

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

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

**DECLARATION OF HENRY HOUH, PH.D. UNDER 37 C.F.R. § 1.68
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW**

TABLE OF CONTENTS

	Page
EXHIBIT LIST	5
I. INTRODUCTION	6
II. QUALIFICATIONS AND PROFESSIONAL EXPERIENCE	7
III. LEVEL OF ORDINARY SKILL IN THE ART	12
IV. RELEVANT LEGAL STANDARDS	13
V. OVERVIEW OF THE 350 PATENT	15
VI. CLAIM CONSTRUCTION	18
VII. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE.....	19
VIII. THE PRINCIPAL PRIOR ART	19
A. Summary of Krantz	19
B. Summary of Herrmann.....	22
C. The Combination of Krantz and Herrmann	26
IX. KRANTZ, OR KRANTZ AND HERRMANN RENDER OBVIOUS CLAIMS 1, 2, 4-10, 13, 16, AND 18-19.....	32
A. Detailed Analysis of the Challenged Claims.....	32
1. Claim 1	32
a. [1.0] <i>A method for network access control, the method comprising:</i>	32
b. [1.1] <i>receiving audit data pertaining to a device that does not have access to a less-restricted subset of a network;</i>	39
c. [1.2] <i>auditing the device in accordance with a security policy based at least in part on the audit data;</i>	45
d. [1.3] <i>reconfiguring an access point to allow access to the less restricted subset of the network in response to the security policy audit;</i>	49

e.	[1.4] receiving updated audit data pertaining to the device subsequent to reconfiguring the access point; and.....	63
f.	[1.5] monitoring continued compliance of the device with the security policy using the updated audit data.	65
2.	Claim 2	67
a.	[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.	67
3.	Claim 4.....	68
a.	[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.	68
4.	Claim 5.....	73
a.	[5.0] The method of claim 1, wherein the security policy includes authentication of the user of the device.	73
5.	Claim 6.....	74
a.	[6.0] The method of claim 4, wherein an agent running on the device collects the audit data.	74
6.	Claim 7.....	79
a.	[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.	79
7.	Claim 8.....	80
a.	[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.	80
8.	Claim 9.....	82

a.	[9.0] <i>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.</i>	82
9.	Claim 10.....	85
a.	[10.0] <i>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.</i>	85
10.	Claim 13.....	89
a.	[13.0] <i>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.</i>	89
11.	Claim 16.....	91
a.	[16.0] <i>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.</i>	91
12.	Claim 18.....	92
a.	[18.0] <i>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.</i>	92
13.	Claim 19.....	94
a.	[19.0] <i>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.</i>	94
X.	CONCLUSION.....	96

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, Henry Houh, Ph.D., do hereby declare as follows:

I. INTRODUCTION

1. I am making this declaration at the request of Petitioner in the matter of the *Inter Partes* Review of U.S. Patent No. 8,347,350 (“the 350 Patent”) to Lum et al.

2. I am being compensated for my work in this matter at my standard hourly rate. I am also being reimbursed for reasonable and customary expenses associated with my work and testimony in this proceeding. My compensation is not contingent on the outcome of this matter or the specifics of my testimony.

3. I have been asked to provide my opinions regarding whether the subject matter of claims 1, 2, 4-10, 13, 16, and 18-19 (“the Challenged Claims”) of the 350 Patent are anticipated or otherwise would have been obvious to a person having ordinary skill in the art (“POSITA”) at the time of the alleged invention, in light of the prior art. It is my opinion that the Challenged Claims would have been obvious to a POSITA.

4. In the preparation of this declaration, I have studied:

- a. the 350 Patent, Ex.1101.
- b. the prosecution history of the 350 Patent (“350 File History”), Ex.1102.

c. U.S. Patent Pub. No. 2004/0111520 to Krantz et al., (“Krantz”),
Ex.1105.

d. U.S. Patent Pub. No. 2004/0107360 to Herrmann et al.
(“Herrmann”), (Ex.1106).

e. The additional references I refer to below and/or identified in
the exhibit list.

5. In forming the opinions expressed below, I have considered: the
documents listed above; the relevant legal standards, including the standard for
obviousness; and my own knowledge and experience based upon my work in the
field of network communications and security as described below.

6. Unless otherwise noted, all **emphasis** in any quoted material has been
added. Claim terms are *italicized*.

II. QUALIFICATIONS AND PROFESSIONAL EXPERIENCE

7. My complete qualifications and professional experience are described
in my *Curriculum Vitae*, a copy of which can be found in Ex.1104. The following
is a brief summary of my relevant qualifications and professional experience.

8. I received a Ph.D. in Electrical Engineering and Computer Science
from the Massachusetts Institute of Technology (“MIT”) in 1998. Beforehand, I
received a Master of Science degree in Electrical Engineering and Computer
Science in 1991, a Bachelor of Science degree in Electrical Engineering and

Computer Science in 1989, and a Bachelor of Science degree in Physics in 1990, all from MIT.

9. I am currently self-employed as an independent technical consultant. I am also president of a company that provides supplemental science, technology, engineering, and mathematics (“STEM”) education to children of all ages.

10. I first entered telecommunications in 1987 when I worked as a summer intern at AT&T Bell Laboratories as part of a five-year dual degree program at MIT. I continued to work at AT&T Bell Laboratories as part of this MIT program. While at MIT, I was a teaching assistant (“TA”) in the Electrical Engineering and Computer Science Department’s core Computer Architectures course. I first was a TA as a senior for a role typically reserved for graduate students. I later became head TA. The course covered various topics in computer architectures. As a TA, I helped write homework assignments, lab assignments, and exams. I also taught in the recitation sections.

11. Later, as part of my doctoral research at MIT from 1991-1998, I was a research assistant in the Telemedia Network Systems (“TNS”) group at the Laboratory for Computer Science. The TNS group built a high-speed gigabit network and created applications that ran over the network. Example applications included ones for remote video capture, processing, and display of video on computer terminals. In addition to working on the design of core network

components, designing and building the high-speed links, and designing and writing the device drivers for the interface cards, I also set up the group's web server.

12. I also helped to build the web pages that initiated the above-mentioned video sessions via a web interface. Vice President Al Gore visited our group in 1996 and received a demonstration of—and remotely drove—a radio-controlled toy car with a wireless video camera mounted on it that was built by our group. This toy car device received commands transmitted over a network from a remote computer, and video data from the toy car was transmitted wirelessly then over a computer network back to the user controller. On occasion, we allowed users visiting our web site to drive the toy car from their remote computer while they watched the video on their computer. The video stream was encoded by TNS-designed hardware, streamed over the TNS-designed network, and displayed using TNS-designed software.

13. I defended and submitted my Ph.D. thesis, titled “Designing Networks for Tomorrow’s Traffic,” in January 1998. As part of my thesis research, I analyzed local area and wide area flows to show a more efficient method for routing packets in a network, based on traffic patterns at the time.

14. From 1997 to 1999, I was a Senior Scientist and Engineer at NBX Corporation, a start-up that made business telephone systems for streaming

packetized audio over data networks instead of using traditional telephone lines.

NBX was later acquired by 3Com Corporation and the phone system is still used today by numerous businesses.

15. As part of my work at NBX, I designed the core audio reconstruction algorithms for the telephones, as well as the packet transmission algorithms. I also designed and validated the core packet transport protocol used by the phone system. The protocol was used for all signaling in the phone system, including for the setup of conference calls.

16. The NBX system also featured a computer interface for initiating phone calls, which could also initiate conference calls. The NBX system also supported the Telephony Application Programming Interface (“TAPI”) that allowed other computer programs to integrate with our system telephony features. We obtained U.S. Patent No. 6,967,963, entitled “Telecommunication method for ensuring on-time delivery of packets containing time-sensitive data,” as part of this work. During my time at NBX, I also evaluated and purchased VPN equipment in order to demonstrate that our system worked over long distances through VPN devices, so that our phones could be located remotely. We used the VPN equipment to connect from various trade shows, for example, in Las Vegas and Los Angeles, remotely into our home network so that phones in the remote network were able to connect to our home facility in Andover, MA.

17. From 1999-2004, I was employed by Empirix or its predecessor company, Teradyne. Empirix was a leader in test tools for telecommunications protocols and systems, providing functional testing tools as well as load testing tools. From 2000-2001, I conceived and built a test platform for testing Voice-over-IP (VoIP). The first application on this new test platform was a cloud emulator for simulating the effects of transmitting VoIP over a busy network.

18. In 2006, as part of my role at BBN Technologies, I helped found PodZinger Inc., now known as RAMP Inc. PodZinger utilized BBN's speech recognition algorithms to search through the spoken words in audio and video segments. While I was Vice President of Operations and Technology, PodZinger followed its initial prototype with a full streaming audio and video search solution. I also created a social networking web site, which BBN sold to a venture-funded startup company. In the process of creating the web site, I designed and specified the authentication and authorization protocols.

19. I have been awarded several United States patents, and I have several patent applications pending including the following examples:

- U.S. Patent No. 7,975,296, "Automated security threat testing of web pages";
- U.S. Patent No. 7,877,736, "Computer language interpretation and optimization for server testing";

- U.S. Patent No. 7,801,910, “Method and apparatus for timed tagging of media content”;
- U.S. Patent 7,590,542, “Method of generating test scripts using a voice-capable markup language”;
- U.S. Patent No. 6,967,963, “Telecommunication method for ensuring on-time delivery of packets containing time-sensitive data”;
- U.S. Patent Application Publication No. 20070106685, “Method and apparatus for updating speech recognition databases and reindexing audio and video content using the same”;
- U.S. Patent Application Publication No. 20070106693, “Methods and apparatus for providing virtual media channels based on media search”;
- U.S. Patent Application Publication No. 20070106760, “Methods and apparatus for dynamic presentation of advertising, factual, and informational content using enhanced metadata in search-driven media applications”;
- U.S. Patent Application Publication No. 20070112837, “Method and apparatus for timed tagging of media content”;
- U.S. Patent Application Publication No. 20070118873, “Methods and apparatus for merging media content”; and
- U.S. Patent Application Publication No. 20090222442, “User-directed navigation of multimedia search results.”

III. LEVEL OF ORDINARY SKILL IN THE ART

20. I understand there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and experience of persons working in the field at the time of the invention; (2) the

sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems.

21. 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 or graduate 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.

22. For purposes of this Declaration, in general, and unless otherwise noted, my statements and opinions, such as those regarding my own experience and what a POSITA would have understood or known generally (and specifically related to the references I consulted herein), reflect the knowledge that existed in the relevant field as of the priority date of the 350 Patent.

IV. RELEVANT LEGAL STANDARDS

23. I am not an attorney. In preparing and expressing my opinions and considering the subject matter of the 350 Patent, I am relying on certain basic legal principles that counsel has explained to me.

24. I understand that prior art to the 350 Patent includes patents and printed publications in the relevant art that predate the priority date of the 350

Patent. For purposes of this Declaration, I am applying September 24, 2003, as the priority date of the 350 Patent, but I take no position on that issue.

25. I have been informed by counsel that a claimed invention is invalid if it is “anticipated” by the prior art. I understand that, for a patent claim to be “anticipated” by the prior art, each and every requirement of the claim must be found, expressly or inherently, in a single prior art reference as recited in the claim. I understand that claim limitations that are not expressly described in a prior art reference may still be there if they are “inherent” to the thing or process being described in the prior art.

26. I understand that if a reference incorporates other documents by reference, the incorporating reference and the incorporated reference(s) should be treated as a single prior art reference for purposes of analyzing anticipation.

27. I understand that it is acceptable to consider evidence other than the information in a particular prior art document to determine if a feature is necessarily present in or inherently described by that reference.

28. I have been informed by counsel that a claimed invention is unpatentable under 35 U.S.C. § 103 if the differences between the claimed invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a POSITA. I have also been informed by counsel that the obviousness analysis considers factual inquiries,

including the level of ordinary skill in the art, the scope and content of the prior art, and the differences between the prior art and the claimed subject matter.

29. I have been further informed by counsel that there are several recognized rationales for combining references or modifying a reference to show obviousness. These rationales include: (a) combining prior art elements according to known methods to yield predictable results; (b) simple substitution of one known element for another to obtain predictable results; (c) use of a known technique to improve a similar device (method, or product) in the same way; (d) applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (e) choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; and (f) some teaching, suggestion, or motivation in the prior art that would have led a POSITA to modify the prior art or to combine prior art teachings to arrive at the claimed invention.

V. OVERVIEW OF THE 350 PATENT

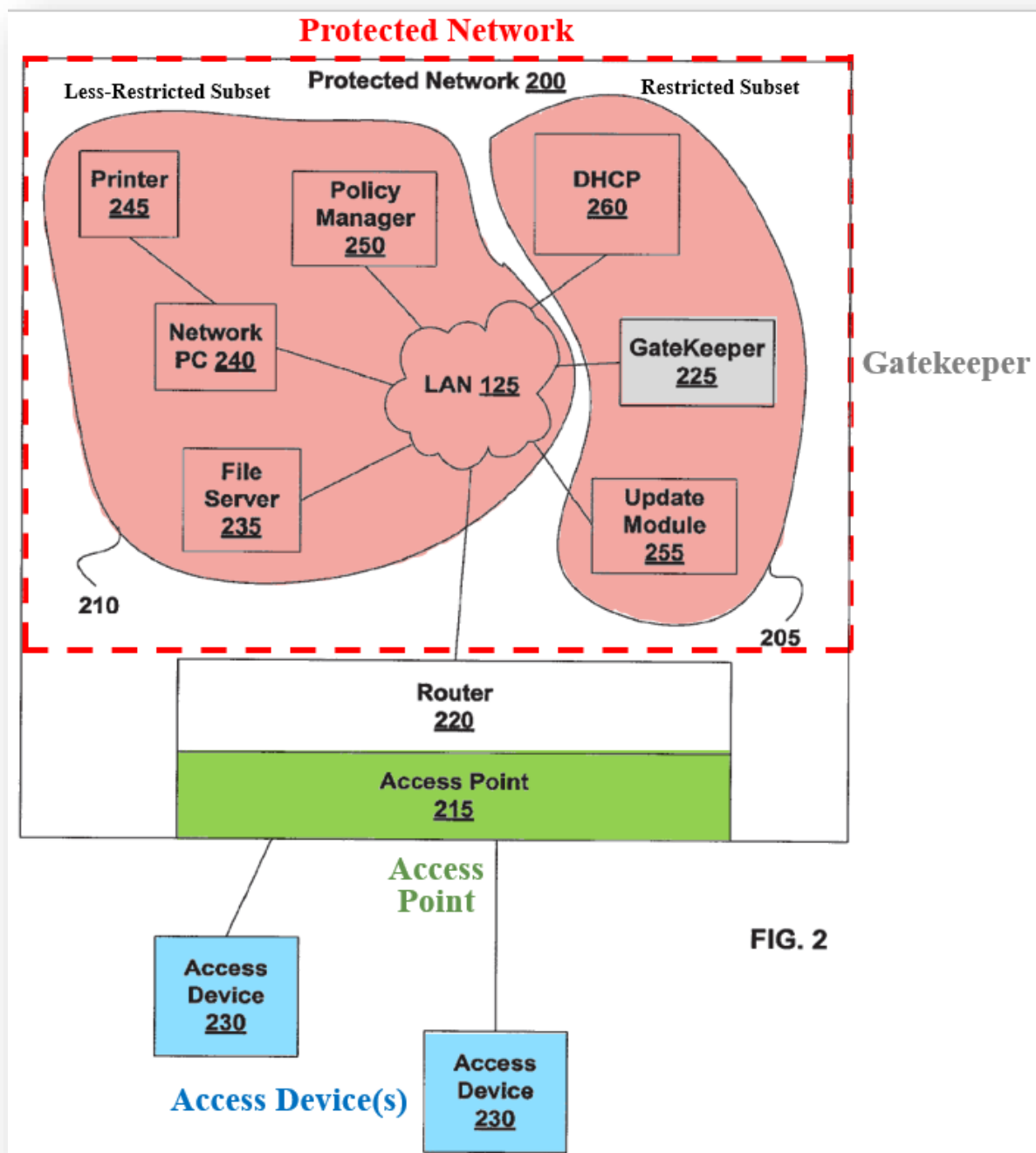
30. The 350 Patent states that it is a continuation and claims the priority benefit of U.S. patent application Ser. No. 10/949,179 filed Sep. 24, 2004 (now U.S. Pat. No. 7,523,484), which claims the priority benefit of U.S. provisional patent application No. 60/505,582 filed Sep. 24, 2003 and U.S. provisional patent application No. 60/513,080 filed Oct. 21, 2003.” Ex.1101, 1:7-18. I have been

asked to assume that **September 24, 2003** is the effective filing date, but I take no position on that issue.

31. I have reviewed the file history of the 350 Patent, including that of the aforementioned U.S. Patents, to which the 350 Patent claims priority, and note that none of the activity there is pertinent to my analysis.

32. U.S. Patent No. 8,347,350 (“the 350 Patent”) is generally directed to systems and methods that describe “a protected network physically or logically divided into a restricted subset and one or more less-restricted subsets.” Ex.1101, 2:52-54. 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”—“are then used to apply security policies” to the device requesting access. 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.

33. Figure 2 depicts various embodiments of the invention described in the 350 Patent, and is annotated below:



Ex.1101 (350 Patent), Fig. 2 (annotated)

34. For example, Figure 2 includes “Protected Network 200,” which is described in the 350 Patent as “either physically or logically divided into a

Restricted Subset 205 and a Less-Restricted Subset 210.” Ex.1101, 5:55-58. The 350 Patent also explains that 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. The 350 Patent further explains 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.).

35. However, as demonstrated below, it was well-known in the prior art to provide access control mechanisms utilizing gatekeepers that facilitate access to protected networks by user devices through the use of security policies.

VI. CLAIM CONSTRUCTION

36. It is my understanding that in order to properly evaluate the 350 Patent, the terms of the claims must first be interpreted. It is my understanding that for the purposes of this *inter partes* review, the claims are to be construed under the so-called *Phillips* standard, under which claim terms are given their ordinary and customary meaning as would have been understood by a POSITA in light of the specification and prosecution history, unless the inventor has set forth a special

meaning for a term. I have also been informed that claim terms only need to be construed to the extent necessary to resolve the unpatentability inquiry.

VII. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

37. The discussion in this Declaration provides a detailed analysis of how the asserted prior art teaches each limitation of the Challenged Claims.

38. As part of my analysis, I have considered, and discuss in detail, the scope and content of the prior art and any differences between the alleged invention and the prior art.

39. It is my opinion that the alleged invention recited in the Challenged Claims would have been obvious in view of the teachings of the asserted prior art and the knowledge of a POSITA.

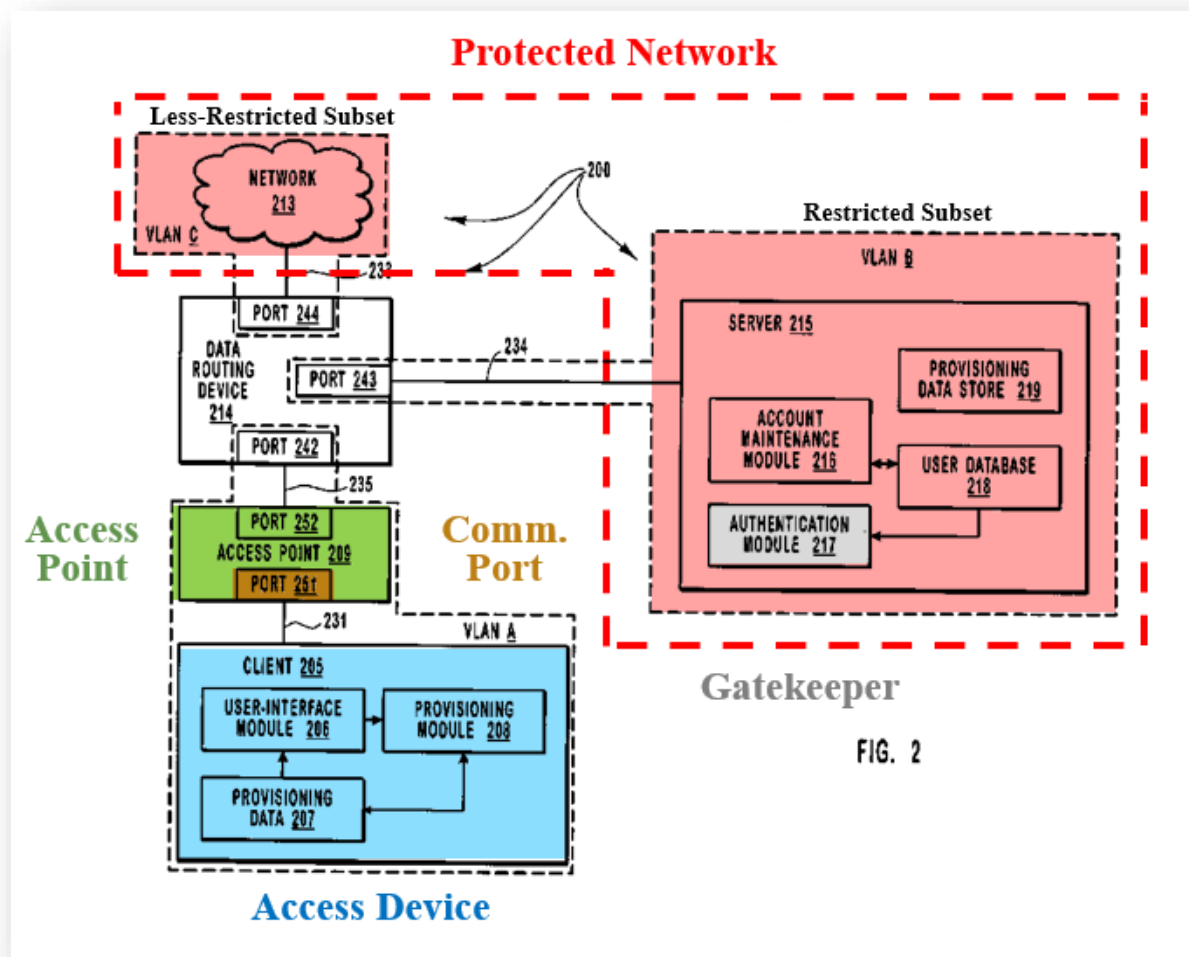
VIII. THE PRINCIPAL PRIOR ART

A. Summary of Krantz

40. 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. I understand that it is therefore prior art to the 350 Patent at least under 35 U.S.C. § 102(a) and (e).

41. Krantz is generally directed to computer-based systems and method for 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].

42. More specifically, Krantz discloses a system in which a device attempts to access a protected network. *See, e.g.*, Ex.1105, [Abstract]. To gain access to such a protected network, Krantz includes a server which can authorize at least partial access to the protected network resources based on credentials supplied by the user. *Id.*, [0016]. An embodiment of this network architecture is depicted below with respect to Fig. 2, which I have annotated:



Krantz, Fig. 2 (Ex.1105) (Annotated)

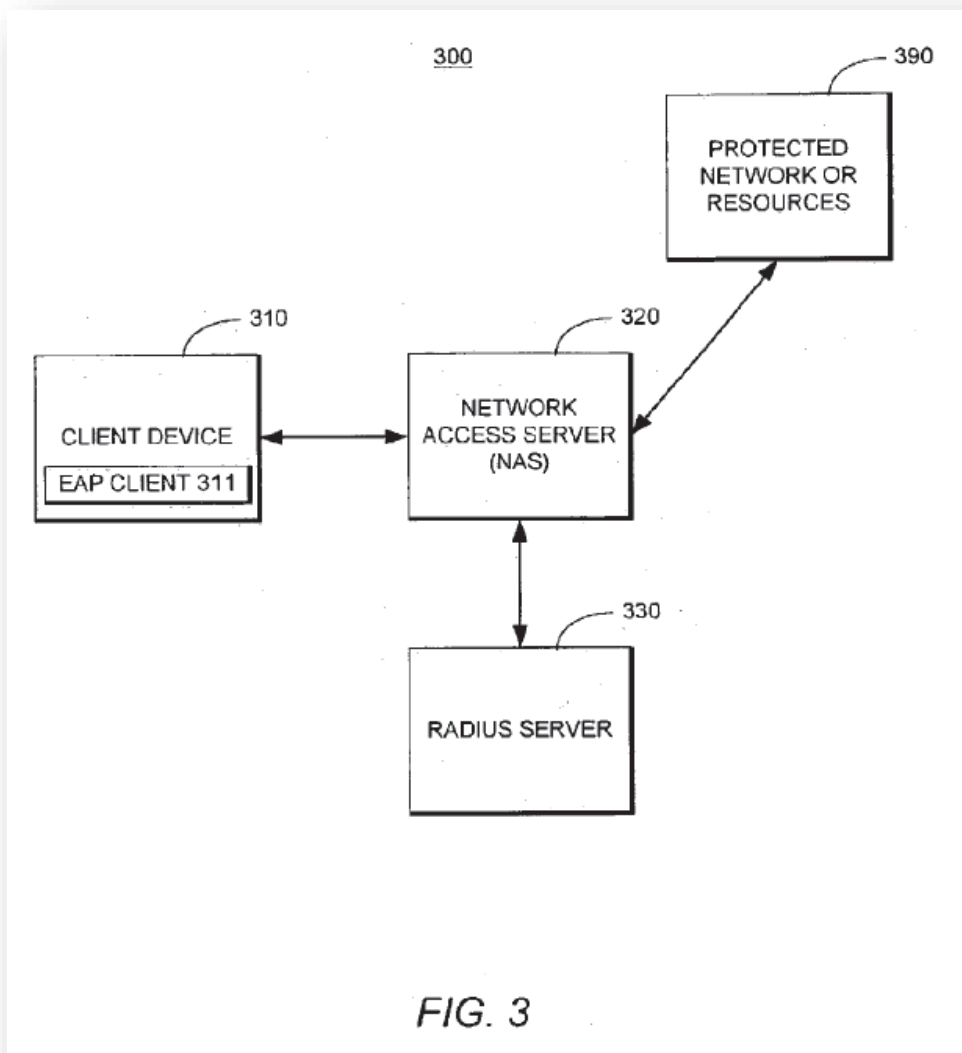
43. As seen above, and described in Krantz, the invention can utilize Virtual Local Area Network (“VLAN”) techniques. *Id.*, [0057]. Moreover, Krantz discloses that the network architecture is logical in nature and can connect sets of disparate computer systems together into one protected network. For instance, it 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.” *Id.*, [0060]. As shown above with respect to Fig. 2, Access Point 209 utilizes ports which can be configured for data transfer in particular ways. *Id.*, [0062].

44. Krantz discloses that a client (access device) requesting access to the network can send credentials to a server to authenticate itself. *Id.*, [0016]. Based upon the credentials supplied, the server “may authorize the client for at least partial access.” *Id.* This can include “at least partial access to [a] single network, such as, for example, by authorizing client access to selected computer systems or modules on the single network.” *Id.*, [0017]. Authentication may be made by authentication module 217, which acts as a gatekeeper. *Id.*, [0073].

B. Summary of Herrmann

45. U.S. Patent Pub. No. 2004/0107360 to Herrmann et al. (Ex.1106) was filed on March 13, 2003, published on June 3, 2004, and claims priority to U.S. Provisional Application No. 60/430,458, which was filed on December 2, 2002. I understand that it is therefore prior to the 350 Patent at least under 35 U.S.C. § 102(a) and (e).

46. Herrmann discloses 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 network access system is described with respect to Figs. 3 and 4. The basic architecture of the system includes at least a client access device, network access server, and protected network and/or resources are shown below in Fig. 3 of Herrmann. *Id.*, [0018].

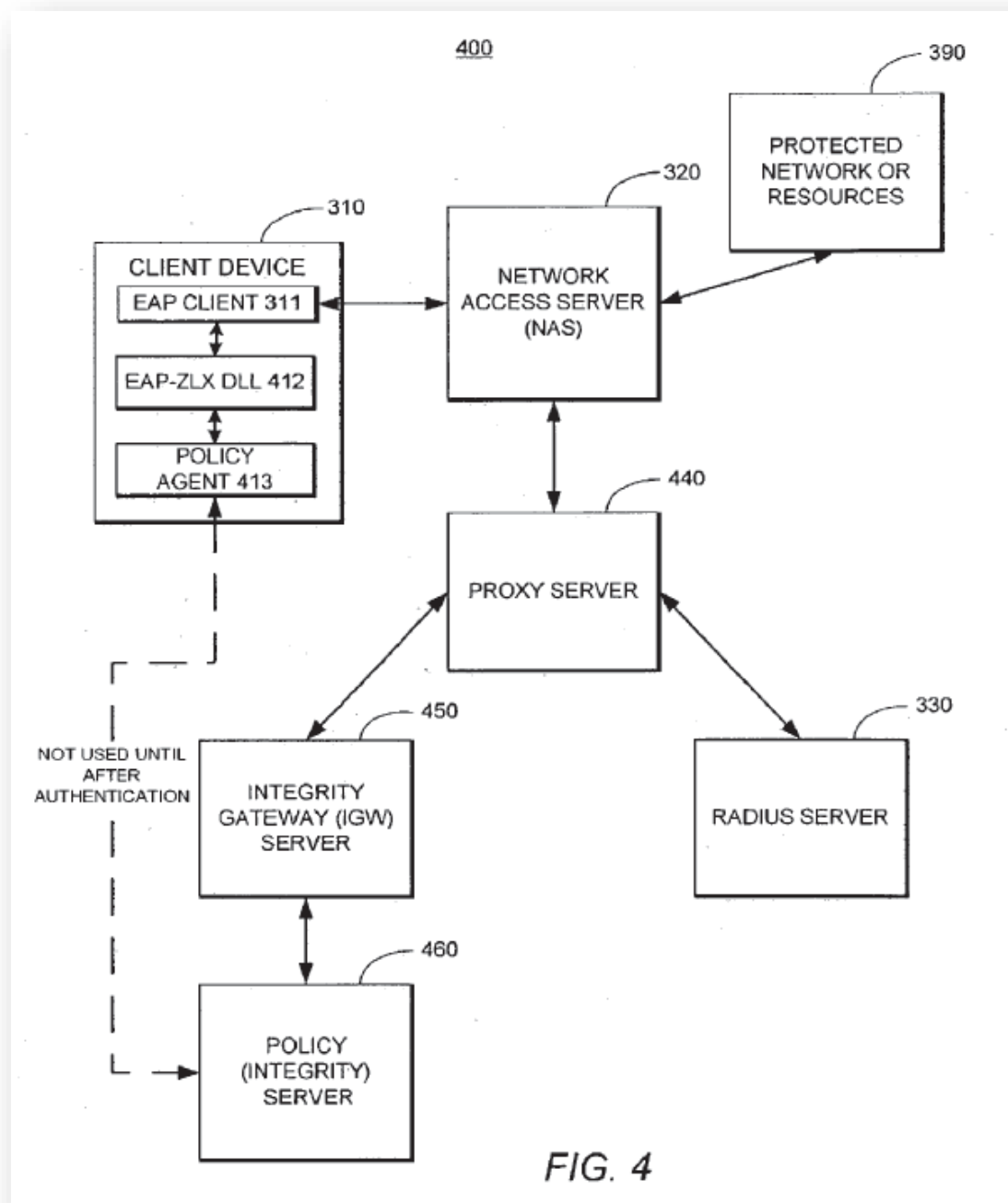


Herrmann, Fig. 3 (Ex.1106)

47. More specifically, Fig. 3 of Herrmann depicts a “network access server environment 300 ... which includes a RADIUS server providing authentication services.” *Id.*, [0053]. As shown above, “a client device 310 requesting access to a protected network 390 (e.g., the Internet, a corporate LAN or other resources) typically connects to a network access server (NAS) 320 using

client software and/or hardware such as a VPN client ... The NAS 320 acts as an access point (i.e., gateway) to a group of resources or collection of data (e.g., the protected network or resources 390) ...” *Id.*

48. Similar to Fig. 3, in the preferred embodiment of Fig. 4, “a client device 310 connects to the NAS 320 to access the protected network or resources 390.” *Id.*, [0062]. However, the system, includes an additional “policy (integrity) server 350” ... 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. *Id.*, [0067].



Herrmann, Fig. 4 (Ex.1106)

49. Fig. 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. *Id.*, [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.” *Id.*, [0067].

C. The Combination of Krantz and Herrmann

50. It would have been obvious to include Herrmann’s techniques *for obtaining system data from an access device* (e.g., evaluating whether or not the access device includes antivirus software) in the system of Krantz for the reasons explained below. In particular, the Krantz system already discloses that “access point 209 may block [] protocols ... from being transferred **until client 205 is authenticated (and authorized)**. Ex.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**.” *Id.*, [0076].

51. A POSITA would recognize that checking for anti-virus software would merely be an additional item for authentication module 217 to check in the authentication process already disclosed by Krantz. Like Krantz, Herrmann discloses a “policy server 460 [which] may enforce a variety of different types of security policies or rules.” Ex.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.” *Id.*;

see also, id., [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).

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

53. The 350 Patent itself confirms my opinion 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 a **prior art** GateKeeper 110 (Ex.1101, 2:30-31) 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.

54. 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.”).

55. *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. *See, e.g.*, Ex.1101, 1:46-48; *see also, id.*, 1:53-60 (“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.”).

56. Krantz discloses a security policy beyond mere user authentication. For instance, “client 205 and server 215 exchange EAP-messages to pass **certificates, keys, and supported cipher suites**. Depending on the EAP type, other credential information may also be exchanged between client 205 and server 215.” Ex.1105, [0074]. 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].

57. 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].

58. Herrmann similarly discloses a “policy agent (or integrity agent) 413 to retrieve information about the current security policy in operation on the client device 310. The information collected by the policy agent 413...” Ex.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)” in order to authenticate the access device. *See, id.*, [0080], [0098].

59. 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].

60. Herrmann discloses that “[t]he 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.” *Id.*, [0068].

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

62. It would have been obvious to combine Herrmann with Krantz because a POSITA would have been motivated to do so based on the teachings of Krantz. For example, Krantz explains that its system relates to “configuring **computer systems** to appropriately communicate on a network, and more specifically, to automatically providing a **computer system** with appropriate information such that **the computer system can be provisioned** to communicate on a network.” EX.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].

63. A POSITA would have also been motivated to apply Herrmann’s technique of checking connecting computer systems for antivirus software as it would not only provide added security but increase automation when connecting to a network. *Id.*, [0068] (“a system administrator may establish a policy requiring that **a specific virus protection program is operational on each client device** that is connected to a network. **The policy server would then evaluate whether or not each client device was in compliance** with the specified policy before approving the client device for network access.”). These are two stated goals of Krantz. *See, e.g.*, 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.

IX. KRANTZ, OR KRANTZ AND HERRMANN RENDER OBVIOUS CLAIMS 1, 2, 4-10, 13, 16, AND 18-19

A. Detailed Analysis of the Challenged Claims

1. Claim 1

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

64. Krantz discloses “[a] *method for network access control.*”

65. The protected “*network*” of the 350 Patent can include multiple networks as opposed to single network implementation. For instance, it explains 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.

66. The network disclosed in Krantz is such a “*network*” as described in the 350 Patent. As will be explained in the following paragraphs, and in particular, VLAN B and VLAN C of Krantz (e.g., as depicted in Fig. 4) 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] (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.”).

67. Krantz 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].

68. Based on Krantz, a POSITA would further understand that combining the first and second networks into a logical “*network*” would be done either physically or logically, although Krantz focuses more 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. . . . Logical communication links may also include portions of a virtual network, such as, for example, Virtual Private Network (“VPN”) or a Virtual Local Area Network (“VLAN”).**

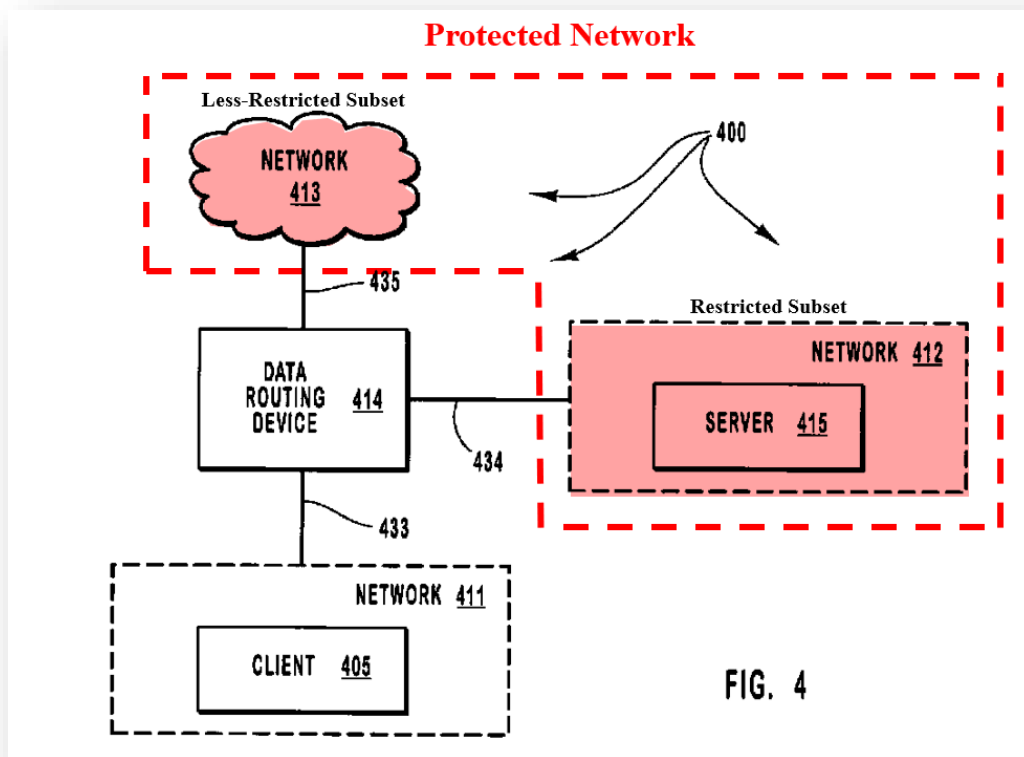
Ex.1105, [0038].

69. In fact, combining two (or more) physical networks together was a common technique in networking that was well-known to POSITAs at the time. *See, e.g.*, Ex.1111, 223 (defining a “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 that 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.”).

70. The 350 Patent describes some of the protected “*network’s*” characteristics. For example, 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., the claimed “*access control*”). Ex.1101, 6:21-33.

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



Ex.1105 (Krantz), Figure 4 (annotated)

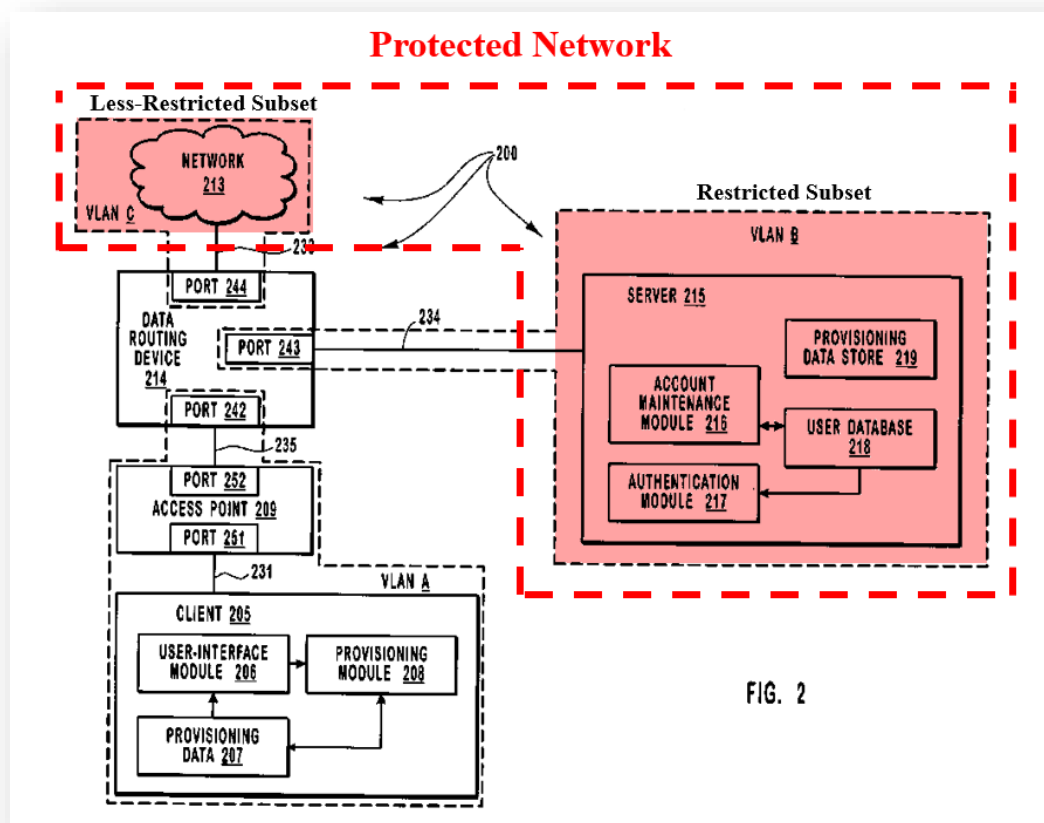


FIG. 2

Ex.1105 (Krantz), Figure 2 (annotated)

72. Krantz describes Figure 4 as “illustrat[ing] generally an example of a network architecture 400 that can provide access to a first network while restricting access to a second network.” Ex.1105, 5:65-6:2. Krantz further explains that “in some embodiments, access to resources located in network 413 can be restricted by the use of Virtual Local Networks (“VLANs”).” Ex.1105, [0052]; *see also* [0054] (similarly explaining that access to resources located on network 413 can also be restricted using VPNs). Figure 2 provides an example of such an embodiment implementing the general architecture of Figure 4 and “using VLAN techniques,”

which “can facilitate increasing the level of automation when provisioning a client.” Ex.1105, [0057]. Figure 2 and its description thus provide certain specific techniques to be implemented in Krantz’s networking architecture. *See generally* Ex.1105, Figures 2 and 4 and related descriptions. Accordingly, and as depicted above, the combination of Network 413 and Network 412 (also annotated as VLAN C and VLAN B) constitute a single logical “*network*.” Given the near similarity in disclosure between the embodiment described in Figure 2 and the 350 Patent, my analysis will focus on Figure 2 and its corresponding description, although I will refer to the general architecture represented in Figure 4 and the corresponding description as necessary.

73. 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] (“In some embodiments, similar techniques can also be used within a single network. In these embodiments, 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.**”); *see also* Ex.1105, [0055].

74. 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], [0071] [0074]-[0076] (“If credential information matches an entry in user database **218**, the identity of a user is authenticated If an authenticated user of client **205** is authorized to access resources located on VLAN C . . . client **205** can then be authorized to access resources located on VLAN C.”); [0104], [0107]-[0109].

75. Accordingly, Krantz discloses a “[*a*] *method for network access control*.”

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

76. Krantz discloses receiving from a client 205 (*i.e.*, “*device*”), “*audit data pertaining to a [the] device that does not have access to a less-restricted subset of a network*.”

77. For example, Krantz discloses that “a server has the functionality to authorize access” to a network and/or selected elements within a network after the client 205 (“*device*”) sends credentials to the server (“*receiving audit data pertaining to a device*.”). *See, e.g.*, Ex.1105, [0016], [0071]. Krantz discloses that the “server (**based at least in part on received credentials**) may authorize the

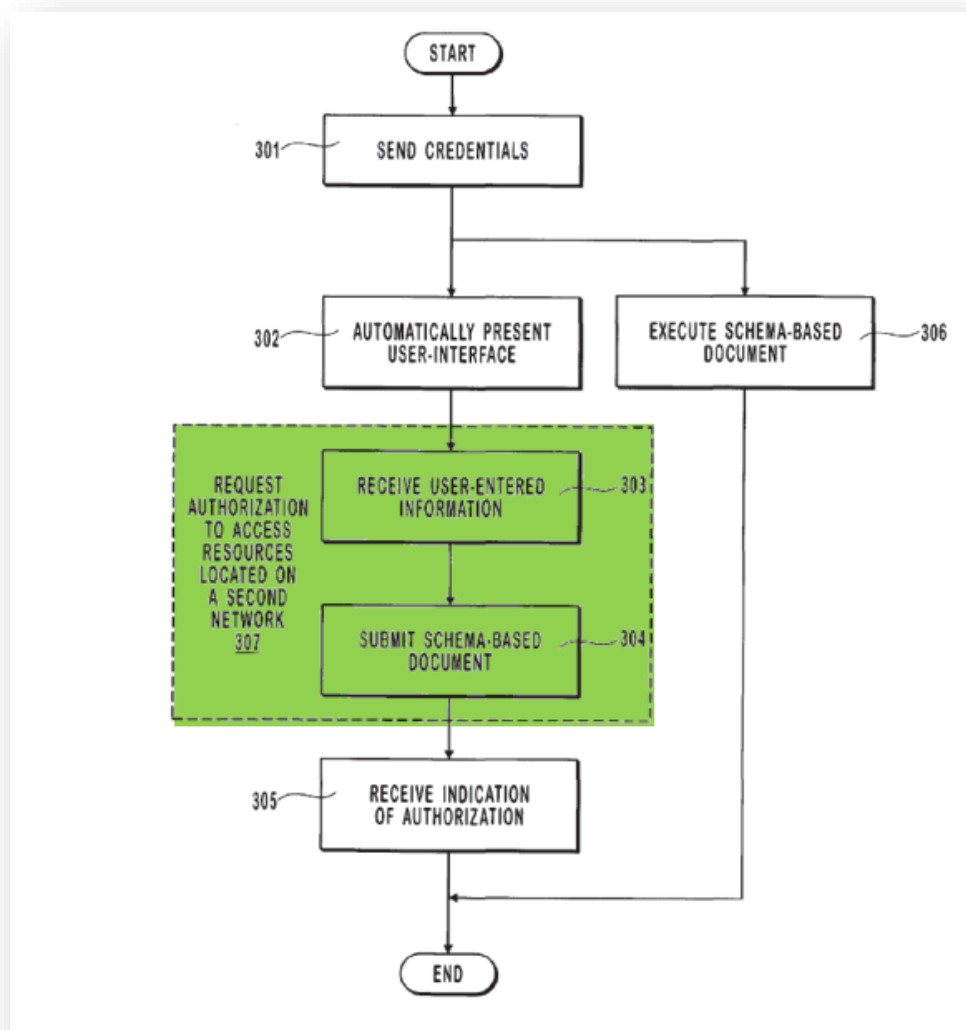
client for at least partial access to the single network” (in other words, previously it did “*not have access to a less-restricted subset of a network*”). Ex.1105, [0017]; *See also* [0074]-[0076], [0104], [0107]-[0109] (collectively describing techniques for requesting access in a VLAN environment).

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

79. Krantz elaborates that the 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.**” *Id.*, [0076]. These

disclosures of Krantz are consistent with the 350 Patent’s description that audit data can be used to authenticate a user. *See*, 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.”).

80. Krantz also explains that Figure 3 “is a flow diagram illustrating a method 300 for provisioning a computer system,” and that the disclosed “method 300 [is] described with respect to components depicted in network architecture 200.” Ex.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)**” (*i.e.*, “*to a less-restricted subset of the network*”). Ex.1105, [0104]. 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.1105 (Krantz), Figure 3 (annotated)

81. In the example depicted in Figure 3, Krantz explains that step 307 “includes [the] corresponding act of receiving user-entered information (act 303). A presented user-interface can be used to receive user-entered information (e.g., user-identifier, password, name, address, credit card information, etc.) from a user at client 205” (*i.e.*, “*receiving audit data pertaining to a device that does not have access*”). Ex.1105, [0104].

82. The “device”—i.e., “Client 205”—sending “audit data” in Krantz is depicted in Figure 2 in blue and annotated below:

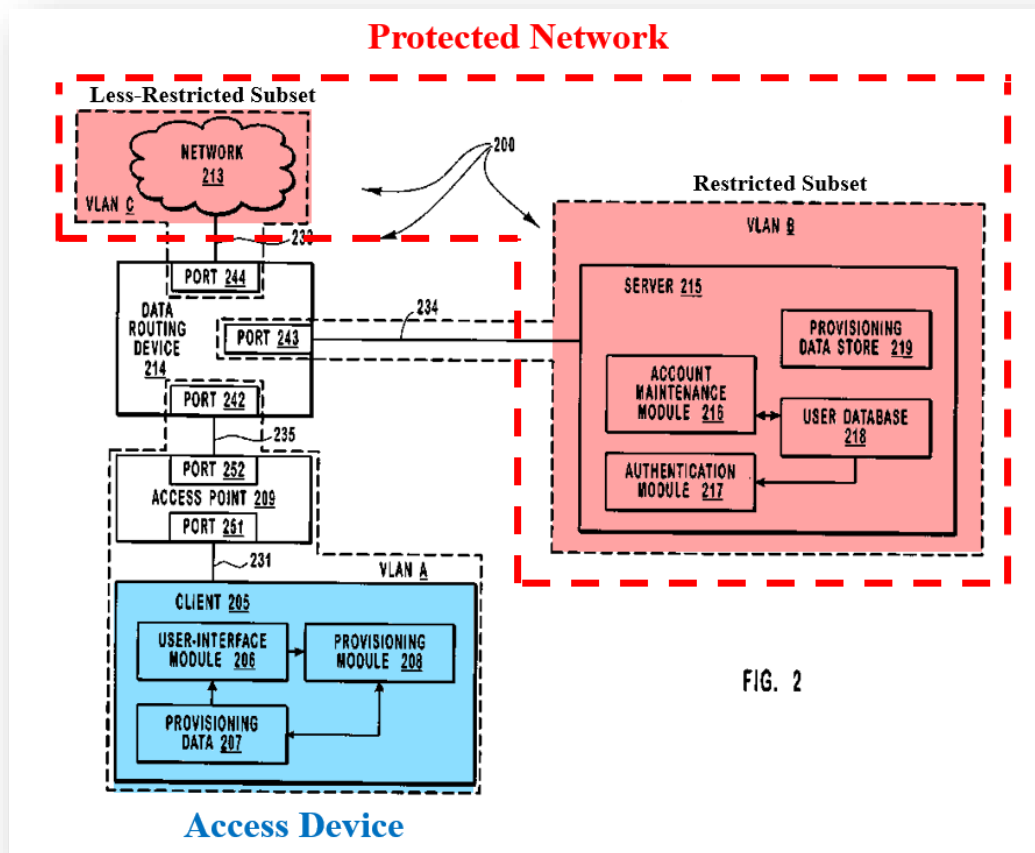


FIG. 2

Ex.1105 (Krantz), Figure 2 (annotated)

83. Moreover, as described above, *see* § X.A.1.a, the combination of second network VLAN C and first network VLAN B constitute a “network.” Krantz discloses that “[b]ased on [client] credentials, “the server **may authorize the client for at least partial access to the second network** [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].

84. In Krantz, the “second network”—*i.e.*, 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]—precisely as the “*less-restricted subset of a network*” is 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. Put another way, the “*less-restricted subset of a network*” as described in the 350 Patent provides greater access to elements and/or resources than the “*restricted subset*”⁷.

⁷ As described in greater detail below, the “*restricted subset*” of Krantz’s protected “*network*” is the first network, *i.e.*, VLAN B.

85. Accordingly, Krantz discloses “receiving audit data pertaining to a device that does not have access to a less-restricted subset of a network.”

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

86. Krantz discloses “auditing the device in accordance with a security policy based at least in part on the audit data.”

87. As explained above, see §X.A.1.b, Krantz discloses “receiving audit data pertaining to a device that does not have access to a less-restricted subset of a 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. Krantz also 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.” Krantz elaborates that “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., “auditing the device in accordance with a security policy”) Ex.1105, [0016]. Krantz goes on: “the server (based at least in part on received credentials) [i.e., “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].

88. Krantz discloses “*a security policy.*” As an initial matter, the 350 Patent explains that “the security policies may include requirements for user identification⁸ 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

89. Krantz discloses several specific examples of “*auditing the device in accordance with a security policy based at least in part on the audit data.*” For instance, Krantz explains that access to the network may be controlled by “configuration settings,” which can include “supported types of encryption” or “supported types of authentication,” which can include an indication for EAP, which is short for “Extensible Authentication Protocol.” Ex.1105, [0066]-[0067]. Krantz further explains that “[a]fter an EAP type is selected . . . **computer systems can attempt to authenticate with one another** through the transfer of

⁸ Krantz’s disclosure of “User Identification” as part of “*applying a security policy* . . . ” is described in detail in claim 5 below.

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.”)

90. 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].

91. 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 (“*applying a security policy to the access device in response to the request.*”) before authorization is granted. *E.g.*, Ex.1117, at 2 (“EAP-TLS. TLS (SSL) is the encryption method used to protect the EAP exchange. In Windows, TLS uses certificates for machine logon and user logon. The computer first authenticates to the network using a machine certificate; this allows for computer policies in the Active Directory and SMS packages to be applied before a user logs on.”)(“In Windows, PEAP supports MS-CHAPv2 in addition to TLS. PEAP-MSCHAPv2 uses machine and user credentials for authentication. MSCHAPv2 uses rotating keys to encrypt both machine and user password hashes. Certificates are still required for the authentication sever (IAS) and are used for server-to-client authentication; credentials, carried inside MSCHAPv2, are used for client-to-server authentication.”).

92. The claimed “security policy” refers to a security requirement of an access device. The “*security policy*” may include confirming a user-identifier and password and/or other information about the user. *See, e.g.*, 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 elaborates that the received credentials (“*audit data*”) are audited at the server in accordance with the security policy as described in the 350 Patent (e.g., comparing username and password credentials to entries in a user database). Ex.1105, [0076].

93. Accordingly, Krantz discloses that “*auditing the device in accordance with a security policy based at least in part on the audit data.*”

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

94. Krantz discloses “*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].

95. Krantz discloses that after the client is audited (“*auditing the device in accordance with a security policy ...*”) see claim [1.2] above, “client 205 can then be authorized to access resources located on VLAN C.” Ex.1105, [0076]; *see also* Ex.1105, [0031]. As I just discussed, 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 (e.g., comparing username and password credentials to entries in a user database). Ex.1105, [0076]. In other words, *in response to the security policy audit*, the system of Krantz can allow access to resources, through *reconfiguring an access point*, as I will explain in the next few paragraphs.

96. Krantz discloses the claimed functionality in several ways.

Mapping #1

97. First, Krantz discloses “*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). And based on the results of the *audit*, the access point can be “*reconfigur[ed]*.” Krantz explains that “[a]ccess point 209 can be a wired or wireless access point **that facilitates communication between client 205 and data routing device 214**. As depicted in network architecture 200, access point 209 is connected to client 205 by corresponding logical communication link 231. ... Access point 209 includes ports 251 and 252. **Data can be transferred between access port [sic]⁹ 209 and client 205 through port 251. Likewise, data can be transferred between access point 209 and data routing device 214**

⁹ Typo in original. “Access port 209” should refer to “Access **Point** 209.”

through port 252.” Ex.1105, at [0063]. In other words, “reconfiguring an access point.”

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

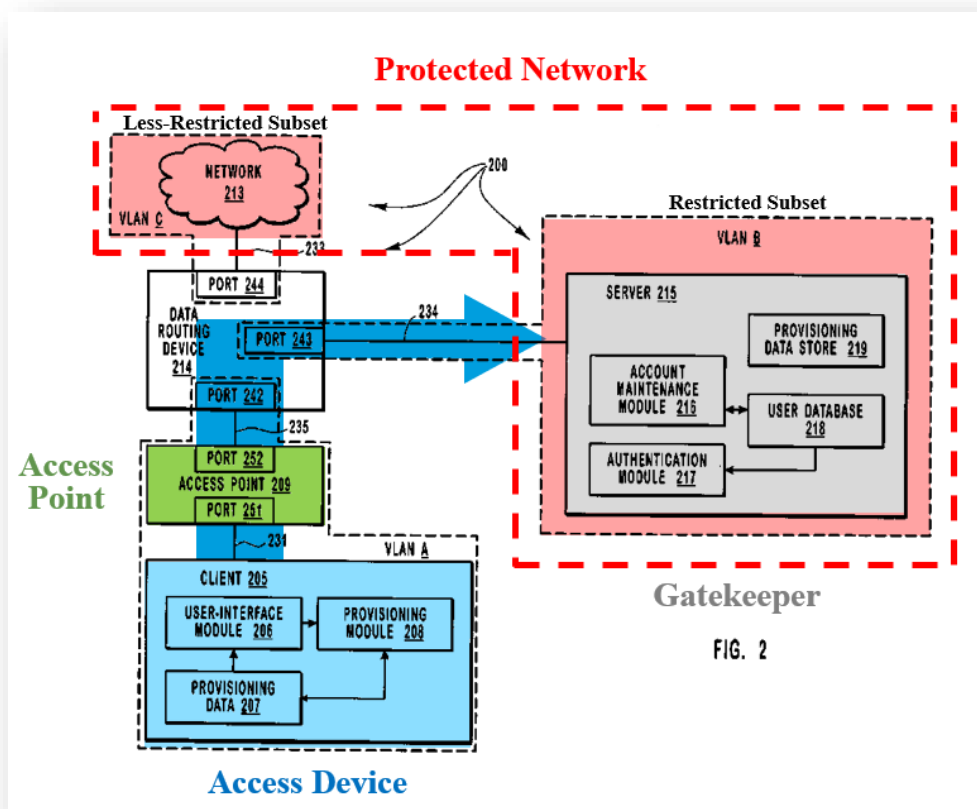
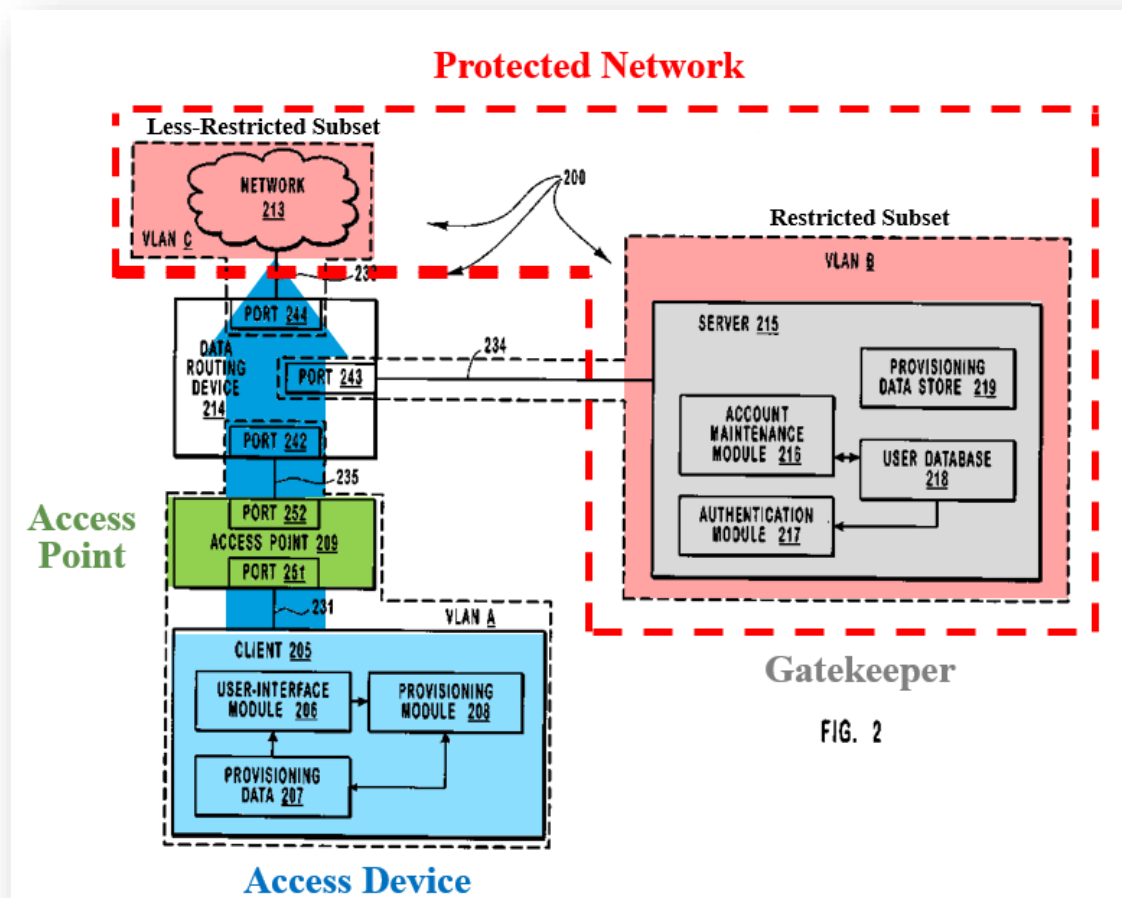


FIG. 2

Ex.1105 (Krantz), Figure 2 (annotated).

99. In Krantz, access point 209 is initially configured to allow access only to VLAN B, *i.e.*, the restricted subset of the protected “network” (as depicted above). Access point 209, including “port 251” 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.”) as depicted below. Ex.1105, at [0063]-[0064], and does so “in response to the security policy audit” as explained *supra* and in more detail below.



Ex.1105 (Krantz), Figure 2 (annotated).

Mapping #2

100. *Second*, Krantz explains that “Access point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C.” Ex.1105, at [0064]. Access Point 209 is initially configured to insert Tag Headers into data frames destined for VLAN B. Ex.1105, [0072] (“Access point 209 can insert a Tag Header into a [data] packet . . . indicating that the [data] packet is to be transferred to VLAN B.”); [0107] (explaining VLAN tagging generally).

101. Indeed, configuring ports in VLAN aware devices to tag incoming data was a well-known technique to POSITAs by 2003. Ex.1107 (IEEE 802.1Q), 11 Table 5-1 (explaining, for example, that when the “Reception Port receives as (and does not discard)” untagged data, it “shall support the insertion of tag headers of a format appropriate to the destination MAC, carrying a non-null VID.”); Ex.1108 (U.S. Patent No. 6,430,621), 4:42-47 (“[S]ource node A transmits the packet. No VLAN tag information is present in a packet transmitted from a source node. At 415, **the packet is received at switch 305, port 2. Port 2 is configured as a member of LAN 1. Thus, a VLAN tag header is inserted in the packet** with a VID=1.”); Ex.1109 (U.S. Patent No. 6,032,194), 16:4-13 (“every 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. In addition to the 402 patent, an IEEE Standards committee is preparing a standard for Virtual Bridged Local Area Networks. *See* IEEE Standard 802.1Q (draft).”); Ex.1110 (Cisco IOS 12.0 Switching Services), p.210 (“The switch that receives the frame from the source station inserts the VLAN ID and the packet is switched onto the shared backbone network. When the frame exits the switched LAN, a switch strips the header and forwards the frame to interfaces that match the VLAN color.”).

102. As Krantz also describes:

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

Ex.1105, [0023] (emphasis added).

103. Krantz is therefore explaining that when configured as a “VLAN aware device,” Krantz’s “*access point*” is “*reconfigur[ed]*” in order “*to allow access to the less restricted subset of the network*” because Access Point 209 (via Port 251) will insert VLAN Tag Headers into incoming data frames from a client

that may now access VLAN C, i.e., the “less-restricted subset.” Ex.1105, [0107].

Port 251 is “reconfigur[ed]” by Access Point 209 because it was previously tagging incoming data from client 205, as described above, with headers that enabled access to VLAN B, i.e., the “restricted subset” only. Put another way, Access Point 209 is “reconfigure[ed]” because Port 251 tags incoming data for transfer to VLAN C rather than VLAN B.

104. In particular, 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].

105. Lastly, this reconfiguration is “*in response to the security policy audit.*” As I discussed prior, 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]. As explained in Krantz, credentials are audited at the server as “authentication module 217 can receive the credentials (e.g., user-identifier and password) **and compare the credentials to entries in user database 218**. If credential information matches an entry in user database

218, the identity of a user is authenticated (i.e., **server 215 believes that the user represented by the user-identifier is the user who entered the credential information**). If an authenticated user of client 205 is authorized to access resources located on VLAN C (e.g., the user is up to date on payments for their account), client 205 can then be authorized to access resources located on VLAN C.” *Id.*, [0076]. In addition, this “*security policy*” is applied in response to the client requesting access to resources on VLAN C. *See, e.g.*, Ex.1105, [0016-0018], [0071]-[0072], [0076], [0104]-[0109].

106. 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]. 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 protected network is depicted again with respect to Figure 2, which I have annotated in blue below:



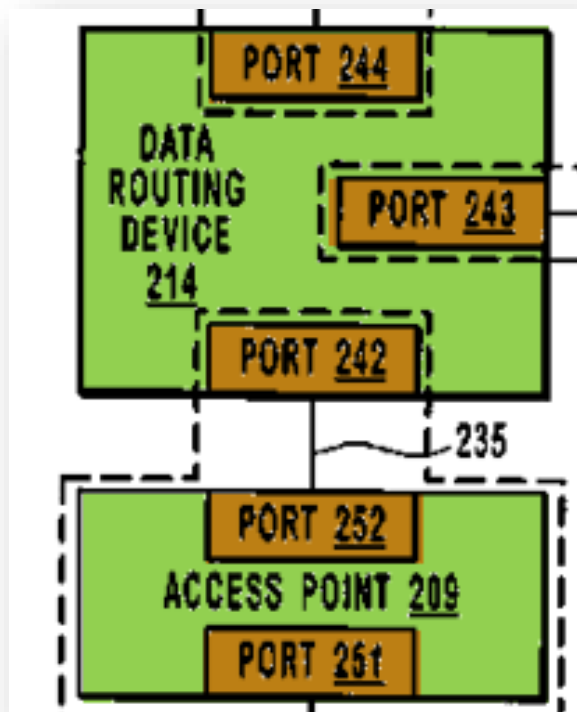
FIG. 2

FIG. 2

FIG. 2

FIG. 2

109. 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.1105 (Krantz), Figure 2 (annotated and focused)

110. 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]. VLANs B and C are depicted below for reference.

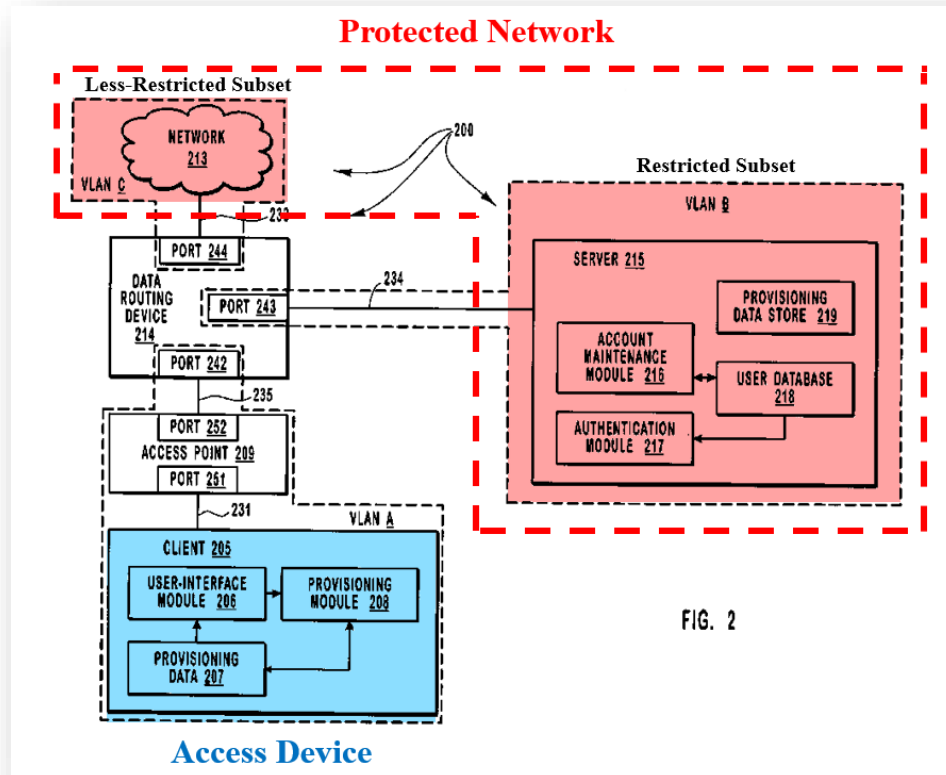


FIG. 2

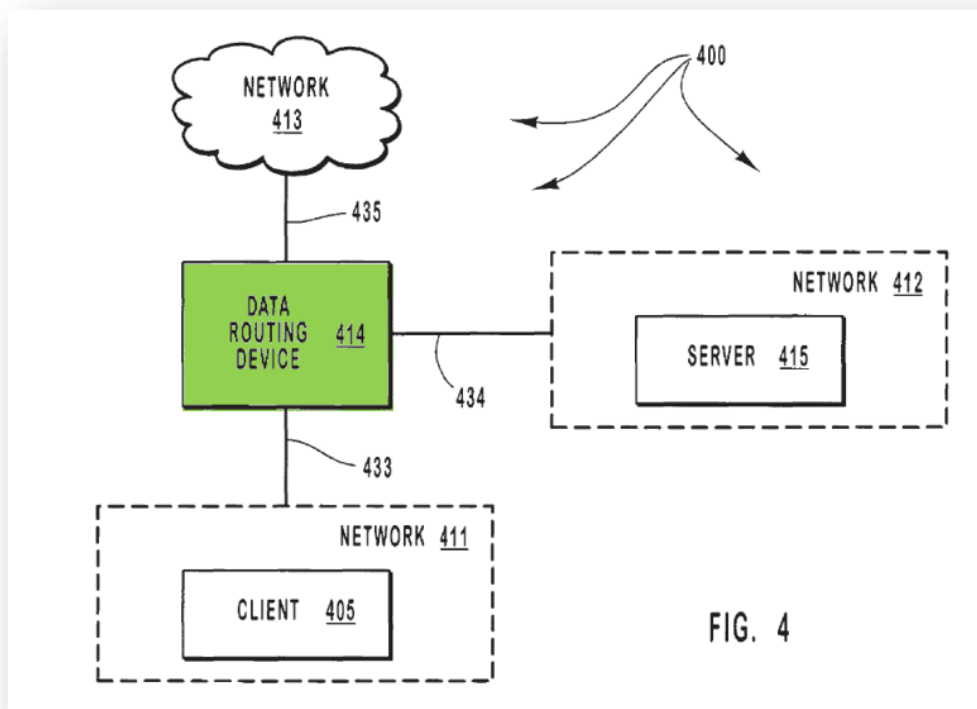
Ex.1105 (Krantz), Figure 2 (annotated)

111. For example, Krantz states that “[n]etwork architecture 200 also includes data routing device 214. **Data routing device 214** logically represents a special-purpose computer system, such as, for example, **a router and/or a switch, that can determine how to transfer data between the ports included in data routing device 214.** That is, when a portion of data, such as, for example, a data frame, is transferred in at a first port (e.g., port 242) **data routing device 214 can**

determine, based on configuration rules, that the frame is to be transferred out at a second port (e.g., port 243). For example, data routing device 214 can determine that a data frame received from access point 209 is to be sent to server 215. It may also be that a data frame is transferred in and out of data routing device 214 at the same port.” *Id.*, [0059]; *see also*, e.g., *id.*, [0060] (“Thus, data routing device 214 can be configured to separate computer systems into different VLANs.”); *see also generally, id.* [0064].

112. A POSITA would have found it obvious that the technique discussed with respect to the “data routing device 214” could simply be implemented **at the access point itself** as the data routing device is merely a “logical representation” of, e.g., a router and/or switch. Ex.1105, [0059]. In such a scheme, the Access Point 209 would implement that port configuration and data transfer techniques described with respect to “data routing device 214”).

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



114. In particular, Krantz explains that:

Data routing device 414 logically represents a computer system that can determine where to transfer data received from network 411, such as, for example, data received from client 405. That is, when data routing device 414 receives data from network 411, data routing device 414 can determine if the data is to be transferred to network 412 or network 413. As such, data routing device 414 can be configured to allow access to one network (e.g., network 412) while at the same time restricting access to another network (e.g., network 413).

Ex.1105, [0051] (emphasis added).

115. Indeed, with respect to the disclosures in Figure 2, Krantz expressly discloses that “Data routing device 214 **logically represents** a special-purpose computer system, such as, for example, a router and/or a switch, that can determine how to transfer data between the ports included in data routing device 214,” Ex.1105, [0059] so a POSITA would understand in view of that disclosure that such a “logical” architecture could readily be implemented in a single device such as an access point. Moreover, Krantz explains that such a logical implementation would include functionality that enables a “data frame” to be “transferred in and out of data routing device 214 **at the same port.**” Ex.1105, [0059] (emphasis added). In fact, Krantz repeatedly describes the “data routing” device and “access point” device as having the same functionality. *Compare, e.g.,* Ex.1105, [0060] (“Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.); [0064] (“Access point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C.”); *see also* [0069], [0073] (describing the same functionality for both the data routing device and access point). Therefore, it is clear that the functionality can occur at the access point and data routing device combined **or** the access point alone, without having any impact on the overall functionality of the system described in Krantz.

Using one technique or the other would merely have been a matter of design choice.

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

117. Accordingly, Krantz renders obvious “*reconfiguring an access point to allow access to the less restricted subset of the network in response to the security policy audit*” for this additional reason as well.

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

118. Krantz discloses “*receiving updated audit data pertaining to the device subsequent to reconfiguring the access point.*”

119. 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** [i.e., “*receive updated audit data pertaining to the device subsequent to reconfiguring the access point*”]. Krantz articulates 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. 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.” Ex.1105, [0108]. Krantz goes on to explain 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]. This means, Krantz is describing a system whereby it is constantly “*receiving updated audit data pertaining to the device*” including “*subsequent to reconfiguring the access point.*”

120. Moreover, Krantz discloses this “*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** [i.e., “*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].

121. 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).

122. Accordingly, Krantz discloses “*receiving updated audit data pertaining to the device subsequent to reconfiguring the access point.*”

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

123. Krantz discloses “*monitoring continued compliance of the device with the security policy using the updated audit data.*”

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

125. Accordingly, Krantz discloses or renders obvious “*monitoring continued compliance of the device with the security policy using the updated audit data.*”

126. Therefore, Krantz discloses or renders obvious claim 1.

2. Claim 2

- a. [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.***

127. Krantz discloses this limitation for the same reasons I discuss 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. 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].

128. 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. *See, e.g., id.*, [0060], Fig. 2.

129. Accordingly, Krantz discloses “[*t*]he method of claim 1, wherein monitoring of the device for continued compliance with the security policy includes continued communications with the device.”

3. Claim 4

- a. **[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.***

130. As I explained previously 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,” (e.g., reconfiguring the device to permit access to less-restricted subset VLAN C) and “monitoring continued compliance of the device with the security policy using the updated audit data.” Such a 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]. A POSITA would

understand this to be the case because Krantz explains that “[a]fter appropriate completion of the renewal user-interface client 205 can be re-authenticated.”

Ex.1105, [0108].

131. Additionally, as I discussed *supra*, Krantz discloses continuous monitoring of the device with respect to the security policy. *See*, Ex.1105, [0108]. This may include requiring the device to re-authenticate and/or renew a subscription [i.e., after “*failing to comply with the security policy*”]. *Id.* In other words, if a device fails to re-authenticate it would be reconfigured such that it can only access restricted VLAN B and no longer be able to access VLAN C (“*wherein the access point is reconfigured to allow access to a different subset.*”) *See, e.g.*, Ex.1105, [0072] (“access point 209 may block [] protocols ... from being transferred **until client 205 is authenticated (and authorized)** ...”). Ex.1105, [0072]; *see also*, Ex.1105, [0076]. Krantz discloses such a “*reconfigur[ation]*” with respect to “**Mapping #1**” and “**Mapping #2**” as I explained above with respect to claim element [1.3].

132. 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.

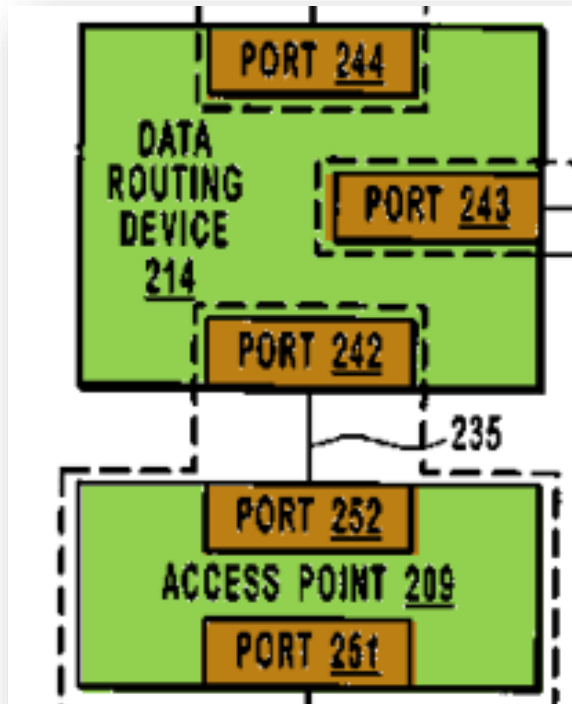
Ex.1105, [0109]. A POSITA would have recognized that the techniques described with respect to **Mapping #3**, as I discussed *supra*. *See also, e.g.*, Ex.1105, [0055] (“For example, **when client 405 is not authorized to access resources located network 413, components in network 411 or logical communication 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.

133. Accordingly, Krantz discloses 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.*”

134. 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 in light of the disclosures in Krantz itself. This is because Krantz discloses that the network architecture of Krantz is logical in nature, i.e., “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, 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, e.g., including additional VLANs D, E, and F.

135. 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).¹⁰ In particular, 235 is a logical communication link connecting the two. Ex.1105, [0060].



Ex.1105 (Krantz), Figure 2 (annotated and focused)

136. 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

¹⁰ See also, my discussion of VLAN tagging with respect to claim limitation [1.3], which I incorporate herein by reference.

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. *See, e.g., id.*, [0063] (“Access point 209 can include **other ports (not shown)** for communicating with other computer systems.”). A POSITA would understand 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. *See, e.g., id.*, [0060] (“data routing device 214 can be configured to separate computer systems into different VLANs.”).

137. Accordingly, Krantz discloses or renders obvious 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.*”

4. Claim 5

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

138. Claim 5 is disclosed by Krantz. In particular, 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.”)

139. Accordingly, Krantz renders obvious “[t]he method of claim 1, wherein the security policy includes authentication of the user of the device.”

5. Claim 6

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

140. Claim 6 is obvious over Krantz in view of the disclosures in Herrmann. As I explain above with respect to claims 1 and 3, Krantz discloses obtaining audit data from an access device and the application of a security policy to determine if access requirements are satisfied. I incorporate those discussions into my analysis for claim 6.

141. A POSITA would have understood that one way to collect the audit data, as disclosed in Krantz, would be by utilizing a client agent, 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 VIII.C.

142. The 350 Patent explains that “Access Device 230 is configured to execute a software and/or hardware agent for communicating with GateKeeper 225. For example, in one embodiment, Access Device 230 includes an agent configured to monitor code running on Access Device 230 and report any suspicious code to GateKeeper 225. In another example, Access Device 230 may include software and/or hardware configured to monitor other devices connected to Access Device 230 and to report information about these devices (e.g., their security statuses or MAC addresses) to GateKeeper 225.” Ex.1101, 7:21-30.

143. 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:

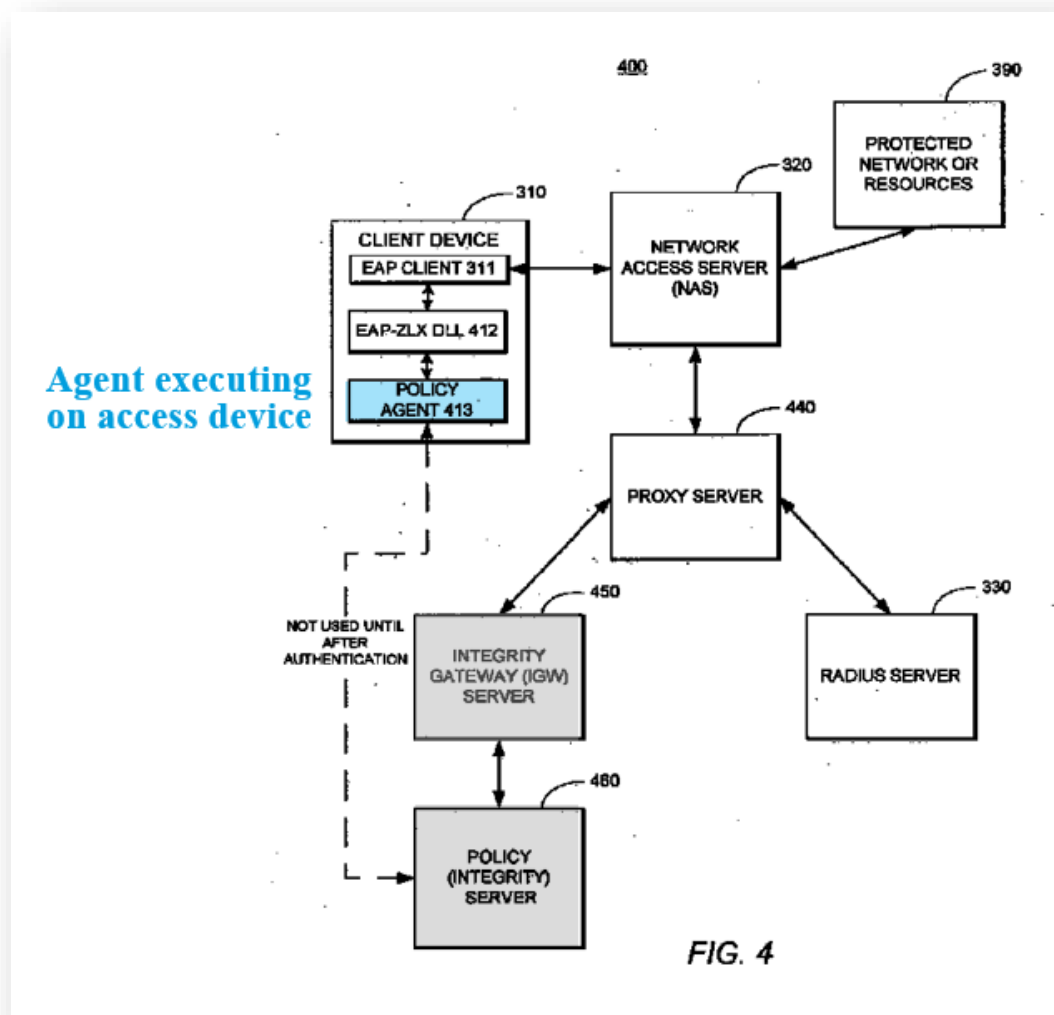
A configuration sub-file to indicate a type of EAP [is] used to authenticate a server with a client and/or to authenticate a client with a server. Either or both of the elements at lines 61 and 62 can be included in a configuration sub-file to indicate different EAP types, such as, for example, EAP-

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].

144. A POSITA would have understood that one way that audit data (e.g., operating system credentials, certificates, keys, Response/Identity message, user-identifier and password, and supported cipher suites, etc.) such as those disclosed in Krantz would collected would be by utilizing a client agent, 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 VIII.C.

145. For example, Herrmann discloses a “POLICY AGENT 413” (emphasized in blue) executing on the client device (*i.e.*, 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 (Herrmann), Fig. 4 (annotated)

146. 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].

147. A POSITA would be motivated to add the security policy agent of Herrmann to the client device of Krantz for several reasons. As I explained previously, two of the stated goals of Krantz involve automation and security. *See, e.g.*, 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.”); *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 the policy **agent** of Herrmann would be complimentary and an improvement to the system of Krantz, as it would provide an automated means of providing network security.

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

149. Accordingly, Krantz in combination with Herrmann renders obvious “[t]he method of claim 4, wherein an agent running on the device collects the audit data.”

6. Claim 7

- a. **[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.***

150. Krantz and Herrmann renders obvious claim 7. I have already explained how Krantz in view of the disclosures in Herrmann discloses “*an agent running on the device that collects the audit data*” with respect to claim 6. I incorporate that discussion into my analysis for claim 7.

151. Additionally, Krantz explains that “[w]hen full access to resources located on the second network is not authorized [i.e., *device fails to comply with the security policy* as I discussed *supra*], 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** [i.e., *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.”); Ex.1105, [0110] (“In parallel with acts 302 through 305, the method 300 also includes an act of executing a schema-based document (act 306). **This can include executing a third schema-based document to configure a client for accessing the second network. For example, provisioning module 208 can execute an XML document, defined in accordance with an XML configuration schema, to appropriately configure client 205 for accessing resources located on VLAN C** [*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.”

152. Accordingly, Krantz and Herrmann renders obvious “[t]he 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.”

7. Claim 8

- a. **[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.**

153. Krantz and Herrmann renders obvious claim 8. I have already explained how Krantz in view of the disclosures in Herrmann discloses “an agent

running on the device that collects the audit data” with respect to claim 6. I incorporate that discussion into my analysis for claim 8.

154. 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. As I discussed with respect to claim 6, 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 and some of the data may include “*audit data . . . concerning the operating system of the device.*” Ex.1105 [0099]:

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

155. Accordingly, Krantz and Herrmann renders obvious “[t]he 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.”

8. Claim 9

- a. **[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.***

156. Krantz in view of the disclosures in Herrmann discloses claim 9. I have already explained how Krantz in view of the disclosures in Herrmann discloses “an agent running on the device that collects the audit data” with respect to claim 6. I incorporate that discussion into my analysis for claim 9.

157. Krantz in view of the disclosures in Herrmann further discloses that the “*audit data collected by the agent ... concerns antivirus software on the device.*”

158. 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.*” *Id.*, [0013].

159. Krantz also specifically discusses how a connecting device may be required to have “provisioning files [] for gaining full access to network 413.” *Id.*, [0056]; *see also*, Ex.1105, [0032], [0078] (discussing provisioning clients for gaining access to the network). A POSITA would have understood that in practice, provisioning files generally relate to network connectivity and security, *see, e.g.*, Ex.1109, [0079], although Krantz does not explicitly mention *antivirus software* as a kind of “*audit data.*” However, as I discussed in § VIII.C, which I incorporate herein, a POSITA would have found it obvious to check for *antivirus software* in view of Herrmann.

160. 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].

161. 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.” *Id.*, [0071] (i.e., the *audit data ... concerns antivirus software on the device*. This may be implemented using security rules and checking system data for connecting devices to ascertain compliance. *See, id.*, [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.**”).

162. 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. *See*, 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 the importance of as confirmed by the 350 Patent itself. In the background section of the 350 Patent it discusses a **prior art** GateKeeper 110 (Ex.1101, 2:30-31) 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.

163. Accordingly, Krantz in combination with Herrmann discloses “[t]he *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.*”

9. Claim 10

- a. [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.*

164. Krantz in view of the disclosures in Herrmann discloses claim 10. I have already explained how Krantz in view of the disclosures in Herrmann discloses “*an agent running on the device that collects the audit data*” with respect to claim 6. I incorporate that discussion into my analysis for claim 10.

165. 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.*”

166. Although 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* § VIII.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.” *Id.*

167. 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.” *Id.*, [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. *Id.*, [0057], [0067].

168. 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.

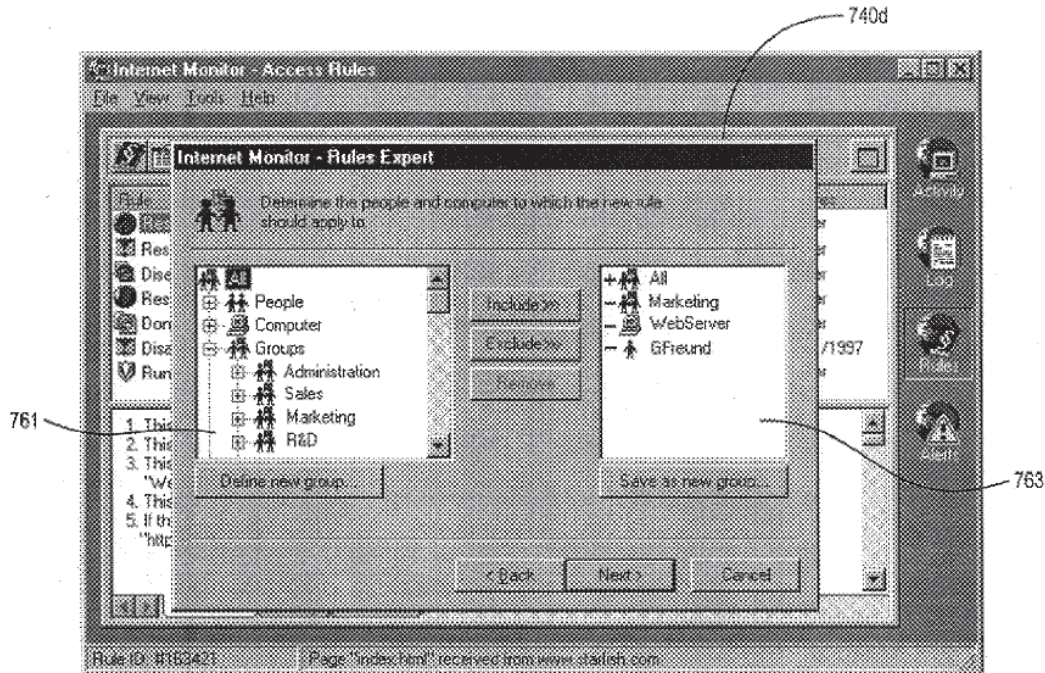


FIG. 7F

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

169. 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 environment (i.e., “concerns other devices coupled to the device.”).

170. Accordingly, Krantz in combination with Herrmann renders obvious “[t]he 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.”

10. Claim 13

- a. **[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.***

171. Krantz in view of the disclosures in Herrmann discloses claim 13. I have already explained how Krantz in view of the disclosures in Herrmann discloses “*an agent running on the device that collects the audit data*” with respect to claim 6. I incorporate that discussion into my analysis for claim 13.

172. Krantz in view of the disclosures in Herrmann additionally discloses that the audit data collected by the agent “*concerns applications executing on the device.*” One such application includes antivirus software. As I explained with respect to claim 9, 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].

173. 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.” *Id.*, [0071]. This may be implemented using security rules and checking system data for connecting devices to ascertain compliance. *See, id.*, [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** [i.e., “*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 the audit data “*concerns application(s) executing on the device.*”

174. As I explained with respect to claim 9, 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. *See*, 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.

175. Accordingly, Krantz in combination with Herrmann renders obvious “[t]he 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.”

11. Claim 16

- a. **[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.***

176. Krantz discloses “wherein the security policy audit is based at least in part on the information concerning an identity of a user of the device.” In particular, 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].

177. Accordingly, Krantz renders obvious “[t]he 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.”

12. Claim 18

- a. [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.*

178. Krantz in view of the disclosures in Herrmann discloses claim 18. I have already explained how Krantz in view of the disclosures in Herrmann discloses “*an agent running on the device that collects the audit data*” with respect to claim 6. I incorporate that discussion into my analysis for claim 18. 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** [i.e., “*updated audit data pertaining to 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. 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”

[i.e., “*updated audit data continues to be received from the agent after reconfiguring the access point*”]. Ex.1105, [0108].

179. 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)** [i.e., “*updated audit data continues to be received from the agent after reconfiguring the access point*”]. If the policy server verifies that the client is indeed in compliance with the assigned policy, it sends an ‘ISS_AUTH_OK’ message to the IGW server to indicate that the session should be unrestricted. In response 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.

180. Accordingly, Krantz in combination with Herrmann renders obvious “[t]he method of claim 6, wherein updated audit data pertaining to the device continues to be received from the agent after reconfiguring the access point.”

13. Claim 19

- a. [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.*

181. Krantz in view of the disclosures in Herrmann discloses claim 19. I have already explained how Krantz in view of the disclosures in Herrmann discloses “an agent running on the device that collects the audit data” with respect to claim 6. I incorporate that discussion into my analysis for claim 13.

182. 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 I 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]. This means that *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).*

183. 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 indeed in compliance with the assigned policy, it sends an ‘ISS_AUTH_OK’ message to the IGW server to indicate that the session should be unrestricted. In response to receiving the ‘ISS_AUTH_OK’ message from the policy server, the IGW server directs the NAS to remove the restrictive filter.” Ex.1106, [0080].

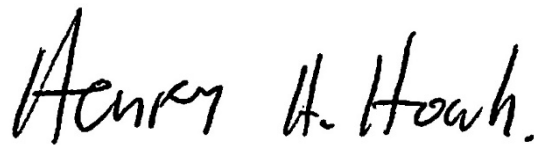
184. As I explained with respect to claim 18, nothing in Krantz or Herrmann suggests that the continued collection of audit data would cease while the device has access to the less-restricted subset of the network; instead use of a session timeout and/or periodic “IA_HEARTBEAT” protocol suggests it would continue even while the device has access to the less-restricted subset of the network.

185. Accordingly, Krantz in combination with Herrmann renders obvious “[t]he 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.”

X. CONCLUSION

186. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and that these statements were made with knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code.

Dated: March 8, 2024

A handwritten signature in black ink that reads "Henry H. Houh." The signature is written in a cursive, slightly slanted style.

Henry Houh, Ph.D.