtaining audit data collected by an agent*” on the access device (e.g., evaluating whether or not the access device includes antivirus software) in the system of Krantz. Herrmann also discloses the use of Local Area Networks, (e.g., a corporate LAN). Ex.1106, [0012]. Herrmann discusses how “[a]n infected computer that is **connected to a particular network (e.g., a corporate LAN)** may be infected with a virus that intentionally tries to spread itself to other machines in the network. One machine that is not running the

correct anti-virus engine or is not equipped with current virus signature definition files may jeopardize the security of the entire network.” Ex.1106, [0012].

Ex.1103, ¶166.

Because of these risks, Herrmann discloses various well-known techniques such as an “agent [that] monitors and controls the interaction of the local machine **with other machines and devices that are connected on a LAN** or a larger wide area network (WAN), such as the Internet, in order to provide security to the machine.” Ex.1106, [0028]. Because any single connected device on, e.g., a corporate LAN, may jeopardize all local connected devices (including the access device), a POSITA would recognize that the policy server 460 would need to be aware of all devices connected to the access device on the LAN to ensure they each have up to date antivirus software. Ex.1106, [0057], [0067]. Ex.1103, ¶167.

Additionally, Herrmann incorporates by reference U.S. Pat. No. 5,987,611 titled “System and Methodology for Managing Internet Access on a Per Application Basis for Client Computers Connected to the Internet” to Freund. Ex.1114 (“Freund”). Freund differentiates from “people” and “computers” on a network and how “groups” can be created for either people or computers, e.g., as

depicted in Fig. 7F. Ex.1103, ¶168.

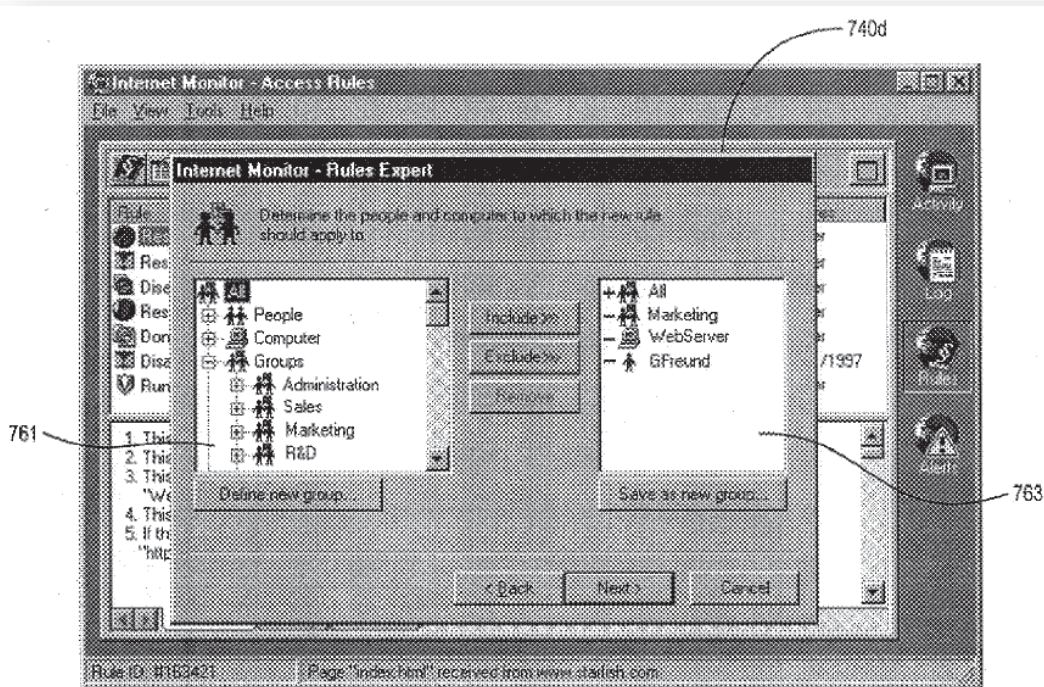


FIG. 7F

Ex.1114, Figure 7F (incorporated by reference in Herrmann).

Thus, a POSITA would recognize that in order to create such “groups” on a LAN, there would need to be an awareness (e.g., by the policy server 460) of devices connected to an access device in the LAN (“*concerns other devices coupled to the device.*”). Ex.1103, ¶169.

Accordingly, Krantz in combination with Herrmann renders obvious claim 10. Ex.1103, ¶170.

6. Claim 13

- i. ***[13.0] The method of claim 6, wherein the security policy audit is based at least in part on audit data collected by the agent, and that concerns applications executing on the device.***

As explained above for claim 6, Krantz in view of the disclosures in Herrmann teaches or suggests “*an agent running on the device that collects the audit data.*” Ex.1103, ¶171.

Krantz in view of the disclosures in Herrmann further teaches or suggests that the “*audit data collected by the agent concerns applications executing on the device.*” Ex.1103, ¶172.

As described above for claim 9, one such application includes antivirus software. Herrmann, for example, specifically 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.1106, [0012]. Ex.1103, ¶172.

Herrmann further discloses that “a network administrator **may require all users accessing the network to implement a virus definition update (e.g., DAT file)** that is targeted at a particular virus.” Ex.1106, [0071]. This may be implemented using security rules and checking system data for connecting devices to ascertain compliance. Ex.1106, [0068] (“The policy server 460 may enforce a

variety of different types of security policies or rules. These security policies may include, 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** [*“applications executing on the device”*] **that is connected to a network.”**). Because antivirus software only works if executed and because Herrmann specifically notes that the virus protection program be “operational,” a POSITA would understand that such audit data *“concerns application(s) **executing** on the device.”* Ex.1103, ¶173.

Dr. Houh explains that a POSITA would be motivated to modify the system of Krantz to include the additional policy requiring a specific virus protection program because Krantz is specifically focused on network authentication and security. Ex.1105, [Abstract]. Further, a POSITA would have had a reasonable expectation that this additional provision would be successful because Krantz already discloses conditions for client access, such as “signup” or “renewal” conditions to authorize access to network resources. Ex.1105, [0019]. Collecting audit data *concerning applications, such as virus detection software executing on the device* would merely be one additional, but important, piece of information to collect. Ex.1103, ¶174.

Accordingly, Krantz in combination with Herrmann renders obvious claim 13. Ex.1103, ¶175.

7. Claim 18

- i. ***[18.0] The method of claim 6, wherein updated audit data pertaining to the device continues to be received from the agent after reconfiguring the access point.***

As explained above for claim 6, Krantz in view of the disclosures in Herrmann teaches or suggests “*an agent running on the device that collects the audit data.*” Ex.1103, ¶178.

Krantz in view of the disclosures in Herrmann additionally discloses that updated audit data pertaining to the device *continues to be received from the agent after reconfiguring the access point.* Krantz explains that “[i]t may be that server 215 sets a **session timeout**, such as, for example, one hour, after which access point 209 **will request client 205 to re-authenticate** [*“updated audit data pertaining to the device”*]. In other words, as explained *supra* with respect to claim 1.4, Krantz is describing a system whereby it is constantly “*receiving updated audit data pertaining to the device*” including “*after to reconfiguring the access point.*” Ex.1103, ¶178.

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. On the other hand, if a subscription period is expired at the time of re-

authentication, server 215 may send an EAP-notification (or TLV object) that causes a renewal user-interface to be presented at client 205. **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 after reconfiguring the access point”*]. Ex.1105, [0108]. Ex.1103, ¶178.

Similarly, Herrmann discloses continuous monitoring, including after reconfiguration. Herrmann explains that “[a]lternatively, if the NAS supports the ability to remove the restrictive filter, then the IGW server can direct the NAS to remove the restrictive filter once the client has established compliance with the required policy. When the client has taken the necessary steps to comply with the policy, **the policy server is notified by the client (e.g., through an ‘IA_HEARTBEAT’ message, which is a periodic status message sent from the client directly to the policy server)** [*“updated audit data continues to be received from the agent after reconfiguring the access point”*]. If the policy server verifies that the client is [complies] with the assigned policy, it sends an ‘ISS_AUTH_OK’ message to the IGW server to indicate that the session should be unrestricted. In response to receiving the ‘ISS_AUTH_OK’ message from the policy server, the

IGW server directs the NAS to remove the restrictive filter.” Ex.1106, [0080].

Notably, nothing in Krantz or Herrmann suggests that the continued collection of audit data would cease once a reconfiguration occurs; instead, use a session timeout and/or a periodic “IA_HEARTBEAT” protocol suggests it would continue even after reconfiguring the access point. Ex.1103, ¶179.

Accordingly, Krantz in combination with Herrmann renders obvious claim 18. Ex.1103, ¶180.

8. Claim 19

- i. *[19.0] The method of claim 6, wherein updated audit data pertaining to the device continues to be received from the agent while the device has access to the less-restricted subset of the network.*

As explained above for claim 6, Krantz in view of the disclosures in Herrmann teaches or suggests “an agent running on the device that collects the audit data.” Ex.1103, ¶181.

Krantz in view of the disclosures in Herrmann additionally discloses that updated audit data pertaining to the device continues to be received from the agent while the device has access to the less-restricted subset of the network. As discussed above with respect to claim 18, Krantz explains that “[i]t may be that server 215 sets a **session timeout**, such as, for example, one hour, after which access point 209 will request client 205 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 client 205 can be re-authenticated.”

Ex.1105, [0108]. In other words, “*updated audit data pertaining to the device continues to be received*” for indefinite periods of time (i.e., even “*while the device has access to the less-restricted subset of the network*”). Ex.1103, ¶182.

Similarly, Herrmann discloses continuous monitoring of the device even “*while the device has access to the less-restricted subset of the network.*” Herrmann explains that “[w]hen the client has taken the necessary steps to comply with the policy, **the policy server is notified by the client (e.g., through an ‘IA_HEARTBEAT’ message, which is a periodic status message sent from the client directly to the policy server)**. If the policy server verifies that the client is [complies] with the assigned policy, it sends an ‘ISS_AUTH_OK’ message to the IGW server to indicate that the session should be unrestricted. In response to receiving the ‘ISS_AUTH_OK’ message from the policy server, the IGW server directs the NAS to remove the restrictive filter.” Ex.1106, [0080]. Ex.1103, ¶183.

As explained with respect to claim 18, nothing in Krantz or Herrmann suggests that 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.

Ex.1103, ¶184.

Accordingly, Krantz in combination with Herrmann renders obvious claim 19. Ex.1103, ¶185.

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 350 Patent (or related patents), as neither Krantz nor Herrmann were cited or considered by the Examiner during prosecution of the 350 Patent. The references in this Petition were neither relied upon during prosecution nor are cumulative of art relied upon during prosecution. Further, the 350 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 statistics⁶ on median time-to-trial for civil actions in the Northern District of California, the median time from filing to trial was 48.9 months. The related litigations were filed in May and August of 2023, so trial can be expected in approximately May 2027 and August of 2027. Any Final Written Decision can be expected in August of 2025, likely over a year before trial. Accordingly, this factor **weighs against** discretionary denial.

3. Parallel Proceeding Investment

Factor 3 **weighs against** discretionary denial. The related litigations are in its early stages of discovery, a motion to dismiss has been filed, and the investment by the parties has been relatively minimal. In addition, claim 16 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

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

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.”

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 350 Patent, is directed at the same problem and proposes the same solutions as the 350 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, 2, 4-10, 13, 16, and 18-19 of the 350 Patent are unpatentable for the reasons demonstrated above.

Dated: March 8, 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 13,812 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 8, 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 8th day of March, 2024, I caused to be served a true and correct copy of the foregoing and any accompanying exhibits by priority mail on the following:

Lewis Roca Rothgerber Christie LLP
PO BOX 29001
Glendale, CA 91209-9001

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 8, 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